Pimpri Chinchwad Education Trust's

Pimpri Chinchwad University

Sathe, Pune - 412106

PCET's Pimpri Chinchwad University

Learn | Grow | Achieve

Curriculum Structure

B.Sc. (Cyber Security)

(Revised 2024 Pattern)

School of Computer Applications

Effective from Academic Year 2024-25

Program Curriculum

Preamble:

At Pimpri Chinchwad University, we present the Bachelor of Science (Cyber Security), an Undergraduate Program designed to equip students with a comprehensive understanding of Computer Science and Cyber Security. As aspiring professionals in the field of computing, we acknowledge the weight of responsibility that accompanies our education. Upholding the highest standards of integrity, professionalism, and ethical conduct is fundamental to our academic pursuits and beyond. We embrace the imperative of continuous learning and adaptability in an era marked by rapid technological advancement, pledging to proactively seek new knowledge and master emerging technologies.

The BSc (Cyber Security) program curriculum is designed to provide students with the practice of protecting computer systems, networks, and data from digital threats, such as unauthorized access, data breaches, malware, and other cyber-attacks.
Overall, an BSc (Cyber Security) program aims to provide students with a well-rounded education that prepares them for a successful career in the IT industry and for further academic pursuits.

Vision and Mission of Program:

Vision:

Explore the different horizons in the field of Cyber Security, digital threats, data breaches and Cyber-attacks.

Mission:

Develop a strong foundation in computer science and information technology. Cultivate smart and ethical cybersecurity professionals and entrepreneurs globally.

Program Educational Objectives:

Here are some possible Program Educational Objectives (PEOs) for a Bachelor of Science (Cyber Security).

1. To prepare youth to take up positions as Secure software designers and developers.
2. To aim at the development of knowledge and skills for defending and developing secure software systems.
3. To prepare students with social interaction skills, communication skills, life skills, entrepreneurial skills, and research skills which are necessary for career growth and for leading a quality life.

Program Outcome

Here are some possible Program Outcomes (POs) for a Bachelor of Science (Cyber Security) program: -

PO 1: Develop Core Competencies: The program aims to develop the core competencies required for a career in computer science and Cyber Security.

PO 2: Develop Practical Cybersecurity Skills: The program focuses on equipping students with practical skills required for securing computer systems and networks.

PO 3: Analyze and Mitigate Security Risks: The program emphasizes the importance of risk management and equips students with the knowledge to make informed decisions regarding security measures.

PO 4: Foster Ethical and Professional Practices: The program instills ethical and professional values in students, emphasizing the importance of integrity, privacy, and responsible use of cybersecurity knowledge and skills.

PO 5: Promote Critical Thinking and Problem-Solving Abilities: The program aims to develop students' analytical and problem-solving skills in the context of cybersecurity.

PO 6: Collaborate and Communicate Effectively: The program emphasizes the importance of teamwork and effective communication skills. These skills are essential for working effectively in multidisciplinary cybersecurity teams and conveying complex concepts to various stakeholders.

PO 7: Stay Updated with Emerging Technologies and Trends: The program aims to keep students abreast of the rapidly evolving field of cybersecurity. They are encouraged to stay updated with emerging technologies, trends, and research advancements in cybersecurity.

PO 8: Establishing strategies in developing and implementing ideas in multi- disciplinary environments using computing, cyber security and management skills as a member or leader in a team.

PO 9: Contribute to progressive community and society in comprehending different cyber security activities.

PO 10: Gain confidence for self and continuous learning to improve knowledge and competence as a member or leader of a team.

PO11: Communication Skills: Express thoughts and ideas effectively in writing and orally; communicate with others using appropriate medium; demonstrate the ability to listen carefully, read and write analytically, and present complex information in a clear and concise manner to different groups.

PO12: Self-directed and Life-long Learning**:** Acquire the ability to engage in independent and life-long learning in the broadest context of socio-technological changes to identify and detect Cyber Vulnerabilities and resolve new Cyber Threats.

Program Specific Outcomes

On successful completion of the programme, the graduates of Bachelor of Science (Cyber Security) programme will be able to:

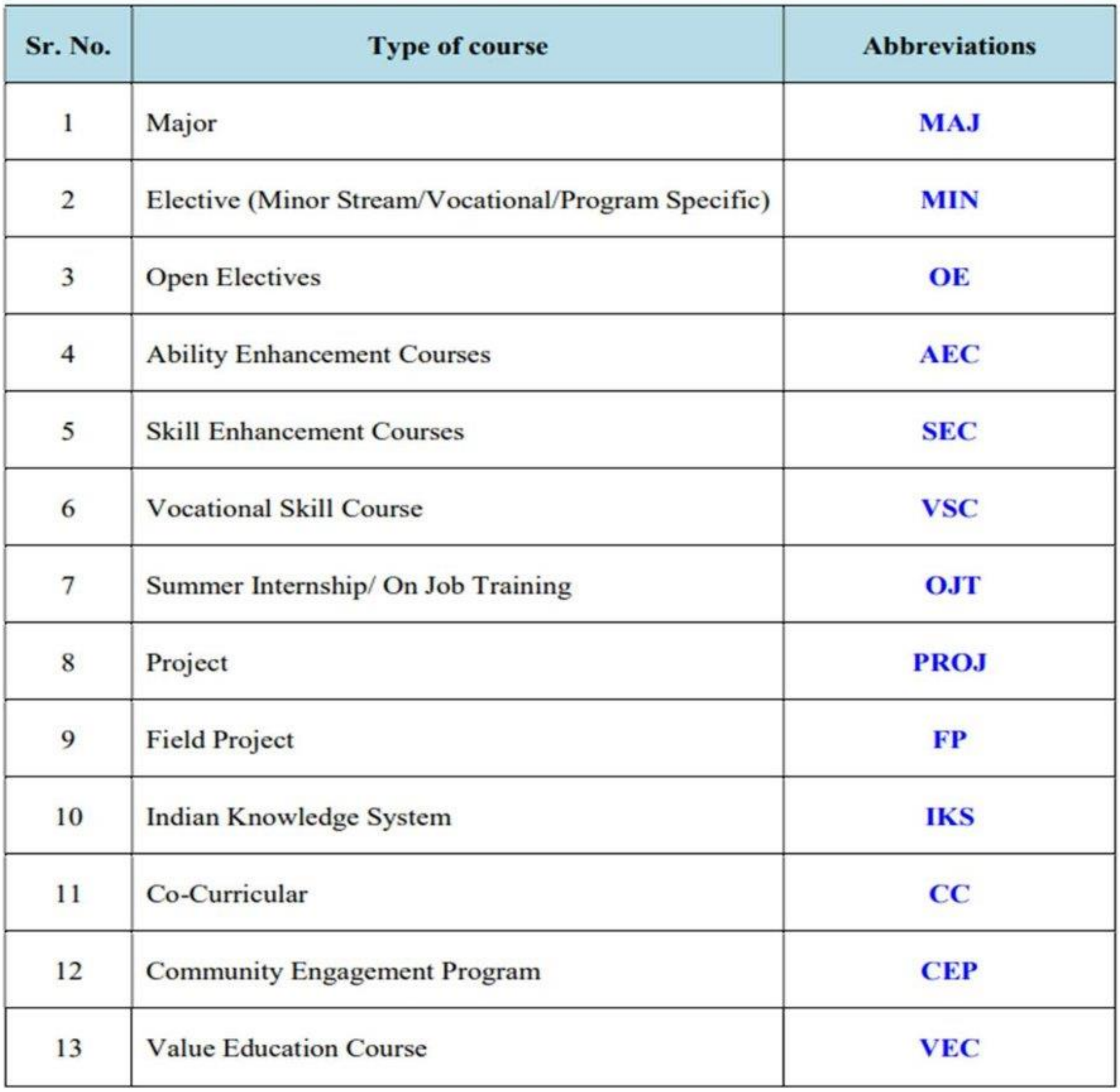
PSO1: -Resolve security issues in computer networks and maintenance of Cyber Security systems to secure an IT infrastructure.

PSO2: -Provide Security Based Solutions with to solve real life problems like malware, phishing, spamming and other Cyber Threats, related to Cyber Security.

PSO3: -Design, Implement, and Monitor-Cyber Security Mechanisms, to ensure the protection of Information Technology Assets through Advanced Penetration Testing and Reverse Engineering to get to know the perspective of Cyber Criminals.

INDEX

CURRICULUM FRAMEWORK



Sr. No.	Type of course	Abbreviations
1	Major	**MAJ**
2	Elective (Minor Stream/Vocational/Program Specific)	**MIN**
3	Open Electives	**OE**
4	Ability Enhancement Courses	**AEC**
5	Skill Enhancement Courses	**SEC**
6	Vocational Skill Course	**VSC**
7	Summer Internship/ On Job Training	**OJT**
8	Project	**PROJ**
9	Field Project	**FP**
10	Indian Knowledge System	**IKS**
11	Co-Curricular	**CC**
12	Community Engagement Program	**CEP**
13	Value Education Course	**VEC**

Sr. No.	Type of course	No. of Courses	Total Credits	
			No	%
1	Major	**33**	**79**	**49**
2	Elective (Minor Stream/Vocational/Program Specific)	**5**	**10**	**6**
3	Open Electives	**4**	**8**	**5**
4	Ability Enhancement Courses	**3**	**-**	**-**
5	Skill Enhancement Courses	**6**	**18**	**11**
6	Vocational Skill Course	**6**	**13**	**8**
7	Summer Internship/On Job Training/Project	**2**	**4**	**3**
8	Field Project	**2**	**26**	**16**
9	Indian Knowledge System	**1**	**-**	**-**
10	Value Education Course (Audit Courses)	**8**	**2**	**1**
Total		**70**	**160**	**100**

CREDIT DISTRIBUTION: SEMESTER WISE

Sr. No.	Type of course	No. of Credits/Semester								Total
		1	2	3	4	5	6	7	8	
1	Major	13	12	13	14	11	3	10	3	**79**
2	Elective (Minor Stream/Vocational/Program Specific)	-	2	2	2	2	2	-	-	**10**
3	Open Electives	2	2	2	2	-	-	-	-	**8**
4	Ability Enhancement Courses	-	-	-	-	-	-	-	-	**0**
5	Skill Enhancement Courses	5	2	3	2	3	-	3	-	**18**
6	Vocational Skill Course	-	2	-	-	2	3	3	3	**13**
7	Summer Internship/On Job Training/Project	-	-	-	-	2	-	2	-	**4**
8	Field Project	-	-	-	-	-	12	-	14	**26**
9	Indian Knowledge System									**AC**
10	Value Education Course (Audit Courses)	-	-	-	-	-	-	2	-	**2**
Total		20	20	20	20	20	20	20	20	160

Course Code Nomenclature

COURSE CODE	COURSE NAME	COURSE TYPE
UBS101	Programming Concepts Using C Language	MAJM
UBS102	Programming Concepts Using C Language Lab	MAJM
UBS103	Data Communication and Networking	MAJM
UBS104	Data Communication and Networking Lab.	MAJM
UBS105	Introduction to Cyber Security	SEC
UBS106	Basic Mathematics	BSC
UBS107	Fundamentals of Computer Architecture	SEC
UEG101	Applied Communication	AEC
ACUHV101	UHV- I: Professional Ethics	AC
ACIKSSS101	IKS: Concepts and Application in Science	AC
UBS108A	OPEN ELECTIVE-I: Introduction to IoT	OE
UBS108B	OPEN ELECTIVE-I: Introduction to Digital Electronics	OE
SEMESTER-II		
UBS109	Programming using Advanced C	MAJM
UBS110	Programming using Advanced C lab	MAJM
UBS111	Unix & Shell Programming	MAJM
UBS112	Unix & Shell Programming Lab	MAJM
UBS114	Foundation of Cryptography	VSC
UBS115	Discrete Mathematics	BSC
ACIKSSS101	IKS: Concepts and Application in Science	AC
ACUHV101	UHV-I: Professional Ethics	AC
UBS116A	OPEN ELECTIVE-II: Cyber Laws	OE
UBS116B	OPEN ELECTIVE-II: e-Commerce	OE
UBSM102	Fundamental of Digital Marketing and E-Commerce	**MOOC**
UBSM103	Privacy Law and Data Protection	**MOOC**
UCEXBS101	VSC: Cyber Defense	VSC
UCEXBS102	VSC: Project	VSC

SEMESTER-III		
UBS201	Design Analysis of Algorithm	MAJM
UBS202	Design Analysis of Algorithm Lab	MAJM
UBS203	Web Application Security	MAJM
UBS204	Web Application Security Lab	MAJM
UBS205A	MAJOR ELECTIVE-I: Operating System Security	MAJE
UBS205B	MAJOR ELECTIVE-I: Firewall and VPN Security	MAJE
UBS207	Statistical Techniques	BSC
ACUHV201	UHV-II: Understanding Harmony	AC
ACCOI201	COI: Constitution of India	AC
UBS208A	OPEN ELECTIVE-III: Foundation of Big data	OE
UBS208B	OPEN ELECTIVE-III: Introduction to Digital Image Processing	OE
UFL201A	Foreign Language-I:rman Ge	AEC
UFL201B	Foreign Language-I: Japanese	AEC
SEMESTER-IV		
UBS209	Operating Systems - Linux	MAJM
UBS210	Operating Systems Lab	MAJM
UBS211	Mobile Security	MAJM
UBS212	Mobile Security Lab	MAJM
UBS213A	MAJOR ELECTIVE-II: Cyber laws & Security Policies	MAJE
UBS213B	MAJOR ELECTIVE-II: Cyber Threat Intelligence	MAJE
UBS214	Data Privacy	SEC
UBS215	Groups and Codings	BSC
UBS216A	OPEN ELECTIVE-IV: Search Engine Optimization	OE
UBS216B	OPEN ELECTIVE-IV: Introduction to WordPress	OE
ACCO1201	COI: Constitution of India	AC
ACUHV201	UHV-II: Understanding Harmony	AC
UFL202A	Foreign Language-II: Japanese	AEC
UFL202B	Foreign Language-II: German	AEC
UDIEXBS201	VSC: Cyber Crime Investigation and Digital Forensics	VSC
UDIEXBS202	Project	VSC

SEMESTER-V

UBS301	Ethical Hacking	MAJM
UBS302	Ethical Hacking Lab	MAJM
UBS303	Malware Analysis & Reverse Engineering	MAJM
UBS304	Malware Analysis & Reverse Engineering Lab	MAJM
UBS305A	MAJOR ELECTIVE-I: Cyberspace Operations and Design	MAJE
UBS305B	MAJOR ELECTIVE-I: Secure Software Design and Development	MAJE
UBS306	Applied Cryptography	BSC
MIN	Minor IV	
UBS307	Mini Project Using Blockchain / Python	PROJ
ACALR301/ACEVS 301	ACALR301/ACEVS301	AC
UFL301A	Foreign Language - III-German	AEC
UFL301B	Foreign Language - III-Japanese	AEC
UBSM107	Security in Wireless Ad hoc Network	MOOC

SEMESTER-VI
(SCHEME - A)

UBS308	BlockChain Technology	MAJM
ACEVS301/ACALR 301	EVS: Environmental Studies / ALR: Aptitude & Logical Reasoning	AC
UETCS105	Minor –V	MIN
UBS310	Industrial Training / Internship / Seminar/ Research Internship	FP
UBSM109	Research Methodologies and Techniques	MOOC
UBSM110	Mobile Forensic	MOOC

SEMESTER-VI
(SCHEME - B)

UBS308	BlockChain Technology	MAJM (MOOC)
ACEVS301/ ACALR301	EVS: Environmental Studies / ALR: Aptitude & Logical Reasoning	AC
UETCS105	Minor –V	MIN
UBS310	Industrial Training / Internship / Seminar/ Research Internship	FP
UBSM109	Research Methodologies and Techniques	MOOC
UBSM110	Mobile Forensic	MOOC

SEMESTER-VII		
UBS401	Vulnerability Assessment & Penetration Testing	MAJM
UBS402	Vulnerability Assessment & Penetration Testing Lab	MAJM
UBS403	Python Programming	MAJM
UBS404	Python Programming Lab	MAJM
UBS405	AI in Cyber Security	BSC
UBS406	Security in Wireless Ad Hoc Networks	VSC
UBS407	Mini Project Using Penetration Testing/Reverse Engineering	PROJ
UBSM111	Cyber Crime	MOOC
UBSM112	Threat Investigation	MOOC
UFL401A	Foreign Language-III-German	AEC
UFL401B	Foreign Language-III-Japanese	AEC
SEMESTER-VIII		
UBSM113	Google Cyber Security Professional	MOOC
UBSM114	Security Analyst Fundamentals Specialization	MOOC
UBSM408	Major Project/Research Project/Internship	FP

PROGRAM STRUCTURE

PIMPRI CHINCHWAD UNIVERSITY, PUNE, MAHARASHTRA

PROGRAM STRUCTURE

SCHOOL OF COMPPUTER APPLICATIONS

BACHELOR OF COMPUTER SCIENCE-CYBER SECURITY (B.Sc.-CS) Revised 2024 PATTERN

(Effective from the Academic Year (2024 - 2025)

SEMESTER I

COURSE CODE	**COURSE TYPE**	**COURSE NAME**	**TEACHING SCHEME**					**ASSESSMENT SCHEME**			
			TH	**PR**	**TUT**	**CREDIT**	**HRS**	**CIA**	**ESA**	**PR/OR**	**TOTAL**
UBS101	MAJM	Programming Concepts Using C Language	3	-	-	3	3	40	60		100
UBS102	MAJM	Programming Concepts Using C Language Lab	-	2	-	1	4	25		25	50
UBS103	MAJM	Data Communication and Networking	3	-	-	3	3	40	60		100
UBS104	MAJM	Data Communication and Networking Lab.	-	2	-	1	4	25		25	50
UBS105	SEC	Introduction to Cyber Security	2	-	-	2	2	20	30		50
UBS106	BSC	Basic Mathematics	3	-	-	3	3	40	60		100
UBS107	SEC	Fundamentals of Computer Architecture	3	-	-	3	3	40	60		100
UEG101	AEC	Applied Communication	2	-	-	-	2	50			50
ACUHV101 / ACIKSSS101	AC	UHV - I: Professional Ethics / IKS: Concepts and Application in Science	2	-	-	-	2	50			50
UBS108	OE	Open Elective - I	2	-	-	2	2	20	30		50
UBSM101	MOOC	Programming with a Purpose(MOOC)	2	-	-	2	2	25	25	-	50
TOTAL			**20**	**4**	**0**	**20**	**28**	**375**	**325**	**50**	**750**
UBS108 OPEN ELECTIVE – I											
UBS108A	OE	Introduction to IoT	2	-	-	2	2	20	30		50
UBS108B	OE	Introduction to Digital Electronics	2	-	-	2	2	20	30		50

SEMESTER II											
COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	HRS	CIA	ESA	PR/OR	TOTAL
UBS109	MAJM	Programming using Advanced C	3	-	-	3	3	40	60		100
UBS110	MAJM	Programming using Advanced C lab	-	1	-	1	2	25		25	50
UBS111	MAJM	Unix & Shell Programming	3	-	-	3	3	40	60		100
UBS112	MAJM	Unix & Shell Programming Lab	-	1	-	1	2	25		25	50
UBS114	VSC	Foundation of Cryptography	2	-	-	2	-	20	30		50
UBS115	BSC	Discrete Mathematics	2	-	-	2	2	20	30		50
	MIN	Minor I	2	-	-	2	2	20	30		50
ACIKSSS101/ ACUHV101	AC	IKS: Concepts and Application in Science / UHV - I: Professional Ethics	2	-	-	-	2	50			50
UBS116	OE	Open Elective – II	2	-	-	2	2	20	30		50
UBSM102	MOOC	Fundamental of Digital Marketing and E-Commerce	2	-	-	2	2	25	25		50
UBSM103	MOOC	Privacy Law and Data Protection	2	-	-	2	2	25	25	-	50
TOTAL			20	2	0	20	22	310	290	50	650
UBS116 OPEN ELECTIVE – II											
UBS116A	OE	Cyber Laws	2	-	-	2	2	20	30		50
UBS116B	OE	E-Commerce	2	-	-	2	2	20	30		50

Exit Policy: UG Certificate in B.Sc. (Cyber Security): A Students who opt to exit after completion of the first year and have scored the required credits offered by the school in the program structure will be awarded a UG certificate in **B.Sc. (Cyber Security)**, provided they must earn additional credits during the summer vacation of the first year.

COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	Hrs.	CIA	ESA	PR/ OR	TOTAL
UCEXBS101	VSC	Cyber Crime Investigation and Digital Forensics/ MOOC	2	-	-	2	2	50	-	-	50
UCEXBS102	VSC	Project	-	2	-	2	4	-	-	50	50

***Project- In-house/ Sponsored/ Case Study/ Fieldwork**

SCHOOL OF COMPUTER APPLICATIONS

BACHELOR OF COMPUTER SCIENCE-CYBER SECURITY (B.Sc.-CS) Revised 2024 PATTERN

Effective from the Academic Year (2024 - 2025)

SEMESTER III

COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CRE DIT	HRS	CIA	ESA	PR/ OR	TOTAL
UBS201	MAJM	Design Analysis of Algorithm	3	-	-	3	3	40	60		100
UBS202	MAJM	Design Analysis of Algorithm Lab	-	1	-	1	2	25		25	50
UBS203	MAJM	Web Application Security	3	-	-	3	3	40	60		100
UBS204	MAJM	Web Application Security Lab	-	1	-	1	2	25		25	50
UBS205	MAJE	Major Elective – I	-	-	-	3	3	40	60		100
UBS207	BSC	Statistical Techniques	2	-	-	2	2	20	30		50
ACUHV201/ ACCOI201	AC	UHV-II: Understanding Harmony / COI: Constitution of India	2	-	-	-	2	50			50
	MIN	Minor II	2	-	-	2	2	20	30		50
UBS208	OE	Open Elective – III	2	-	-	2	2	20	30		50
UFL201	AEC	Foreign Language – I	2	-	-	-	2	50			50
UBSM104	MOOC	Introduction to Web Technology	**3**	-	-	3	3	50	50		100
TOTAL			**19**	**2**	**0**	**20**	**26**	**370**	**320**	**50**	**750**
UBS205 MAJOR ELECTIVE – I											
UBS205A	MAJE	Operating System Security	3	-	-	3	3	40	60		100
UBS205B	MAJE	Firewall And VPN Security	3	-	-	3	3	40	60		100
UBS208 OPEN ELECTIVE – III											
UBS208A	OE	Foundation of Big data	2	-	-	2	2	20	30		50
UBS208B	OE	Introduction to Digital Image Processing	2	-	-	2	2	20	30		50
UFL201 FOREIGN LANGUAGE – I											
UFL201A	AEC	Foreign Language-I: German	2	-	-	-	2	50			50
UFL201B	AEC	Foreign Language-I: Japanese	2	-	-	-	2	50			50

SEMESTER IV												
COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CRE DIT	HRS	CIA	ESA	PR/ OR	TOTAL
UBS209	MAJM	Operating Systems - Linux	3	-	-	3	3	40	60		100
UBS210	MAJM	Operating Systems Lab	-	1	-	1	2	25		25	50
UBS211	MAJM	Mobile Security	3	-	-	3	3	40	60		100
UBS212	MAJM	Mobile Security Lab	-	1	-	1	2	25		25	50
UBS213	MAJE	Major Elective – II	3	-	-	3	3	40	60		100
	MIN	Minor III	2	-	-	2	2	20	30		50
ACCOI201/ ACUHV201	AC	COI: Constitution of India / UHV-II: Understanding Harmony	2	-	-	-	2	50			50
UBS214	OE	Open Elective – IV	2	-	-	2	2	20	30		50
UFL202	AEC	Foreign Language – II	2	-	-	-	2	50			50
UBSM105	MOOC	Certified Information Systems Security Professional Specialization	2	-	-	2	2	25	25		50
UBSM106	MOOC	IT Support Professional Certificate	3	-	-	3	3	50	50	-	100
TOTAL			22	2	0	20	26	385	315	50	750

UBS213 MAJOR ELECTIVE - II												
UBS213A	MAJE	Cyber laws & Security Policies	3	-	-	3	3		40	60		100
UBS213B	MAJE	Cyber Threat Intelligence	3	-	-	3	3		40	60		100
UBS216 OPEN ELECTIVE - IV												
UBS214A	OE	Search Engine Optimization	2	-	-	2	2		20	30		50
UBS214B	OE	Introduction to WordPress	2	-	-	2	2		20	30		50
UFL202 FOREIGN LANGUAGE - II												
UFL202A	AEC	Foreign Language-II: Japanese	2	-	-	-	2		50			50
UFL202B	AEC	Foreign Language-II: German	2	-	-	-	2		50			50

Exit Policy: UG Diploma in B.Sc. (Cyber Security): A Students who opt to exit after completion of the second year and have scored the required credits offered by the school in the program structure will be awarded a UG diploma in **B.Sc. (Cyber Security)**, provided they must earn additional credits during the summer vacation of the second year.

COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME						ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	Hrs.		CIA	ESA	PR/ OR	TOTAL
UDIEXBS201	VSC	Cyber Defense/MOOC	**2**	**-**	-	**2**	**2**		**-**	**-**	**50**	**50**
UDIEXBS202	VSC	Project	**-**	**4**	-	**4**	**8**		**50**	**-**	**50**	**100**

***Project- In-house/ Sponsored/ Case Study/ Fieldwork**

SEMESTER V											
COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	HRS	CIA	ESA	PR/OR	TOTAL
UBS301	MAJM	Ethical Hacking	3	-	-	3	3	40	60		100
UBS302	MAJM	Ethical Hacking Lab.	-	1	-	1	2	25		25	50
UBS303	MAJM	Malware Analysis & Reverse Engineering	3	-	-	3	3	40	60		100
UBS304	MAJM	Malware Analysis & Reverse Engineering Lab	-	1	-	1	2	25		25	50
UBS305	MAJE	Major Elective - III	3	-	-	3	3	40	60		100
UBS306	SEC	Applied Cryptography	3	-	-	3	3	40	60		100
	MIN	Minor IV	2	-	-	2	2	20	30		50
UBS307	PROJ	Mini Project Using Ethical Hacking/Reverse Engineering	-	2	-	2	4	25		25	50
ACALR301 /ACEVS301	AC	ALR: Aptitude & Logical/ ReasoningEVS: Environmental Studies	2	-	-	-	2	50			50
UFL301	AEC	Foreign Language - III	2	-	-	-	2	50			50
UBSM107	MOOC	Security in Wireless Ad hoc Network	2	-	-	2	2	25	25		50
TOTAL			18	4	0	20	28	480	295	75	750

UBS305 MAJOR ELECTIVE – III											
UBS305A	MAJE	Cyberspace Operations and Design	3	-	-	3	3	40	60		100
UBS305B	MAJE	Secure Software Design and Development	3	-	-	3	3	40	60		100

SEMESTER VI
SCHEME - A

COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME						ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	HRS		CIA	ESA	PR/OR	TOTAL
UBS308	MAJM	BlockChain Technology	2	-	-	2	2		20	30		50
ACEVS301/ ACALR301	AC	EVS: Environmental Studies / ALR: Aptitude & Logical Reasoning	2	-	-	-	2		50			50
UETCS105	MIN	Minor –V	2	-	-	2	2		20	30		50
UBS310	FP	Industrial Training / Internship / Seminar/ Research Internship	-	12	-	12	12		250		250	500
UBSM109	**MOOC**	Research Methodologies and Techniques	2	-	-	2	2		25		25	50
UBSM110	**MOOC**	Mobile Forensic	2	-	-	2	2		25		25	50
TOTAL			**10**	**12**	**0**	**20**	**22**		**390**	**60**	**300**	**750**

SEMESTER VI
SCHEME - B

COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	HRS	CIA	ESA	PR/OR	TOTAL
UBSM111	**MAJM (MOOC)**	BlockChain Technology	2	-	-	2	2	20	30		50
ACEVS301 / ACALR301	AC	EVS: Environmental Studies / ALR: Aptitude & Logical Reasoning	2	-	-	-	2	50	-	-	50
UETCS105	MIN	Minor –V	2	-	-	2	2	20	30	-	50
UBS310	FP	Industrial Training / Internship / Seminar/ Research Internship	-	12	-	12	12	250		250	500
UBSM109	**MOOC**	Research Methodologies and Techniques	2	-	-	2	2	25	-	25	50
UBSM110	**MOOC**	Mobile Forensic	2	-	-	2	2	25		25	50
TOTAL			**10**	**12**	**0**	**20**	**22**	**390**	**60**	**300**	**750**

Note:

1. Scheme A – Regular Students (student should maintain a minimum attendance of 75%)
2. Scheme B – Students with Pre-Placement Offer (students should follow the activity schedule and report accordingly).

SEMESTER VII

COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	HRS	CIA	ESA	PR/OR	TOTAL
UBS401	MAJM	Vulnerability Assessment & Penetration Testing	3	-	-	3	3	40	60		100
UBS402	MAJM	Vulnerability Assessment & Penetration Testing Lab	-	1	-	1	2	25		25	50
UBS403	MAJM	Python Programming	3	-	-	3	3	40	60		100
UBS404	MAJM	Python Programming Lab	-	1	-	1	2	25		25	50
UBS405	SEC	AI in Cyber Security	3	-	-	3	3	40	60		100
UBS406	VSC	Security in Wireless Ad Hoc Networks	3	-	-	3	3	40	60		100
UBS407	PROJ	Mini Project Using Penetration Testing/Python	-	2	-	2	4	25		25	50
UBSM111	MOOC	Cyber Crime	2	-	-	2	2	25		25	50
UBSM112	MOOC	Threat Investigation	2	-	-	2	2	25		25	50
UFL401	AEC	Foreign Language - IV	2	-	-	-	2	50			50
TOTAL			**18**	**4**	**0**	**20**	**26**	**335**	**240**	**125**	**700**

SEMESTER-VIII

COURSE CODE	COURSE TYPE	COURSE NAME	TEACHING SCHEME					ASSESSMENT SCHEME			
			TH	PR	TUT	CREDIT	HRS	CIA	ESA	PR/OR	TOTAL
UBSM113	MOOC	Google Cyber Security Professional Certificate	3	-		3	3	50		50	100
UBSM114	MOOC	Security Analyst Fundamentals Specialization	3	-		3	3	50		50	100
UBS408	FP	Major Project/ Research Project / Internship	-	14	-	14	24	250		250	500
TOTAL			**6**	**14**	**0**	**20**	**30**	**350**	**--**	**350**	**700**

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester - I

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: I**		**Level: UG**	
Course Name		**Programming Concepts Using C Language**		**Course Code/ Course Type**		UBS101/MAJM	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
3	-	-	3	3	40	60	-
Prerequisite: Students should have basic Computer Knowledge							
Course Objectives (CO):				The objectives of Programming Concepts Using C Language are: 1. To remember the knowledge about Computer fundamentals. 2. To understand and trace the execution of programs written in C language. 3. To apply input and output operations using programs in C language. 4. To analyze the concepts and techniques in C Programming language. 5. To Design and create C code for a given problem.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the basic concepts of the C programming language. 2. Explain the compilation process in C language. 3. Apply knowledge of C programming to create Code for a given problem. 4. Analyze the use of Input Output Operations. 5. Evaluate the C code for a given Problem.			

Course Contents/Syllabus

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Fundamentals of Computers & Problem Solving in C: Fundamentals of Computers,Introduction,History of Computers,Generations of Computers, Classification of Computers,Basic Anatomy of a Computer System,Input Devices,Processor,OutputDevices,MemoryManagement,Types of Software,Overview of Operating System,Programming Languages,Translator Programs,Problem Solving Techniques.	**CLO 1**	**9**
UNIT II		
Overview of C: Overview of C,History and Features of C,Structure of a C Program with Examples,Creating and Executing a C Program,Compilation process in C,C Character Set,C tokens,Keywords,Identifiers,Constants and variables,Data types.	**CLO 1**	**9**
UNIT III		
Programming Basic Concepts: Declaration and initialization of variables; Symbolic constants,Formatted I/O functions,printf and scanf,Control strings and escape sequences,Output specifications with printf functions, Unformatted I/O functions to read and display single character and a string, getchar,putchar,gets and puts functions.	**CLO3**	**9**
UNIT IV		
Input and output with C: Formatted I/O functions,printf and scanf,control strings and escape sequences,output specifications with printf functions, Unformatted I/O functions to read and display single character and a string, getchar,putchar,gets and puts functions.	**CL04**	**9**
UNIT V		
C Operators, Expressions and Control Structures: Arithmetic operators, Relational operators,Logical operators,Assignment operators,Increment & Decrement operators,Bitwise operators,Conditional operator,Special operators,Operator Precedence and		

Associativity,Evaluation of arithmetic expressions,Type conversion,Decision making Statements,Simple if, if else, nested if else,else if ladder,Switch Case,goto,break & continue statements, Looping Statements,Entry controlled and exit controlled statements,while, do while,for loops,Nested loops.	**CLO5**	**9**
Total hours		**45**

Learning resources

Textbooks:
1. E Balagurusamy: Computing Fundamentals & C Programming – Tata McGraw-Hill
2. P. K. Sinha & Priti Sinha: Computer Fundamentals.
3. Kamthane: Programming with ANSI and TURBO C (Pearson Education)

Reference Books:
1. Henry Mullish & Hubert L.Cooper: The Spirit of C, Jaico
2. Ashok N Kamthane: Programming with ANSI and Turbo C, Pearson
3. V. Rajaraman: Programming in C.

Online Resources/E-Learning Resources

1. https://onlinecourses.nptel.ac.in/noc20_cs913
2. https://www.programiz.com/c-programming

Name of the Program:		**BSc (Cyber Security)**		**Semester: I**		**Level: UG**	
Course Name		**Programming Concepts Using C Language Lab**		**Course Code/ Course Type**		UBS102/MAJM	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme							**Assessment Scheme**
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
-	2	-	2	4	25	-	25
Prerequisite: Basic Computers is required.							
Course Objectives (CO):				The objectives of Programming Concepts Using C Language are: - 1. To Understand the fundamentals of programming in C Language. 2. To apply solution to problems and implement in C. 3. To analyze programming components to solve computing problems. 4. To evaluate and debug programs in C language. 5. To Design and create C Programs.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify data type for implementing programs in C language 2. Explain the modular programs involving input output operations. 3. Apply knowledge of decision making and looping constructs. 4. Analyze decision making and looping constructs. 5. Evaluate the C code for a given Problem.			

COURSE CURRICULUM

Course Contents/Syllabus: Practical Plan

Activity Number	Assignment/Practical/Activity Title	Week Number/Turn	Details	CLO	Hours
1	Familiarization with the Programming Environment. Introduction to Programming, Writing of Algorithms, Introduction to Drawing flow Charts /Preparation of Flowchart/ Steps for Writing Code in C/ Turbo C	Week 1 / Turn 1 and 2	To understand the basic fundamentals of C Programming. 1.1 First Basic Program-Writing a Single Statement. 1.2 Writing a Program to print your Basic details Multi statements.	CLO1	4
2	Using Turbo C and Fundamentals of Programming Language	Week 2/ Turn 1 and 2	To understand the basic fundamentals of C Programming 1.1 To perform simple Input-Output Operations. 1.2 To add two numbers.	CLO1	4
3	Assignment on use of data types, simple operators	Week 3/ Turn 1 and 2	To understand the basic fundamentals of C Programming.	CLO1	4

	(expressions)		1.1 WAP to perform simple arithmetic operations in C(Addition, Subtraction, Multiplication, Division, Modulus)		
4	Debugging and Single-Stepping of Programs	Week 4/ Turn 1 and 2	To understand the basic fundamentals of C Programming. 1.1 WAP to find the area and perimeter of the circle. 1.2 WAP to find area and perimeter of rectangle	CLO1	4
5	Formatted I/O functions – printf and scanf	Week 5/ Turn 1 and 2	To perform the various, I/O functions. 1.1 Given the values of three variable entered by user, write a program to compute and display the value of x, where x=a/(b-c)	CLO2	4
6	Read and display single character and a string	Week 6/ Turn 1 and 2	To apply the operations on character and string. 1.1 Write a C program to read a single character as input 1.2 To read sentences as input from the user 1.3 Read and Display ASCII values. 1.4 Read multiple inputs from the user.	CLO2	4
7	Assignment on decision making statements (if and if else)	Week 7/ Turn 1 and 2	Solve the Programming problems. 1.1 To find whether a given number is positive or not. 1.2 WAP to find the greatest of two numbers. 1.3. WAP to find the greatest of three numbers using nested if/else if statements only.	CLO3	4
8	Assignment on decision making statements-nested if	Week 8/ Turn 1 and 2	Solve the Programming problems. 1.1 Program for analysis of people of certain age groups who are eligible for getting a suitable job if their condition and norms get satisfied using nested if statement. 1.2 Program to find which number is greater among the considered number and then how the execution happens with the help of nested if statement if the flow gets successful then it is counted as normal flow.	CLO3	4
9	Assignment on decision making statements (switch case)	Week 9/ Turn 1 and 2	1.1 WAP to design a simple calculate using switch case statements. 1.2 WAP to print day of a week	CLO3	4

			using switch case statement		
10	Assignment on use of while loops	Week 10/ Turn 1 and 2	1.1 WAP to print counting 1 to 10 using while loop 1.2 WAP to print table of any number.	CLO4	4
11	Assignment on writing C programs in a modular way.	Week 11/ Turn 1 and 2	1.1 WAP to print the Fibonacci series up to 10 level. 1.2 WAP to find whether the given number is Armstrong or Not. 1.3 WAP to find whether the given number is Palindrome or Not.	CLO4	4
12	Looping related problems	Week 12/ Turn 1 and 2	Create the Programs 1.1 WAP to print the Fibonacci series up to 10 level. 1.2 WAP to find whether the given number is Armstrong or Not. 1.3 WAP to find whether the given number is Palindrome or Not. 1.4 WAP to find whether the given number is prime or not. 1.5 WAP to reverse the digits of a given number	CLO5	4
13	Assignment on Conditional operator, Special operators	Week 13/ Turn 1 and 2	1.1 Find the number is positive or negative using the conditional operator. 1.2 Make a comparison between them with the conditional operator. If the first number is greater than the second, perform a division operation otherwise multiplication operation.	CLO5	4
14	Assignment on Operator Precedence	Week 14/ Turn 1 and 2	1.1 program that prints the result of all the operators available in c (including pre/ post increment, bitwise and logical). 1.2 Write a program which will demonstrate all the operations done by using Operator Precedence.	CLO5	4
15	Evaluation of arithmetic expressions; Type conversion	Week 15/ Turn 1 and 2	1.2 Create a program to calculate the percentage of a user's score in relation to the maximum score in a game. 1.3 Use type conversion to make sure that the result of the following example is 1.5, and not just 1.	CLO5	4
Total					**60 hrs.**

Learning resources

Textbooks:

1. E Balagurusamy: Computing Fundamentals & C Programming – Tata McGraw-Hill
2. P. K. Sinha & Priti Sinha: Computer Fundamentals.
3. Kamthane: Programming with ANSI and TURBO C (Pearson Education)

Reference Books:

1. Henry Mullish & Hubert L.Cooper: The Spirit of C, Jaico
2. Ashok N Kamthane: Programming with ANS and Turbo C, Pearson
3. V. Rajaraman: Programming in C.

Online Resources/E-Learning Resources

1. https://onlinecourses.nptel.ac.in/noc20_cs913
2. https://www.programiz.com/c-programming

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: I**		**Level: UG**	
Course Name		**Data Communication and Networking**		**Course Code/ Course Type**		**UBS103/MAJM**	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
3	-	-	3	3	40	60	-
Prerequisite: Students should have basic Computer Knowledge							
Course Objectives (CO):				The objectives of Data Communication and Networking are: 1. To remember the networks, topologies, and the key concepts. 2. To understand about the layered communication architectures and its functionalities. 3. To understand the principles, key protocols, design issues in different protocols. 4. To apply the concepts of network services in network applications. 5. To analyze the significance of each layer in ISO and TCP/IP.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the different network models for networking links. 2. Discuss different transmission media and different switching networks. 3. Apply knowledge and classify medium access control protocols 4. Compare the different protocols in networking. 5. Determine application layer services and client server protocols working with the client server paradigms like WWW, HTTP etc.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction: Network Types,LAN,MAN,WAN,Network Topologies Reference models,The OSI Reference Model,The TCP/IP Reference Model,Comparison of the OSI and TCP/IP Reference Models,OSI Vs TCP/IP,Lack of OSI models success,Physical Layer, Introduction to Guided Media,Twisted-pair cable,Coaxial cable and Fiber optic cable and unguided media,Wireless-Radio waves, microwaves, infrared.	**CLO1**	**9**
UNIT II		
Data link layer: Design issues,Framing,fixed size framing,variable size framing,flow control,error control,error detection and correction codes,CRC,one's complement,services provided to Network Layer,Elementary Data Link Layer protocols,simplex protocol,Simplex stop and wait,Simplex protocol for Noisy Channel.Sliding window protocol,Selective Repeat Stop and wait protocol,Data link layer in HDLC,Configuration and transfer modes,frames, control field,point to point protocol(PPP),Framing transition phase,multiplexing,multi-link PPP.	**CLO2**	**9**
UNIT III		
Media Access Control: Random Access,ALOHA,Carrier sense multiple access (CSMA), CSMA with Collision Detection,CSMA with Collision Avoidance,Controlled Access Reservation,Polling,Token Passing,Channelization,Frequency Division Multiple Access	**CLO3**	**9**

(FDMA),Time division multiple access(TDMA),Code division multiple access (CDMA).		
UNIT IV		
The Network Layer Design Issues: Store and Forward Packet Switching Service,Provided to the Transport layer,Implementation of Connectionless Service,Implementation of Connection Oriented Service,Comparison of Virtual Circuit and Datagram Networks,Routing Algorithms,The Optimality principle shortest path, Flooding, Distance vector,Link state,Hierarchical Congestion Control algorithms.	**CLO4**	**9**
UNIT V		
The Transport Layer: Transport layer protocols, Introduction services port number, User datagram protocol,User datagram,UDP services,UDP applications,Transmission control protocol,TCP services features,Segment,A TCP connection,Windows in TCP, Flow Control,Error Control, Congestion control in TCP.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Computer Networks — Andrew S Tanenbaum, Fifth Edition. Pearson Education/PH
2. Data Communications and Networks – Behrouz A. Forouzan, Fifth Edition TMH.

Reference Books:

1. Data Communications and Networks- Achut S Godbole, Atul Kahate
2. Computer Networks, Mayank Dave, CENGAGE

Online Resources/E-Learning Resources

1. **https://www.tutorialsduniya.com/notes/computer-networks-notes/**
2. https://www.guru99.com/data-communication-computer-network

COURSE CURRICULUM

Name of the Program:	BSc (Cyber Security)	Semester: I	Level: UG
Course Name	Data Communication and Networking Lab.	Course Code/ Course Type	UBS104/MAJM
Course Pattern	2024	Version	1.0

Teaching Scheme					Assessment Scheme		
Theory	Practical	Tutorial	Total Credits	Hours	CIA (Continuous Internal Assessment)	ESA (End Semester Assessment)	Practical/Oral
-	2	-	2	4	25	-	25

Prerequisite: Basic Knowledge of Data Communication is required.

Course Objectives (CO):	The objectives of Data Communication and Networking Lab are: - 1. List out the basic network concepts. 2. To Classify the various types of topologies used in configuration of Network. 3. Make use of Network devices to install the LAN. 4. Examine performance of the network by using various commands. 5. Make use of Network Protocols to Transfer files, Configure Connectivity, Configure firewall.
Course Learning Outcomes (CLO):	Students would be able to: 1. Define the wired computer network topologies. 2. Explain the relevant network model for data communication. 3. Illustrate Error Correction and Error Detection Methods. 4. Analyze the performance of the given network. 5. Configure the network component and assign an IP address.

Course Contents/Syllabus: Practical Plan

Activity Number	Assignment/Practical/Activity Title	Week Number/Turn	Details	CLO	Hours
1	Introduction to Basic Network types and connection.	Week 1/ Turn 1 and 2	Type of network topology used in the lab and prepare technical specifications for it.	CLO1	4
2	Connecting Computers	Week 2/ Turn 1 and 2	Connect computers in bus topology and transfer the data.	CLO1	4
3	Network Topology	Week 3/ Turn 1 and 2	Connect computers in star topology and test the performance.	CLO1	4

4	Configure LAN	Week 4/ Turn 1 and 2	Install/configure/Test Peer to Peer LAN and sharing of resources.	CLO2	4
5	Point to Point Network	Week 5/ Turn 1 and 2	Configure Point to Point network in laboratory.	CLO2	4
6	Connect devices on the LAN	Week 6/ Turn 1 and 2	Prepare patch cord and cross connection cables,use to connect the devices on the LAN.	CLO2	4
7	Install LAN Network	Week 7/ Turn 1 and 2	Using a Hub/ Switch Install a LAN network consisting of 6 computers.	CLO3	4
8	Error Detection.	Week 8/ Turn 1 and 2	Locate the error bit in the given data stream by applying the different error detection methods.	CLO3	4
9	Error Correction Methods	Week 9/ Turn 1 and 2	Correct the error in a given data stream by applying the different error correction methods.	CLO3	4
10	Performance of Network	Week 10/ Turn 1 and 2	Use route command to test the performance of the given network.	CLO4	4
11	Install,Test Router	Week 11/ Turn 1 and 2	Install and test Router, Repeater and Bridge	CLO4	4
12	IP Address.	Week 12/ Turn 1 and 2	Assign IP address to the PC connected to the internet.	CLO5	4
13	Configure Connectivity.	Week 13/ Turn 1 and 2	Configure/Test Internet connectivity	CLO5	4
14	Transfer files.	Week 14/ Turn 1 and 2	Use FTP protocol to transfer file from one system to another system.	CLO5	4
15	Configure Firewall.	Week 15/ Turn 1 and 2	Install and configure a Firewall for the network security.	CLO5	4
Total					**60 hours**

Learning resources

Textbooks:

1. Data Communications and Networking By Behrouz A. Forouzan
2. Data Communications and Networking with TCP/IP Protocol Suite 6th Edition by Behrouz A. Forouzan

Reference Books:

1. Computer Networking by Kurose
2. Data Communications Networking by Behrouz A. Forouzan

Online Resources/E-Learning Resources

1. https://www.youtube.com/watch?reload=9&v=aHJElrgj6UA
2. https://www.youtube.com/watch?v=_VRToy-9SD0

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: I**		**Level: UG**	
Course Name		**Introduction to Cyber Security**		**Course Code/ Course Type**		UBS105/SEC	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	-	-	2	2	20	30	-
Prerequisite: Students should have basic knowledge of Networks.							
Course Objectives (CO):				The objectives of Introduction to Cyber Security are: 1. To remember network basics and familiarize on the security of network protocols. 2. To understand the field of digital security and concepts of access control mechanisms. 3. To apply keywords and jargons involved in securing browsers. 4. To examine the need of cyber-attacks and data privacy. 5. To analyze the significance of security methods in the cyber domain.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the digital security measures taken to protect device from threats 2. Explain the access control mechanism and understand how to protect servers. 3. Explain the importance of network basics and security of network protocols. 4. Analyze the cyber-attacks, learn data privacy issues and preventive measures. 5. Analyze the various attacks in the web interface.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Cyber security: Overview of Computer and Web-technology,Architecture of cyberspace,Communication and web technology,Internet,World wide web,Advent of internet,Internet infrastructure for data transfer and governance,Internet society,Regulation of Cyberspace,Concept of Cyber Security,Issues and challenges of cyber security.	**CLO1**	**6**
UNIT II		
Networking: Networking basics (home network and large-scale business networks), Networking protocols, Security of protocols, Sample application hosted on-premises.	**CLO2**	**6**
UNIT III		
Digital Security: Basics of Digital security, Protecting personal computers and devices, Protecting devices from Virus and Malware,Identity,Authentication and Authorization,Need for strong credentials,Keeping credentials secure, Protecting servers using physical and logical security,World Wide Web (www),The Internet and the HTTP protocol,Security of browser to web server interaction.	**CLO3**	**6**
UNIT IV		
Cyber Attacks: Introduction,Application security(design, development and testing),Operations	**CLO4**	**6**

Security,Monitoring,identifying threats and remediating them, Principles of data security,Confidentiality,Integrity and Availability,Data Privacy,Data breaches,Preventing attacks and breaches with security Controls,Compliance standards,Computer Ethics.		
UNIT V		
Cybercrime and Cyber law: Classification of cybercrimes,Common cyber crimes cybercrime targeting computers and mobiles,Cybercrime against women and children,financial frauds, social engineering attacks,malware and ransomware attacks,zero day and zero click attacks,Cybercriminals modus operandi,Reporting of cybercrimes,Remedial and mitigation measures,Legal perspective of cybercrime,IT Act 2000 and its amendments,Cybercrime and offenses,Organizations dealing with Cybercrime and Cyber security in India,Case studies.	**CLO5**	**6**
Total hours		**30**

Learning resources

Textbooks:

1. Cybersecurity For Dummies by Joseph Steinberg
2. Big Breaches: Cybersecurity Lessons for Everyone by Neil Daswani, Moudy Elbayadi

Reference Books:

1. Cybersecurity: The Beginner's Guide by Dr. Erdal Ozkaya
2. Confident Cybersecurity: How to Get Started in Cybersecurity and Futureproof Your Career by Dr. Jessica Barker

Online Resources/E-Learning Resources

1. The Complete Cyber Security Course: Hackers Exposed --- https://www.udemy.com/course
2. Foundations of Cybersecurity----- https://www.coursera.org/

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: I**		**Level: UG**	
Course Name		**Basic Mathematics**		**Course Code/ Course Type**		UBS106/BSC	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	3	40	60	-
Prerequisite: Basic Concepts of Mathematics.							
Course Objectives (CO):				The objectives of Basic Mathematics are: 1. To memorize the Matrices and its operations. 2. Classify the trigonometric functions. 3. To execute various operations on analytical geometry. 4. To compare the various forms of differential calculus. 5. To evaluate the different forms of calculus.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the matrices and the operations associated with it. 2. Explain the various trigonometric functions. 3. Apply knowledge of geometry to various real-life situations. 4. Examine the differential calculus with respect to different forms. 5. Execute gamma functions and its properties.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Matrices: Matrices,Types of matrices,Elementary properties of matrices, inverse matrices,Rank of a matrix,Symmetric,Skew symmetric and Orthogonal matrices,System of linear equations,Gauss elimination method and Gauss Jordan method.	**CLO 1**	**9**
UNIT II		
Trigonometry: Introduction, Trigonometric ratios, Transformations, Identities, Inverse trigonometric functions (only elementary topics)	**CLO 2**	**9**
UNIT III		
Analytical Geometry: Scalar product,vector product,angle between two vectors,shortest distance between two lines,conditions for two lines to intersect,point of intersection,collinearity of three points(self- study topics),Direction ratios,direction cosines of a line passing through two points,equation of a line in space,angle between two lines, shortest distance between two lines, plane, equation of a plane in normal form.	**CLO3**	**9**
UNIT IV		
Differential Calculus: Limit continuity,Differentiability, Roll's Theorem, Mean value theorems (Cauchy's and Lagrange's),Power series expansions of functions in Taylor's and Maclaurin's forms,indeterminate forms and L'Hospital's rule.	**CLO4**	**9**
UNIT V		

Integral Calculus: Integral as limit of sum,Fundamental theorem of calculus, indefinite integrals,Methods of Integration,Substitution method, Integration by parts and by partial fraction technique,Beta Gamma functions and their properties.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Hugh Neill, Trigonometry: A complete Introduction, John Murray Learning, 2018.
2. George B. Thomas and Ross L. Finney, Calculus and Analytical Geometry, Addison- Wesley, 9th Edn, 1998.

Reference Books:

1. Erwin Krayzie, Advanced Engineering Mathematics, John Wiley and sons, Inc.10th Edition.
2. B.S. Grewal, Higher Engineering Mathematics, Khanna Publishers, 44th Edition, 2010.

Online Resources/E-Learning Resources

1. https://bs-ug.iisc.ac.in/UG-Math.pdf
2. https://mathinova.com/

COURSE CURRICULUM

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc (Cyber Security)</b></td><td colspan="2"><b>Semester: I</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Fundamentals of Computer Architecture</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2">UBS107/SEC</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hrs.</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/Oral</b></td></tr>
<tr><td>3</td><td>-</td><td>-</td><td>3</td><td>3</td><td>40</td><td>60</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite: Students should have basic Computer Knowledge</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Fundamentals of Computer Architecture are:
1. To remember the Fundamental structure of Computers
2. To understand the various types of Instructions for performing operations.
3. Illustrate the standard input output Interfaces, buses and their types.
4. Highlight the need for different types of Memory systems and their functions.
5. Discuss the processing units and their roles.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Identify the structure of a computer system.
2. Explain various addressing modes and the role of Input output operations.
3. Illustrate the Input Output Interfaces and their role for memory access.
4. Examine the different memory systems and their functions.
5. Elaborate the role of processing units for performing arithmetic or any other logical operation.</td></tr>
</table>

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Basic Structure of Computers: Functional unit,Basic Operational Concepts,Bus structures,System Software,Performance,The history of computer development, Machine Instruction and Programs,Instruction and Instruction Sequencing,Register Transfer Notation,Assembly Language Notation,Basic Instruction Types.	**CLO1**	**9**
UNIT II		
Addressing Modes: Basic Input/output Operations,The role of Stacks and Queues in computer programming equations,Component of Instructions,Logic Instructions,Shift and Rotate Instructions,Type of Instructions,Arithmetic and Logic Instructions, Branch Instructions,Addressing Modes,Input/output Operations.	**CLO2**	**9**
UNIT III		
Input Output Organization: Accessing I/O Devices,Interrupts,Interrupt Hardware,Enabling and Disabling Interrupts,Handling Multiple Devices,Direct Memory Access,Buses,Synchronous Bus,Asynchronous Bus,Interface Circuits, Standard I/O Interface.	**CLO3**	**9**
UNIT IV		

Memory Systems: Basic memory circuits,Memory System Consideration,ReadOnly Memory,ROM,PROM,EPROM,EEPROM,Flash Memory, Cache Memories,Mapping Functions,Magnetic Hard Disks,Optical Disks.	**CLO4**	**9**
UNIT V		
Processing Unit: Fundamental Concepts,Register Transfers,Performing an Arithmetic Or Logic Operation,Fetching a Word From Memory,Micro programmed Control, Microinstructions, Microprogram Sequencing.	**CLO5**	**9**
Total hours		**45**

Learning resources

Textbooks:

1. Computer Organization, Carl Hamacher, Zvonks Vranesic, Safea Zaky, 5th Edition,McGraw Hill, 2011.
2. Computer Architecture and Organization, John P. Hayes, 3rd Edition, McGraw Hill,2002.

Reference Books:

1. Computer Architecture: Fundamentals and Principles of Computer Design, 2nd Edition, by Joseph D. Dumas
2. Essentials of Computer Organization and Architecture, 5 th Edition, by Linda Null.

Online Learning/E-learning Resources

1. http://www.cs.iit.edu/~virgil/cs470/Book/
2. https://www.cse.iitd.ac.in/~srsarangi/archbook/chapters/intro.pdf

COURSE CURRICULUM

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc(CS)</b></td><td colspan="2"><b>Semester: I</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Applied Communication</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2">UEG101/AEC</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hours</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/Oral</b></td></tr>
<tr><td>2</td><td>-</td><td>-</td><td>-</td><td>2</td><td>50</td><td>-</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite:</b> Anyone can take this course with basic knowledge of English communication.</td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Applied Communication are:
1. To Comprehend the basic English communication components.
2. To Identify the Factors influencing interpersonal communication.
3. To Apply the knowledge of written communication.
4. To Demonstrate English communication in public speaking and presentation.
5. To develop students' understanding of digital communication tools, media literacy skills, and ethical considerations in online communication.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Define communication and explain its significance in personal, professional, and societal contexts.
2. Apply interpersonal communication skills in various contexts, such as social interactions, group discussions, teamwork, leadership, and professional settings.
3. Understand the fundamental principles of effective writing, including clarity, coherence, conciseness, and correctness.
4. Reflect on their presentation experiences, seek feedback from peers.
5. Use digital tools for collaboration, communication, and productivity, including project management platforms.</td></tr>
</table>

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction to Communication: Definition and models of communication, Importance of effective communication in personal and professional contexts, Basic elements of communication: sender, receiver, message, channel, feedback, Communication barriers and strategies for overcoming them, Verbal and nonverbal communication skills.	**CLO 1**	**6**
UNIT II		
Interpersonal Communication: Understanding interpersonal relationships, Factors influencing interpersonal communication: culture, gender, perception, and self-concept, Effective listening skills and techniques, Assertiveness and conflict resolution strategies, Building and maintaining healthy, relationships	**CLO 2**	**6**
UNIT III		

Written Communication: Principles of effective writing,clarity, coherence,conciseness and correctness,Types of written communication, emails, memos,letters,reports and resumes,Planning and organizing written documents,Grammar, punctuation and style conventions, Proofreading and editing techniques	**CLO3**	**6**
UNIT IV		
Public Speaking and Presentation Skills: Understanding the importance of public speaking,Preparing and organizing a presentation,topic selection, audience analysis and speech outline,Delivery techniques,voice modulation, body language, and eye contact,Overcoming stage fright and anxiety,Handling questions and feedback from the audience	**CLO4**	**6**
UNIT V		
Digital Communication and Media Literacy: Overview of digital communication tools,email,social media,instant messaging and video conferencing,Netiquette and online professionalism, Understanding media messages and sources	**CLO5**	**6**
Total Hours		**30 Hours**

Learning resources

Textbooks:

1. **Communication in Everyday Life: A Social Interpretation" by Steve Duck and David T. McMahan**
2.
3. Applied Communication in the 21st Century" by Carole L. Huston and Ronald B. Adler

Reference Books:

1. The SAGE Handbook of Communication and Instruction" edited by Deanna L. Fassett and John T. Warren
2. Communication: Principles for a Lifetime" by Steven A. Beebe, Susan J. Beebe, and Diana K. Ivy

Online Resources/E-Learning Resources

1. https://www.udemy.com/topic/communication-skills/free/
2. https://www.uou.ac.in/sites/default/files/slm/BHMAECC-II.pd

COURSE CURRICULUM

Name of the Program:		**BSC(CS)**		**Semester:I**		**Level: UG**	
Course Name		**UHVI:Professional Ethics**		**Course Code/ Course Type**		**ACUHV101/AC**	
Course Pattern		**2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	**-**	**-**	**-**	**2**	**50**	**-**	**-**
Pre-Requisite: UHV-I							
Course Objectives (CO):				The objectives of Universal Human Value- Professional Ethics are: 1. To make the students understand the importance of ethical behaviour. 2. To expose the students to the ethical practices to be followed in profession 3. To sensitize the students to become responsible persons who will uphold ethics in profession when they pursue their career 4. To make students understand Psychological and Philosophical approaches 5. To make students understand social responsibility and corporate Sustainability			
Course Learning Outcomes (CLO):				Students would be able to: 1. Equip themselves with an understanding of moral, professional and personal values. 2. Understand the need of ethics in shaping their profession The learners will hone their decision-making skills. 3. Refine their business ethics based on psychological and philosophical perspective. 4. Assess the need for a balance between ecology, and economy. 5. Equip themselves with a better understanding of themselves and the society they live in and the responsibilities they shoulder in creating a sustainable world.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Individual and Professional Ethics: Introduction to Professional Ethics, Morals, Values and Ethics – Personal and Professional- Sensé of Professional Ethics – Code of Ethics by NSPE-Making decisions with ethical dimensions–definition–roadmap to ethical decision making–common standards– internal obstacles – bias – empathy	**CLO 1**	**6**
UNIT II		
Business Ethics: Philosophical approaches to Business Ethics – ethical reasoning – ethical issues in business - Social Responsibility of Business- conflict of interest–cultural relativism-Ethical Leadership-Resisting un-ethical authority and domination-Global Business Ethics	**CLO 2**	**6**
UNIT III		
Psychological Approaches: Ethical Theories-Psychological and Philosophical Approaches-Myths about Morality-conflict of interest in psychological perspective - Courage-Integrity – ethical dilemma – Emotional Intelligence (Mahabharata- Iskcon Publications)	**CLO 3**	**6**
UNIT IV		
Workplace Ethics: Ethics in changing domains of Research, academic integrity, intellectual honesty-Role of Engineers and Managers, Ethical issues in Diverse workplace, competition,free will-Confidentiality,employee rights – Intellectual property rights – discrimination	**CLO 4**	**6**
UNIT V		
Safety, Responsibilities and Rights: Ecology, and Economy-Risk benefit analysis and reducing risk SDGs–Corporate social responsibility and Corporate Sustainability - CSR in India - Sustainability Case Studies	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. Subramanian. R. Professional Ethics, Oxford Publication,2013.

2. Nagarasan. R. S. Professional Ethics and Human Values. New Age International Publications,

2006.

Reference Book:

Mike W Martin and Roland Schinzinger, Ethics in Engineering,4th edition, Tata McGraw Hill Publishing Company Pvt Ltd, New Delhi,2014

Online Resources/E-Learning Resources

1. https://www.nspe.org/resources/ethics/code-ethics
2. https://www.toolshero.com/tag/ethical-decision-making/
3. https://pagecentertraining.psu.edu/public-relations-ethics/introduction-to-public-relations-ethics/lesson-1/ethical-theories/
4. https://peer.asee.org/case-studies-in-engineering-ethics.pdf

CIA Guidelines

Online Quiz (Based on MCQ)- 20 marks

Activity (with short Report Submission) - 20 Marks

Academic Sincerity - 10 marks

Few of the suggested activities are Assignments, Debates, Poster presentations, Model making, Group presentation, Field visits and Group Discussions.

Few of suggested topics related to UHV1- Professional Ethics are:

Debate Topics

- Ethical Approach versus Realistic Approach
- Individual and Social Approach
- Dilemma between heart and Mind

Activity

- Analyze the wastage (Electricity or any other) at work place? How you managed.

Assignment

- Analyze the code of ethics at work place.
- If you fulfil the duties, rights will automatically fall in place. Justify the statement

References:

1. https://uhv.org.in/
2. https://vvce.ac.in/wp-content/uploads/2021/04/Realising-Aspirations-of-NEP2020-UHV.pdf

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester: I**		**Level: UG**	
Course Name		**Concepts and Application in Science**		**Course Code/ Course Type**		ACIKSSS101	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	50	-	-
Prerequisite: Basic knowledge of science.							
Course Objectives (CO):				The objectives of Concepts and Application in Science are: 1. To remember Indian Knowledge Systems: Origin, Evolution and Ontological Approach 2. To understand Indian Knowledge Approaches. 3. To apply Sciences of Life and Mind. 4. To examine Indian Knowledge System Torchbearers – Ancient and Modern 5. To analyse Self-Knowledge for Personal Effectiveness.			
Course Learning Outcomes (CLO):				Students would be to: 1. Identify and appreciate the rich heritage that resides in our traditions. 2. Explain the mind/voice dynamic in Indian knowledge systems. 3. Explain the practices that will prepare one for the inner-journey to discover the Self. 4. Analyse the need and importance of Sanskrit in getting to the roots of the philosophical concepts. 5. Analyse the various functions in Indian knowledge systems.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Indian Knowledge System and Vedic Corpus: Introduction to IKS, Need for IKS, Historicity of IKS,Salient aspects of IKS,IKS in ancient India and in modern India. Introduction to Vedas, Four Vedas, Sub-classification of Vedas, Messages in Vedas, Basics of Nirukta and Chandas.	**CLO1**	**6**
UNIT II		
Wisdom through the Ages: Puranas, Ithihasas, Nitishastras, Subhasitas,Linguistics, Components of a language,Paṇini's work on Sanskrit grammar,Phonetics in Sanskrit, Role of Sanskrit in natural language processing,Framework for establishing valid knowledge.	**CLO2**	**6**
UNIT III		
Number Systems and Units of Measurement: Salient features of the Indian numeral system, Importance of decimal representation, The discovery of zero and its importance, Unique approaches to represent numbers, Unique aspects of Indian Mathematics, Great mathematicians and their significant contributions in the area of arithmetic, algebra, geometry, trigonometry, combinatorial problems in Chandaḥ-sastra of Pingala	**CLO3**	**6**
UNIT IV		
Knowledge Framework and classifications: Indian scheme of knowledge, The knowledge triangle, Prameya,A vaiśeṣikan approach to physical reality, Dravyas, The constituents of the physical reality	**CLO4**	**6**

UNIT V		
Science and Technology in the Vedic Age and Post-Vedic Records. **Knowledge:** Framework and Classification, Astronomy Encryption Method used in ancient India, Introduction to Yantra Shastra,Vaimanik Shashtra, Agriculture Technologies	**CLO5**	**6**
Total hours		**30**

Activity 1: Comparative Analysis of Traditional and Modern Scientific Methods

Activity 2: Presentation on Indian scientific texts such as the Phonetics in Sanskrit, Astronomy Encryption Method used in ancient India

Learning resources

Textbooks:

1. Health Science: Concepts and Applications, Authors: Jacquelyn Rhine Marshall and Sue C. Roe

2. Introduction to Indian Knowledge Systems: Concepts and Applications by Prof. B Mahadevan

Reference Books: -

1. Introduction to Indian Knowledge System: Concepts and Applications by Pallavi Ghosh

Online Resources/E-Learning Resources

1. https://onlinecourses.swayam2.ac.in/

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester: I**		**Level: UG**	
Course Name		**Introduction to IoT**		**Course Code/ Course Type**		UBS108A/OE	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	20	30	-
Prerequisite: Basic Knowledge of Computer Networks.							
Course Objectives (CO):				The objectives of Introduction to IoT are: 1. To remember the fundamental concepts of IoT. 2. To understand the role of sensors in IoT. 3. To apply different protocols used for IoT design. 4. To be familiar with data handling and analytics tools in IoT. 5. To analyse the role of IoT in various domains of Industry.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Understand various concepts, terminologies and architecture of IoT systems 2. Explain the Use sensors and actuators for design of IoT. 3. Apply various protocols for design of IoT systems. 4. Analyse the various techniques of data storage and analytics in IoT. 5. Discuss the APIs to connect IoT related technologies.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Fundamentals of IoT: Introduction,Definitions & Characteristics of IoT,IoT Architectures, Physical & Logical Design of IoT,Enabling Technologies in IoT,History of IoT,About Things in IoT,The Identifiers in IoT,About the Internet in IoT,IoT frameworks,IoT and M2M.	**CLO1**	**6**
UNIT II		
Sensors Networks: Definition, Types of Sensors, Types of Actuators, Examples and Working of IoT, Development Boards, Arduino IDE and Board Types.	**CLO2**	**6**
UNIT III		
Raspberry Pi: Development Kit, RFID Principles and components, Wireless Sensor Networks: History and Context, The node, Connecting nodes, Networking Nodes, WSN and IoT.	**CLO3**	**6**
UNIT IV s		
Wireless Technologies for IoT: WPAN Technologies for IoT,IEEE 802.15.4, ZigBee, HART, NFC,Z-Wave,BLE,Bacnet,Modbus,IP Based Protocols for IoT IPv6,6LowPAN,RPL,REST, AMQP,CoAP, MQTT,Edge connectivity and protocols	**CLO4**	**6**
UNIT V		
Applications of IoT: Home Automation, Smart Cities, Energy, Retail Management, Logistics, Agriculture, Health and Lifestyle, Industrial IoT, Legal challenges, IoT design Ethics, IoT in Environmental Protection.	**CLO5**	**6**
Total		**30 hrs.**

Learning resources

Textbooks:

1. "The Internet of Things" by Samuel Greengard.
2. "Getting started with Internet of Things" by Cuno Pfister

Reference Books:

1. Daniel Minoli, — "Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications", ISBN: 978-1-118-47347-4, Willy Publications
2. Pethuru Raj and Anupama C. Raman, "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", CRC Press

Online Resources/E-Learning Resources

1. https://onlinecourses.nptel.ac.in/noc17_cs22/course
2. http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html

COURSE CURRICULUM

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc (Cyber Security)</b></td><td colspan="2"><b>Semester: I</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Introduction to Digital Electronics</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2">UBS108B/OE</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hrs.</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/ Oral</b></td></tr>
<tr><td>2</td><td>-</td><td>-</td><td>2</td><td>2</td><td>20</td><td>30</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite: Basic Knowledge of Number system.</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Introduction to Digital Electronics are:
1. To understand the number systems, Binary codes and Complements.
2. To understand the Boolean algebra and simplification of Boolean expressions.
3. To analyze logic processes and implement logical operations using combinational logic circuits.
4. To analyze sequential systems in terms of state machines.
5. To understand characteristics of memory and their classification.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Identify the various concepts, terminologies of Number system and Codes.
2. Analyze, design and implement combinational logic circuits.
3. Classify different semiconductor memories.
4. Analyze, design and implement sequential logic circuits.
5. Simulate and implement combinational and sequential logic circuits.</td></tr>
</table>

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Number System and Codes: Decimal, Binary, Hexadecimal,Octal,Codes,BCD, Gray and Excess 3 codes, code conversions,Complements (1's, 2's,9's and 10's),Addition - Subtraction using complement methods.	**CLO1**	**6**
UNIT II		
Boolean Algebra and Theorems: Boolean Theorems,De-Morgan's laws,Digital logic gates,Multi-level NAND & NOR gates,Standard representation of logic functions (SOP and POS),Minimization Techniques(Karnaugh Map Method)	**CLO2**	**6**
UNIT III		
Combinational Digital Circuits: Address Half & full adder,Subtractor Half and full subtractors,Parallel binary adder,Magnitude Comparator,Multiplexers(4:1))and Demultiplexers (1:4)	**CLO3**	**6**
UNIT IV		

Sequential Digital Circuits: Flip Flops,SR,FF,JK,FF,T and D type,FFs,Master-Slave FFs,Excitation tables,Registers,Serial in Serial Out,Parallel In and Parallel Out, Counters Asynchronous,Mod-8,Mod-10	**CLO4**	**6**
UNIT V		
Memory Devices: General Memory Operations,ROM,RAM (Static and Dynamic), PROM, EPROM, EEPROM, EAROM.	**CLO5**	**6**
Total hours		**30**

Learning resources

Textbooks:

1. "Herbert Taub and Donald Schilling. "Digital Integrated Electronics" . McGraw Hill.
2. S.K. Bose. "Digital Systems". 2/e. New Age International.

Reference Books:

1. D.K. Anvekar and B.S. Sonade. "Electronic Data Converters : Fundamentals & Applications". TMH.
2. Malvino and Leach. " Digital Principles and Applications". TMG Hill Edition.

Online Resources/E-Learning Resources

1. https://www.agner.org/digital/digital_electronics_agner_fog.pdf
2. 01Title.fm (clarkson.edu)

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester - II

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: II**		**Level: UG**	
Course Name		**Programming using Advanced C**		**Course Code/ Course Type**		UBS109/MAJM	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
3	-	-	3	3	40	60	-
Prerequisite: Students should have basic C Programming.							
Course Objectives (CO):				The objectives of Programming using Advanced C are: 1. To remember the knowledge about Functions and its types. 2. To understand and trace the execution of pointers in C language. 3. To apply preprocessor operations using programs in C language. 4. To analyze the concepts and techniques associated with structures in C Programming language. 5. To Design and create file handling operations.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the basic concepts of functions. 2. Explain the reason why pointers are available in C language. 3. Apply knowledge of preprocessor directives to create Code for a given problem. 4. Analyze the use of structures. 5. Evaluate the various file handling operations.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
User-Defined Functions: User-Defined Functions,Need and Elements of User-Defined Functions,Return Values and their types,Function Calls,Category of Functions,Nesting of Functions,Recursion,Passing Arrays and Strings to Functions,The Scope,Visibility and Lifetime of Variables.	**CLO1**	**9**
UNIT II		
Pointers & File Management: Introduction,Understanding pointers,Accessing the address of a variable,Declaration and Initialization of pointer Variable, Accessing a variable through its pointer Chain of pointers,Pointer Expressions,Pointer Increments and Scale factor,Pointers and Arrays,Pointers and Strings.	**CLO2**	**9**
UNIT III		
Preprocessor: Concept, Format of preprocessor directives, File inclusion directives (#include), Macro substitution directives (#define), nested macros, parameterized macros, Macros versus functions, #error / #pragma #directives,Conditional compilation (#if/#ifdef/#else/#elif/#endif), Predefined macros (_DATE_ / _TIME_ /_FILE_ /_LINE_/ _STDC_)	**CLO3**	**9**
UNIT IV		
Structures: Concept, Declaration,Definition,initialization,Accessing structure members(.Operator),Array of structures,Pointers to structures,Declaring pointer to structure,Accessing	**CLO4**	**9**

structure members via pointer to structure,Structures & functions,Passing each member of structure as a separate argument, Passing structure by value/address,Nested structures,typedef & structures		
UNIT V		
File Handling: Concept of streams, need, Types of files, Operations on text & binary files, Random access file, library functions for file handling,fopen,fclose, fgetc,fseek,fgets, fputc etc.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. E Balagurusamy: Computing Fundamentals & C Programming – Tata McGraw-Hill
2. P. K. Sinha & Priti Sinha: Computer Fundamentals.
3. Kamthane: Programming with ANSI and TURBO C (Pearson Education)

Reference Books:

1. Henry Mullish & Hubert L.Cooper: The Sprit of C, Jaico
2. Ashok N Kamthane: Programming with ANS Iand Turbo C, Pearson
3. V. Rajaraman: Programming in C.

Online Resources/E-Learning Resources

1.https://onlinecourses.nptel.ac.in/noc20_cs91/
2.https://www.gnu.org/software/gnu-c-manual/gnu-c-manual.pdf

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: II**		**Level: UG**	
Course Name		**Programming using Advanced C**		**Course Code/ Course Type**		UBS110/MAJM	
Course Pattern		**Revised2024**		**Version**		1.0	
Teaching Scheme				**Assessment Scheme**			
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
-	2	-	2	4	25	-	25
Prerequisite: Basic Knowledge of C Programming is required.							
Course Objectives (CO):				The objectives of Programming using Advanced C 1. Define the fundamentals of programming in C Language. 2. Illustrate the use of Functions, recursion and Arrays. 3. Classify the different operations on Strings,Arrays. 4. Analyze the use of Pointers in various scenarios. 5. Evaluate the significance of Structures and File Handling.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define the implementation of programs in C language. 2. Explain the different types of programs based on functions, recursion and arrays. 3. Apply knowledge of Arrays, Strings for data manipulation. 4. Analyze the concept of pointers for implementing programs. 5. Design the use of structures for displaying elements.			

Activity Number	Assignment/Practical/ Activity Title	Week Number/Turn	Details	CLO	Hours
1	Familiarization with the C Programming Environment.	Week 1/ Turn 1 and 2	1. Finding maximum and minimum of a given set of numbers. 2. Finding roots of quadratic equation.	CLO1	4
2	Assignment on Functions	Week 2/ Turn 1 and 2	1. Check Prime or Armstrong Number Using User-defined Function. 2. Factorial of a Number Using Recursion	CLO1	4
3	Programs Based on Function Call by value,	Week 3/ Turn 1 and 2	1. Swapping numbers using Function Call by Value.	CLO1, CLO2	4
4	Recursion	Week 4/ Turn 1 and 2	1. Recursion: factorial, Fibonacci, GCD	CLO1, CLO2	4
5	Arrays	Week 5/ Turn 1 and 2	1. Calculate Average 2. Access elements out of its bound	CLO2	4
6	Arrays	Week 6/ Turn 1 and 2	1. Matrix addition and multiplication using arrays	CLO2, CLO3	4
7	Strings	Week 7/ Turn 1 and 2	1. Functions for string manipulations	CLO3	4
8	Structures and unions	Week 8/ Turn 1 and 2	1. Programs on structures and unions.	CLO3	4
9	Preprocessor directives	Week 9/ Turn 1 and 2	1. Using #define preprocessor 2. Using #if, #elif and #else Directive	CLO3	4
10	Pointers	Week 10/ Turn 1 and 2	1. Swapping two variables 2. Compare strings using pointer 3. Find largest element in array	CLO4	4
11	Pointers	Week 11/ Turn 1 and 2	1. Program to swap two numbers using pointers. 2. Program to change the value of constant integer using pointers.	CLO4, CLO5	4
12	Structures	Week 12/	1. Create structure & display	CLO5	4

		Turn 1 and 2	elements. 2. Program to Add Two Distances (in inch-feet system) using Structures.		
13	Structures	Week 13/ Turn 1 and 2	1. Menu driven program for employee structure. 2. Program to Store Information of a Student Using Structure.	CLO5	4
14	File Handling	Week 14/ Turn 1 and 2	1. Reading and writing to a text file. 2. size of data to be written in the disk	CLO5	4
15	File Handling(Getting data using fseek())	Week 15/ Turn 1 and 2	1. Move the file pointer to different locations inside a file.	CLO5	4
Total					**60 hrs.**

Course Contents/Syllabus: Practical Plan

Learning resources

Textbooks:

1. E Balagurusamy: Computing Fundamentals & C Programming – Tata McGraw-Hill
2. P. K. Sinha & Priti Sinha: Computer Fundamentals.
3. Kamthane: Programming with ANSI and TURBO C (Pearson Education)

Reference Books:

1. Henry Mullish & Hubert L.Cooper: The Sprit of C, Jaico
2. Ashok N Kamthane: Programming with ANS Iand Turbo C, Pearson
3. V. Rajaraman: Programming in C.

COURSE CURRICULUM

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc (Cyber Security)</b></td><td colspan="2"><b>Semester: II</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Unix & Shell Programming</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2">UBS111/MAJM</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hrs.</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/ Oral</b></td></tr>
<tr><td>3</td><td>-</td><td>-</td><td>3</td><td>3</td><td>40</td><td>60</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite: Basic Computer Knowledge is required.</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Unix & Shell Programming are:
1. Define the basic Concepts of Linux and its utilities.
2. To identify the various commands associated with Linux Shell.
3. To execute the various operations in the unix file system and grep.
4. To relate between different types of processes.
5. Evaluate the communication mechanism used in the Inter process.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Identify the Linux commands that are used to manipulate system operations.
2. Explain the various commands to be performed on Linux Shell.
3. To make use of application to manipulate the internal kernel File System.
4. Examine the various processes for synchronization.
5. Classify the different Inter process communication.</td></tr>
</table>

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Linux and Linux Utilities: History of LINUX, Architecture of LINUX, Features of LINUX, Introduction to vi editor,Linux commands-PATH, man, echo, printf, script, passwd, uname, who, date, stty, pwd, cd, mkdir, rmdir, ls, cp, mv, rm, cat, more, wc, lp, od, tar, gzip, file handling utilities, security by file permissions, process utilities, disk utilities.	**CLO1**	**9**
UNIT II		
Introduction to Shells: Linux Session, Standard Streams, Redirection, Pipes,TeeCommand,CommandExecution,CommandLine,Editing,Quotes,Command,Substitution,JobControl,Aliases,Variables,Predefined Variables, Options, Shell/Environment Customization, Filters and Pipes, Concatenating files, Display Beginning and End of files.	**CLO2**	**9**
UNIT III		
Grep: Operation, grep Family, Searching for File Content,Sed:Scripts, Operation, Addresses, commands,Applications, grep and sed,UNIX FILE STRUCTURE, Introduction to UNIX file system, inode (Index Node), file descriptors, system calls and device drivers.	**CLO3**	**9**
UNIT IV		
Process And Signals: Process identifiers,Process structure,Process table, Viewing processes, system processes, process scheduling, starting new processes,waiting for a process, zombie processes, orphan process, fork,vfork,exit, wait, waitpid, exec, signals functions.	**CLO4**	**9**
UNIT V		
Inter Process Communication: Pipe,Process pipes,The pipe call, Parent and child Processes,named pipes,fifos,semaphores,semget,semop, semctl,message queues,msgget,msgsnd,msgrcv,msgctl,sharedmemory,shmget, shmat,shmdt,shmctl, ipc status commands.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Linux System Programming, Robert Love, O’Reilly, SPD.
2. Advanced Programming in the UNIX environment, 2nd Edition, W.R. Stevens, Pearson Education.

Reference Books:

1. UNIX Network Programming, W.R. Stevens, PHI.
2. UNIX for Programmers and Users, 3rd Edition, Graham Glass, King Ables, Pearson Education

Online Resources/E-Learning Resources

1. https://www.udemy.com/course/bash-scripting
2. https://onlinecourses.swayam2.ac.in/

Name of the Program:		**BSc (Cyber Security)**		**Semester:II**		**Level: UG**	
Course Name		**Unix and Shell Programming Lab**		**Course Code/ Course Type**		UBS112/MAJM	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
-	2	-	2	4	25	-	25
Prerequisite: Basic Knowledge of C Programming is required.							
Course Objectives (CO):				The objectives of Programming using Unix and Shell Programming. 1. Define the fundamentals of Unix Shell Commands. 2. Illustrate the commands based on I/O redirection. 3. Classify the basic operations on Shell Programming. 4. Analyze the use of Shell Script with various cases. 5. Evaluate the significance of Shell Script.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define the implementation of Unix Commands. 2. Explain the different types of commands related to I/O operations and Shell Programming. 3. Apply knowledge of Shell Script for performing varied tasks. 4. Analyze the use of variables in scripts. 5. Develop scenarios for creating programs based on Shell Scripts.			

<u>COURSE CURRICULUM</u>

Course Contents/Syllabus:

Activity Number	Assignment/Practical/Activity Title	Week Number/Turn	Details	CLO	Hours
1	Use of basic Unix Shell Commands	Week 1/ Turn 1 and 2	Unix Shell Commands ls, mkdir, rmdir, cd, cat, banner, touch,file, wc, sort	CLO1	4
2	Use of basic Unix Shell Commands	Week 2/ Turn 1 and 2	cut, grep, dd, dfspace, du, ulimit. Commands related to inode	CLO1	4
3	Commands related to I/O redirection	Week 3/ Turn 1 and 2	I/O redirection, piping, process control commands,	CLO1, CLO2	4
4	Shell Programming	Week 4/ Turn 1 and 2	Interactive shell script Positional parameters Arithmetic	CLO1, CLO2	4

5	Shell Programming	Week 5/ Turn 1 and 2	If-then-fi, if-then-else, if nested if-else Logical operators	CLO2	4
6	Shell Programming	Week 6/ Turn 1 and 2	Else + if equals elif, case structure While,for loop Meta characters	CLO2, CLO3	4
7	Shell script	Week 7/ Turn 1 and 2	Create a file in $USER /class/batch directory. Input a page profile to yourself, copy it into other existing file. Start printing file at certain line Print all the difference between two file, copy the two files at $USER/CSC/2007 directory Print lines matching certain word patterns.	CLO3	4
8	Shell script	Week 8/Turn 1 and 2	Showing the count of users logged in. Printing Column list of files in your home directory. Listing your job with below normal priority. Continue running your job after logging out.	CLO3	4
9	Shell script	Week 9/ Turn 1 and 2	Shell script to change date format. Show the time taken in execution of this script	CLO3	4
10	Shell Script	Week 10/ Turn 1 and 2	Print file names in directory showing date of creation & serial no. of file.	CLO4	4
11	Shell Script	Week 11/ Turn 1 and 2	To count lines, words & characters in its input.(do not use wc)	CLO4, CLO5	4
12	Shell Script	Week 12/ Turn 1 and 2	To print end of a Glossary file in reverse order using array	CLO5	4
13	Shell Script	Week 13/ Turn 1 and 2	To check whether Ram logged in, continue checking further after every 30 seconds till success.	CLO5	4
14	Shell Script	Week 14/ Turn 1 and 2	To compute GCD & LCM of two numbers.	CLO5	4
15	Shell Script	Week 15/ Turn 1 and 2	To find whether a given number is prime	CLO5	4
Total					**60 hrs.**

Learning resources

Textbooks:

1. The Linux Programming Interface: A Linux and UNIX System Programming by Michael Kerrisk
2. The Linux Command Line: A Complete Introduction by William Shots

Reference Books:

1. Linux Bible by Christopher Negus (Author) and Christine Bresnahan (contributor)
2. Linux for Beginners: An Introduction to the Linux Operating System and Command Line by Jason Cannon

Name of the Program:		**BSc (Cyber Security)**		**Semester: II**		**Level: UG**	
Course Name		**E-Commerce & E-Governance**		**Course Code/ Course Type**		UBS113/SEC	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	-	-	2	2	20	30	-
Prerequisite: Basic Knowledge of Commerce and digital governance.							
Course Objectives (CO):				The objectives of E-Commerce & E-Governance are: 1. To recall the various concepts of e-commerce. 2. To recognize the technology associated with e-commerce. 3. To apply the basics of designing a secure web page. 4. To analyze the various types of Interactions in e-governance. 5. To assess the Models of Digital Governance.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the concepts associated with e-commerce. 2. Explain the technologies for designing e-commerce systems. 3. Apply the knowledge of HTML in designing secured web sites. 4. Analyze the various advantages and disadvantages of e-governance. 5. Evaluate the different e-governance models.			

COURSE CURRICULUM

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to e-commerce: Meaning and concept of ecommerce, ecommerce vs e-business, advantages and disadvantages of ecommerce, value chain in e commerce, Porter's value chain model, competitive advantage and competitive strategy, different types of ecommerce like B2B, B2C, C2C, C2B, G2C. E-core values: ethical issues, legal issues, taxation issues and international issues.	**CLO1**	**6**
UNIT II		
Technology in e-commerce: An overview of the internet,basic network architecture and the layered model, internet architecture,intranets and building and hosting your website,choosing an ISP, registering a domain name,e-cycle of internet marketing, personalization,mobile agents,tracking customers,customer service,CRM and e-value. URLs and HTTP, cookies.	**CLO2**	**6**
UNIT III		
Web Page Design & Security: Overview of HTML, basic structure of an HTML document, basic text formatting, links, images, tables, frames, forms,Security threats, Security in cyberspace, Kinds of threats and crimes,Basic cryptography for enabling security in e commerce,encryption and its Types,Public and Private key Encryption, Authentication and trust using digital signature and digital certificates, internet security using VPN, firewalls, SSL.	**CLO3**	**6**
UNIT IV		
Introduction to e-Governance: An Overview,Why E-Governance,Basic Structure of e-Governance,Scope of e-Governance,Stages of e-Governance,Types of Interactions in e-Governance,Use of Technology in addressing Governance Issues,Advantages of E-governance, Future Perspective of E-governance.	**CLO4**	**6**
UNIT V		

e-Governance Models: Introduction,Models of Digital Governance, Broadcasting/Wider Dissemination Model, Critical Flow Model, Comparative Analysis Model, Mobilization and Lobbying Model, Interactive Service Model, Government-to-Citizen-to-Government Model (G2C2G),Evolution in E-Governance and Maturity Models, Five Maturity Levels,Characteristics of Maturity Levels.	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. Arun Kumar. E-commerce. New Delhi, Global India Publications, 2010
2. Vishwas Tripathi. E-governance: Perspective and challenges.

Reference Books:

1. Mishra, Jibitesh. E-commerce.
2. Timmers, Paul. Electronic Commerce – Strategies and Models for Business-to-Business Trading. Chichester, John Wiley, 2000.

Online Resources/E-Learning Resources

1. http://hdl.handle.net/123456789/25880
2. http://ecommerce.internet.com/resources/library

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: II**		**Level: UG**	
Course Name		**Foundation Of Cryptography**		**Course Code/ Course Type**		UBS114/VSC	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	-	-	2	2	20	30	-
Prerequisite: Students should have basic Knowledge of Networking							
Course Objectives (CO):				The objectives of Introduction to Foundations of Cryptography are: 1. To describe the fundamental concepts of security. 2. Classify the various mechanisms used in encryption. 3. Explain the mathematics of cryptography. 4. Compare the different key management schemes used for Data Integrity. 5. Evaluate the security mechanism used at different layers of the network.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the basic goals of security. 2. Explain the different types of encryption methods. 3. Examine the types of encryptions used in cryptography. 4. Analyze the schemes for Data management. 5. Justify the role of different layers for network security.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Basic Principles: Security Goals,Cryptographic Attacks,Services and Mechanisms, Mathematics of Cryptography.	**CLO1**	**6**
UNIT II		
Symmetric Encryption: Mathematics of Symmetric Key Cryptography,Introduction to Modern,Symmetric Key Ciphers,Data Encryption Standard,Advanced Encryption Standard.	**CLO2**	**6**
UNIT III		
Asymmetric Encryption: Mathematics of Asymmetric Key Cryptography, Asymmetric Key, Cryptography.	**CLO3**	**6**
UNIT IV		
Data Integrity, Digital Signature Schemes & Key Management: Message Integrity and Message Authentication,Cryptographic Hash Functions,Digital Signature,Key Management.	**CLO4**	**6**
UNIT V		
Network Security-I: Security at application layer: PGP and S/MIME, Security at the Transport Layer: SSL and TLS, Network Security-II: Security at the Network Layer: IPSec, System Security.	**CLO5**	**6**
Total Hours		**30**

Learning resources

TextBooks: -

1. Cryptography and Network Security, 3rd Edition Behrouz A Forouzan, Deb deep Mukhopadhyay, McGraw Hill,2015
2. Cryptography and Network Security,4th Edition, William Stallings, (6e) Pearson,2006

Reference Books:

1. Everyday Cryptography, 1st Edition, Keith M.Martin, Oxford,2016
2. Network Security and Cryptography, 1st Edition, Bernard Meneges, Cengage Learning,2018

Online Resources/E-Learning Resources

1. The Complete Cyber Security Course: Hackers Exposed --- https://www.udemy.com/course
2. Foundations of Cybersecurity----- https://www.coursera.org/

COURSE CURRICULUM:

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc (Cyber Security)</b></td><td colspan="2"><b>Semester: II</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Discrete Mathematics</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2">UBS115/BSC</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hrs.</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/Oral</b></td></tr>
<tr><td>2</td><td>-</td><td>-</td><td>2</td><td>2</td><td>20</td><td>30</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite: Basic Knowledge of Mathematics.</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Discrete Mathematics are:
1. To remember Graph theory and associated concepts.
2. Recognize the mathematical logic of truth tables.
3. To apply set operations in algebraic structures.
4. Classify the different properties of relations.
5. To evaluate the relative frequency.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Identify the fundamental concepts of graph theory.
2. Explain the use of the truth table in mathematical logic.
3. Complete the operations on sets,
4. Assess the various operations on relations.
5. Justify the use of Probability.</td></tr>
</table>

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Graph Theory: Introduction, Simple graph, adjacency/ incident/ neighborhood/ degree of a vertex, degree sequence of a graph, first fundamental theorem of graphs, subgraph and induced sub-b graphs, Adjacent matrices and incidence matrices, walk, length of a walk, open and closed walks, trial and path, circuit and cycle, connected graph and disconnected graph.	**CLO1**	**6**
UNIT II		
Mathematical Logic: Introduction, proposition, connectives, truth tables and duality, converse/contrapositive/inverse,tautology,contradiction,contingency,logically equivalent, DNF, CNF, PDNF, PCNF	**CLO2**	**6**
UNIT III		
Algebraic Structures:Introduction,sets and set operations,functions,relations and their properties & representations of relation by matrix,closure of different types of relations,equivalence relations,primitive recursive function.	**CLO3**	**6**
UNIT IV		
Relations and Partially Ordering: Introduction,Properties of relations,relation matrix,directed graph,closures of relation,equivalence relations, congruence relation, equivalence classes,equivalence classes and partitions,Partially ordered set,lexicographic ordering, Hesse diagrams, minimal and maximal elements, upper and lower bounds.	**CLO4**	**6**
UNIT V		
Probability and Statistics: Introduction,Classical relative frequency and axiomatic,Definition of probability,Addition rule and conditional probability,multiplication rule and total probability,Bayes' theorem and independence problems,measures of central tendency,measures of dispersion,coefficient of variation.	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. Erwin Kreyszig, Advanced Engineering Mathematics, 10th Edition, John Wiley & Sons, 2014.
2. Ronald E Walpole, Raymond H Myers, Sharon L Myers, and Keying E Ye, "Probability and Statistics for Engineers and Scientists", Pearson Education, Delhi-9th edition, 2012.
3. B S Grewal, "Higher Engineering Mathematics", 44th edition, Khanna Publishers.

Reference Books:

1. B.S. Grewal, Higher Engineering Mathematics, Khanna Publishers, 44thEdition, 2010.
2. B S Grewal, Numerical methods in engineering and science, 10th Edition, Khanna publishers, 2016.
3. Kishor S Trivedi, "Probability and Statistics with reliability, Queuing and Computer Science Applications", John Wiley & Sons, 2nd edition, 2008.

Online Resources/E-Learning Resources

1. https://www.edx.org/learn/discrete-mathematics
2. https://www.codecademy.com/learn/discrete-math

COURSE CURRICULUM

Name of the Program:	**BSc(Cyber Security)**	**Semester: II**	**Level: UG**
Course Name	**Concepts and Application in Science**	**Course Code/ Course Type**	ACIKSSS101
Course Pattern	**2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	50	-	-

Prerequisite: Basic knowledge of Science.	
Course Objectives (CO):	The objectives of Concepts and Application in Science are: 1. To remember Indian Knowledge Systems: Origin, Evolution and Ontological Approach 2. To understand Indian Knowledge Approaches. 3. To apply Sciences of Life and Mind. 4. To examine Indian Knowledge System Torchbearers – Ancient and Modern 5. To analyze Self-Knowledge for Personal Effectiveness.
Course Learning Outcomes (CLO):	Students would be to: - 1. Identify and appreciate the rich heritage that resides in our traditions. 2. Explain the mind/voice dynamic in Indian knowledge systems. 3. Explain the practices that will prepare one for the inner-journey to discover the Self. 4. Analyze the need and importance of Sanskrit in getting to the roots of the philosophical concepts. 5. Analyze the various functions in Indian knowledge systems.

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Indian Knowledge System and Vedic Corpus: Introduction to IKS,Need for IKS, Historicity of IKS,Salient aspects of IKS,IKS in ancient India and in modern India.Introduction to Vedas, Four Vedas, Sub-classification of Vedas, Messages in Vedas, Basics of Nirukta and Chandas.	**CLO1**	**6**
UNIT II		
Wisdom through the Ages: Puranas,Ithihasas,Nitishastras,Subhasitas,Linguistics, Components of a language,Paṇini's work on Sanskrit grammar,Phonetics in Sanskrit, Role of Sanskrit in natural language processing,Framework for establishing valid knowledge.	**CLO2**	**6**
UNIT III		
Number Systems and Units of Measurement: Salient features of the Indian numeral system,Importance of decimal representation, The discovery of zero and its importance,Unique approaches to represent numbers, Unique aspects of Indian Mathematics,Great mathematicians and their significant contributions in the area of arithmetic, algebra, geometry, trigonometry, combinatorial problems in Chandaḥ-sastra of Pingala	**CLO3**	**6**
UNIT IV		
Knowledge Framework and classifications: Indian scheme of knowledge,The knowledge triangle,Prameya,A vaiśeṣikan approach to physical reality, Dravyas,The constituents of the physical reality	**CLO4**	**6**
UNIT V		
Science and Technology in the Vedic Age and Post-Vedic Records. **Knowledge:** Framework and Classification, Astronomy Encryption Method used in ancient India, Introduction to Yantra Shastra,Vaimanik Shashtra, Agriculture Technologies	**CLO5**	**6**

Total hours		**30**

Activity 1: Comparative Analysis of Traditional and Modern Scientific Methods.

Activity 2: Presentation on Indian scientific texts such as the Phonetics in Sanskrit, Astronomy Encryption Method used in ancient India.

Learning resources

Textbooks:

1. Health Science: Concepts and Applications, Authors: Jacquelyn Rhine Marshall and Sue C. Roe
2. Introduction to Indian Knowledge Systems: Concepts and Applications by Prof. B Mahadevan

Reference Books: -

1. Introduction to Indian Knowledge System: Concepts and Applications by Pallavi Ghosh

Online Resources/E-Learning Resources

1. https://onlinecourses.swayam2.ac.in/

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester : II**		**Level: UG**	
Course Name		**UHVI: Professional Ethics**		**Course Code/ Course Type**		**ACUHV101/AC**	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	-	-	-	2	50	-	-
Pre-Requisite: UHV-I							

Course Objectives (CO):

The objectives of Universal Human Value- Professional Ethics are:

1. To make the students understand the importance of ethical behaviour.
2. To expose the students to the ethical practices to be followed in profession
3. To sensitize the students to become responsible persons who will uphold ethics in profession when they pursue their career
4. To make students understand Psychological and Philosophical approaches
5. To make students understand social responsibility and corporate Sustainability

Course Learning Outcomes (CLO):

Students would be able to:

1. Equip themselves with an understanding of moral, professional and personal values.
2. Understand the need of ethics in shaping their profession The learners will hone their decision-making skills.
3. Refine their business ethics based on psychological and philosophical perspective.
4. Assess the need for a balance between ecology, and economy.
5. Equip themselves with a better understanding of themselves and the society they live in and the responsibilities they shoulder in creating a sustainable world.

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Individual and Professional Ethics: Introduction to Professional Ethics, Morals, Values and Ethics – Personal and Professional- Sensé of Professional Ethics – Code of Ethics by NSPE-Making decisions with ethical dimensions–definition–roadmap to ethical decision making–common standards– internal obstacles – bias – empathy	**CLO 1**	**6**
UNIT II		
Business Ethics: Philosophical approaches to Business Ethics – ethical reasoning – ethical issues in business - Social Responsibility of Business- conflict of interest–cultural relativism-Ethical Leadership-Resisting un-ethical authority and domination-Global Business Ethics	**CLO 2**	**6**
UNIT III		
Psychological Approaches: Ethical Theories-Psychological and Philosophical Approaches-Myths about Morality-conflict of interest in psychological perspective - Courage-Integrity – ethical dilemma – Emotional Intelligence (Mahabharata- Iskcon Publications)	**CLO 3**	**6**
UNIT IV		
Workplace Ethics: Ethics in changing domains of Research–academic integrity–intellectual honesty-Role of Engineers and Managers-Ethical issues in Diverse workplace – competition – free will**-** Confidentiality – employee rights – Intellectual property rights – discrimination	**CLO 4**	**6**

UNIT V		
Safety, Responsibilities and Rights: Ecology, and Economy-Risk benefit analysis and reducing risk SDGs–Corporate social responsibility and Corporate Sustainability - CSR in India - Sustainability Case Studies.	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. Subramanian. R. Professional Ethics, Oxford Publication,2013.
2. Nagarasan. R. S. Professional Ethics and Human Values. New Age International Publications, 2006.

Reference Book:

1. Mike W Martin and Roland Schinzinger, *Ethics in Engineering*,4th edition, Tata McGraw Hill Publishing Company Pvt Ltd, New Delhi,2014

Online Resources/E-Learning Resources

1. https://www.nspe.org/resources/ethics/code-ethics
2. https://www.toolshero.com/tag/ethical-decision-making/
3. https://pagecentertraining.psu.edu/public-relations-ethics/introduction-to-public-relations-ethics/lesson-1/ethical-theories/
4. https://peer.asee.org/case-studies-in-engineering-ethics.pdf

CIA Guidelines

Online Quiz (Based on MCQ)- 20 marks

Activity (with short Report Submission) - 20 Marks

Academic Sincerity - 10 marks

Few of the suggested activities are Assignments, Debates, Poster presentations, Model making, Group presentation, Field visits and Group Discussions.

Few of suggested topics related to **UHV1- Professional Ethics** are:

Debate Topics

- Ethical Approach versus Realistic Approach
- Individual and Social Approach
- Dilemma between heart and Mind

Activity

- Analyze the wastage (Electricity or any other) at work place? How you managed.

Assignment

- Analyze the code of ethics at work place
- If you fulfil the duties, rights will automatically fall in place. Justify the statement

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: II**		**Level: UG**	
Course Name		**Cyber Laws**		**Course Code/ Course Type**		UBS116A/OE	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	-	-	2	2	20	30	-
Prerequisite: Students should have basic Knowledge of Cyber.							
Course Objectives (CO):				The objectives of Introduction to Cyber Laws are: 1. To remember the fundamental concepts of Cyber Laws 2. To understand the role of Regulatory Framework in Cyber Laws. 3. To demonstrate the different cybercrimes. 4. To compare different types of e-commerce issues. 5. To examine various IPR Issues with respect to Cyber Laws.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Memorize the basics of Cyber Laws. 2. Discuss the framework about cyber crimes. 3. Examine the different cybercrimes and their objectives. 4. Classify the different types of issues associated with e-commerce. 5. Review the various IPR issues.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Cyber Law: Introduction about the cyberspace,Regulation of cyberspace,Introducing cyber law, Scope of Cyber laws,e-commerce,online contracts, IPRs(copyright, trademarks and software patenting),e-taxation,e-governance and cybercrimes, Cyber law in India with special reference to Information Technology Act 2000	**CLO1**	**6**
UNIT II		
Regulatory Framework: International Legal Regime, International legal regime relating to Cyber Crimes, European Convention on Cyber Crimes, Hague Convention on Jurisdiction and Foreign Judgments,Jurisdiction Agreement, International legal regime relating to E-Commerce.	**CLO2**	**6**
UNIT III		
Cyber Crimes: Introduction to computer crime and cybercrimes,Classification of cybercrimes,Distinction between cybercrime and conventional crimes, Reasons for commission of cyber crime,Cyber forensic, Cyber criminals and their objectives, Cyber stalking,Cyber pornography,Forgery and Fraud,Crime related to IPRs,Cyber terrorism,computer vandalism etc.	**CLO3**	**6**
UNIT IV		
E-Commerce: Definition of E-commerce, Types of E-commerce, Important Issues in Global E-commerce,Application of conventional territory-based law to E-commerce Taxation, Intellectual Property Rights, International Trade, Commercial law and standards, Dispute resolution	**CLO4**	**6**
UNIT V		
IPR Issues: Copyright Issues in Cyberspace Linking, Inlining,Framing,Protection of content on web site,International Treaties,Trademark Issues in cyberspace,Domain Name Dispute,Cybersquatting,Uniform Dispute Resolution Policy,Meta-tags and Keywords.	**CLO5**	**6**
Total hours		**30**

Learning resources

Textbooks:

1. Cyber Law" by Dr Pavan Duggal
2. Cybersecurity Law, Standards and Regulations By Schreider Tari

Reference Books:

1. "Information Technology Law and Practice" by Vakul Sharma and Seema Sharma
2. Cybersecurity Law by Jeff Kosseff John Wiley & Sons, Inc.

Online Resources/E-Learning Resources

1. https://www.legalbites.in/cyber-space-meaning-regulation-scope/
2. https://lawbhoomi.com/

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: II**		**Level: UG**	
Course Name		**E-Commerce**		**Course Code/ Course Type**		UBS116B/OE	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	-	-	2	2	20	30	-
Prerequisite: Students should have basic Knowledge of commerce.							
Course Objectives (CO):				The objectives of Introduction to E-commerce are: 1. To Recognize the need of e-commerce. 2. Illustrate the different frameworks of e-commerce. 3. Identify the various types of e-commerce applications. 4. Analyze the types of electronic data security mechanisms used in e-commerce applications. 5. Discuss the e-marketing techniques used.			
Course Learning Outcomes (CLO):				Students would be able to: 1. List out the applications of e-commerce. 2. Explain the network services used in e-commerce. 3. Demonstrate the various modes of payments used in e-commerce applications. 4. Analyze the different security and Privacy Implementation. 5. Plan various techniques used for e marketing.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction:E-Commerce,Meaning,Advantages & Limitations,Traditional & Contemporary Model, Impact of E-Commerce on Business Models,Classification of E Commerce,B2B,B2C,C2B,C2C,B2E,Applications of Ecommerce,E-Commerce Organization Applications.	**CLO1**	**6**
UNIT II		
Framework of E-Commerce: Application Services,Interface Layers,Secure Messaging,Middleware Services and Network Infrastructure ,Site Security Firewalls & Network Security,TCP/IP,HTTP ,Secured HTTP ,SMTP ,SSL.	**CLO2**	**6**
UNIT III		
Consumer Oriented e-commerce Applications: Introduction,Mercantile Process Model,Consumers Perspective and Merchant's Perspective,Electronic Payment Systems,Legal Issues & Digital Currency,E-Cash & E-Cheque,Electronic Fund Transfer (EFT),Advantages and Risks,Digital Token Based E-Payment System.	**CLO3**	**6**
UNIT IV		
Electronic Data Interchange: Introduction,EDI Standards,Types of EDI,EDI Applications in Business,Legal Security and Privacy issues of EDI,EDI Software Implementation	**CLO4**	**6**
UNIT V		
E-Marketing Techniques: Introduction,New Age of Information,Based Marketing,Influence on Marketing,Search Engines & Directory Services, Charting the OnLine Marketing Process,Chain Letters,Applications of 5P's (Product, Price, Place, Promotion, People).	**CLO5**	**6**
Total hours		**30**

Learning resources

Textbooks:

1. Frontiers of Electronic Commerce: Ravi Kalakota, Andrew B Whinston, Pearson
2. E-Commerce: Tulasi Ram Kandula, HPH.
3. E-Commerce: An Indian Perspective: P.T. Joseph, S.J, PHI

Reference Books:

1. E-Commerce & Mobile Commerce Technologies: Pandey, SaurabhShukla, S. Chand
2. Electronic Commerce: Pete Loshin / John Vacca, Firewall Media
3. E-Commerce, Strategy, Technologies And Applications : David Whiteley, Tata Mcgraw Hill

Online Resources/E-Learning Resources

1. https://www.edx.org/learn/ecommerce
2. https://www.coursera.org/professional-certificates/google-digital-marketing-ecommerce

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester - III

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester:III**		**Level: UG**	
Course Name		**Design Analysis of Algorithm**		**Course Code/ Course Type**		**UBS201/MAJM**	
Course Pattern		**2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basics of Algorithms.							
Course Objectives (CO):				The objectives of Design Analysis of Algorithm are: 1. To describe the fundamentals of Algorithms. 2. Explain the rigorous correctness proofs for algorithms. 3. To associate the principles of optimality with major algorithms. 4. Classify the methods for Iterative improvement. 5. To evaluate limitations of Algorithms.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define the various problem types and algorithms. 2. Explain a problem into two or more sub-problems of the same or related type. 3. Apply knowledge of different algorithm design techniques for a given problem. 4. Analyze different algorithm design techniques. 5. Examine the techniques to account for the true cost of the computation.			

Course Contents/Syllabus:		
Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction: Notion of an Algorithm, Fundamentals Algorithmic, Problem Solving, Important Problem Types, Fundamentals of the Analysis of Algorithmic Efficiency, Asymptotic Notations and their properties,Analysis Framework,Empirical analysis,Mathematical analysis for Recursive and Non-recursive algorithms.	**CLO 1**	**9**
UNIT II		
Brute Force and Divide and Conquer: Brute Force,Computing an String Matching,Closest Pair and Convex Hull Problems,Exhaustive Search,Travelling Salesman Problem,Knapsack Problem,Assignment problem,Divide and Conquer Methodology,Binary Search,Merge sort,Quick sort,Heap Sort.	**CLO 2**	**9**
UNIT III		
Dynamic Programming and Greedy Technique: Dynamic programming,Principle of optimality,Coin changing problem,Computing a Binomial Coefficient,Floyd's algorithm,Multi stage graph,Optimal Binary Search Trees,Knapsack Problem.Greedy Technique,Container loading problem,Prim's algorithm and Kruskal's Algorithm.	**CLO3**	**9**
UNIT IV		
Iterative Improvement: The Simplex Method,The Maximum Flow Problem,Maximum Matching in Bipartite Graphs,Stable marriage Problem.	**CLO4**	**9**
UNIT V		

Coping With the Limitations of Algorithm Power: Lower Bound Arguments,P,NP,NP Complete and NP Hard Problems,Backtracking,n Queen problem, Hamiltonian Circuit Problem, Subset Sum Problem, Branch and Bound,LIFO Search and FIFO search, Assignment problem,Knapsack Problem.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. AnanyLevitin, ―Introduction to the Design and Analysis of Algorithms‖, Third Edition, Pearson Education, 2017.
2. Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran, Computer Algorithms/ C++, Second Edition, Universities Press, 2007.

Reference Books:

1. AlfredV.Aho, John E. Hopcroft and Jeffrey D. Ullman.
2. Data Structures and Algorithms‖, Pearson Education Reprint 2006.
3. HarshBhasin, ―Algorithms Design and Analysis‖, Oxford university press, 2015.

Online Resources/E-Learning Resources

1. https://soumadip.github.io/courses/DAA/
2. https://ocw.mit.edu/courses/6-046j-design-and-analysis-of-algorithms

COURSE CURRICULUM

Name of the Program:	**BSc (Cyber Security)**	**Semester: III**	**Level: UG**
Course Name	**Design Analysis of Algorithm Lab**	**Course Code/ Course Type**	UBS202/MAJM
Course Pattern	**2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
-	1	-	1	2	25	-	25

Prerequisite: Basic Knowledge of C,OS and Algorithm is required.

Course Objectives (CO):	The objectives of Design Analysis of Algorithm Lab are: - 1. To Understand the fundamentals of design analysis of algorithm. 2. Compare the various types of Algorithms like sorting, searching. 3. To analyze the use of Divide and Conquer technique for time complexity. 4. To evaluate complex problems by breaking them down into simpler subproblems. 5. To Solve problems by using greedy method.
Course Learning Outcomes (CLO):	Students would be able to: 1. Identify the use of algorithms. 2. Explain the forms of Algorithms for Performance Analysis. 3. Apply different designing methods for development of algorithms to realistic problems. 4. Describe the dynamic-programming, backtracking paradigm and explain when an algorithm design situation calls for it. 5. Design paradigms for complex problems and solve novel problems, by choosing the appropriate algorithm.

Course Contents/Syllabus: Practical Plan

Activity Number	**Assignment/Practical/Activity Title**	**Week Number/Turn**	**Details**	**CLO**	**Hours**
1	Introduction to Algorithms with Pseudo Code	Week 1	To find the max element of an array.	CLO1	2
2	Performance Analysis	Week 2	Assignment based on Space Complexity.	CLO1	2
3	Performance Analysis	Week 3	Time Complexity.	CLO1	2
4	Sorting Algorithm	Week 4	To implement following algorithm using array as a data structure and analyze its time complexity. a. Bubble sort b. Radix sort	CLO2	2
5	Searching Algorithm	Week 5	To implement Linear search	CLO2	2

			and Binary search		
6	Searching Algorithm	Week 6	To Analyze its time complexity	CLO2	2
7	Divide and Conquer Technique	Week 7	To implement following algorithm using array as a data structure and analyze its time complexity. a. Merge sort	CLO3	2
8	Divide and Conquer Technique	Week 8	Quick sort	CLO3, CLO4	2
9	Dynamic Programming	Week 9	To Implement Matrix Chain Multiplication.	CLO4	2
10	Dynamic Programming	Week 10	To Implement Largest Common Subsequence.	CLO4	2
11	Greedy Algorithm	Week 11	To implement Knapsack Problem	CLO4	2
12	Greedy Algorithm	Week 12	To implement an Activity Selection Problem.	CLO5	2
13	Greedy Algorithm	Week 13	To implement Huffman Coding and analyze its time complexity.	CLO5	2
14	Greedy Algorithm	Week 14	Task Scheduling	CLO5	2
15	Shortest Path Graph	Week 15	To implement Dijkstra's Algorithm.	CLO5	2
Total					**30 hrs.**

Learning resources

Textbooks:

1. Fundamentals of Computer Algorithms, Ellis Horowitz, SartajSahni and Rajasekharan, Universities press
2. Design and Analysis of Algorithms, P. h. Dave,2nd edition,Pearson Education.

Reference Books:

1. Introduction to the Design And Analysis of Algorithms A Levitin Pearson Education
2. Algorithm Design foundations Analysis and Internet examples, M.T.Goodrich and R Tamassia John Wiley and sons

Online Resources/E-Learning Resources

1. https://soumadip.github.io/courses/DAA/
2. https://ocw.mit.edu/courses/6-046j-design-and-analysis-of-algorithms

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester : III**		**Level: UG**	
Course Name		**Web Application Security**		**Course Code/ Course Type**		**UBS203/MAJM**	
Course Pattern		**2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basic knowledge of Network and Security is required.							
Course Objectives (CO):				The objectives of Web Application Security are: 1. Identify the need of Web Application security. 2. Classify the different security mechanisms in web applications. 3. Use security principles to design a reliable web application. 4. Categorize the different attacks in web applications. 5. Designing a secure web application.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define the vulnerabilities in the web applications. 2. Explain the various types of security measures for web application. 3. Execute the security principles for web browsers. 4. Categorize the different types of Vulnerabilities. 5. Make use of penetration testing to improve the security of web applications.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Overview of Web Applications & Security: Introduction,History of web applications, Drawbacks of web applications,Web application Vs Cloud application, Software Security,Recognizing Web Application,Threats,Authentication and Authorization.	**CLO 1**	**9**
UNIT II		
Web Application Security Fundamentals: Security Fundamentals,Input Validation,Attack Surface Reduction, Rules of Thumb,Classifying and Prioritizing Threads,Microsoft Security Development Lifecycle (SDL).	**CLO 2**	**9**
UNIT III		
Browser Security Principles: Origin Policy,Exceptions to the Same Origin Policy,Cross Site Scripting and Cross Site Request, Forgery,Reflected XSS, HTML Injection	**CLO3**	**9**
UNIT IV		
Web Application Vulnerabilities: Understanding vulnerabilities in traditional client server application and web applications,client state manipulation,cookie based attacks, SQL injection.	**CLO4**	**9**
UNIT V		
Web Application Mitigations: Http request,Http response,Rendering and events,Html image tags,image tag security issues, java script on error, Javascript timing,remote scripting,running remote code, frame and iframe , browser sandbox	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Professional, 2011.
2. Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley Sons, 2011

Reference Books:

1. Michael Cross, Developer's Guide to Web Application Security, 2007, Syngress Publishing, Inc.
2. Ravi Das and Greg Johnson, Testing and Securing Web Applications, 2021, Taylor & Francis Group, LLC.

Online Resources/E-Learning Resources

1. https://portswigger.net/web-security
2. https://www.coursera.org/learn/codio-software-security-for-web-applications

COURSE CURRICULUM

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc (Cyber Security)</b></td><td colspan="2"><b>Semester: III</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Web Application Security Lab</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2">UBS204/MAJM</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="4"><b>Teaching Scheme</b></td><td colspan="4"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hours</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/Oral</b></td></tr>
<tr><td>-</td><td>1</td><td>-</td><td>1</td><td>2</td><td>25</td><td>-</td><td>25</td></tr>
<tr><td colspan="8"><b>Prerequisite: Basic Knowledge Web is required.</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Web Application Security Lab are: -
1. To Understand the fundamentals of web browser and web security
2. Classify the hierarchy of objects used in a web application.
3. Illustrate the attacks and their types.
4. Differentiate between the types of attacks and their effects.
5. To Solve the problems of attacks by using various security mechanisms.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Understand and identify the need for security.
2. Explain the hierarchy of objects in a web application.
3. Apply various security mechanisms for enhancing web experience.
4. Describe the types of attacks and their prevention.
5. Make use of the Encryption mechanism for enhancing the security aspect of the web.</td></tr>
</table>

Course Contents/Syllabus: Practical Plan

Activity Number	Assignment/Practical/Activity Title	Week Number/ Turn	Details	CLO	Hours
1	Introduction to Web Security.	Week 1	1. Inside look at modern web browsers.	CLO1	2
2	Navigation and its Process	Week 2	1. What happens in navigation	CLO1	2
3	Renderer Process in Web	Week 3	1. Inner workings of a Renderer Process 2. Renderer processes handle web contents	CLO1	2
4	Hierarchy of Objects in Web	Week 4	1. Parsing 2. Construction of DOM 3. Sub resource loading	CLO2	2
5	Blocking the Parsing	Week 5	1. JavaScript can block the parsing. 2. Style calculation 3. Logout	CLO2	2
6	Introduction to HTTP	Week 6	1. Client: the user-agent 2. The Web server 3. Proxies	CLO2	2
7	Client Side Attacks	Week 7	1. HTTP cookies 2. Creating cookies 3. Define the lifetime of a cookie 4. Restrict access to cookies	CLO3	2
8	Client Side Attacks	Week 8	1. Where cookies are sent 2. Path attribute 3. SameSite attribute 4. Cookie prefixes	CLO3 , CLO4	2
9	Session Attacks	Week 9	1. Cross-Site Request 2. Forgery Prevention	CLO4	2
10	Server Side Attacks	Week 10	1. Command Injection 2. SQL Injection.	CLO4	2

11	Server Security	Week 11	1. Demonstrate the Risk.	CLO5	2
12	Encryptions	Week 12	1. HTTP Encryptions on the Web.	CLO5	2
13	HTTPS in the Real World	Week 13	1. Pinning	CLO5	2
14	HTTPS in the Real World	Week 14	1. Somebody Always Watching.	CLO5	2
15	Web Security	Week 15	1. Harvesting credit card numbers and passwords from your site	CLO5	2
Total					**30 hrs.**

Learning resources

Textbooks:

1. Web Application Security by Andrew Hoffman O'Reilly Media, Inc
2. Grokking Web Application Security by Malcolm McDonald

Reference Books:

1. Web Application Security by Malcolm McDonald
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition

Online Resources/E-Learning Resources

1. https://owasp.org/#

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester: III**		**Level: UG**	
Course Name		**Operating System Security**		**Course Code/ Course Type**		**UBS205A/MAJE**	
Course Pattern		**2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basic knowledge of Computers is required.							
Course Objectives (CO):				The objectives of Operating System Security are: 1. To recall the basic concepts of Operating Systems. 2. To explain the various process management concepts including scheduling, synchronization, threads and deadlock. 3. Identify the memory, file and I/O management activities of the Operating system. 4. Examine the requirements of a secured system. 5. Elaborate how security is implemented in various operating systems.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define the need of an Operating system. 2. Infer the process management activities in an operating system. 3. Classify the various activities of memory management. 4. Highlight the goals of a secure system. 5. Discuss the need of a secured operating system.			

Course Contents/Syllabus

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Operating System Overview: Introduction, Computer System, Organization, Architecture, Operating System Operations, Resource Management, Security and Protection, Kernel Data Structures, Operating System Services, System Calls, System Services, Why applications are Operating System Specific	**CLO 1**	**9**
UNIT II		
Process Management: Process Concept, Process Scheduling,Operation on Processes,Inter process Communication,Threads,Threading issues,CPU Scheduling,Scheduling criteria,Scheduling algorithms,Deadlock characterization,Methods for handling deadlock,Deadlock prevention,Deadlock avoidance,Detection,Recovery.	**CLO 2**	**9**
UNIT III		
Memory Management and File Systems: Introduction,Swapping,Paging,Contiguous Memory Allocation,Segmentation,Virtual Memory,Demand Paging,Page Replacement,Allocating Kernel Memory,File concept, Access methods,Directory Structure,Sharing and Protection,File System Structure,Allocation Methods.	**CLO3**	**9**
UNIT IV		
Secure Systems and Verifiable Security Goals: Security Goals,Trust and Threat Model,Access Control Fundamentals,Protection System,Reference Monitor,Secure Operating System Definition,Assessment Criteria, Information Flow,Information Flow Secrecy Models,Biba Integrity Model,ClarkWilson IntegrityModel.	**CLO4**	**9**
UNIT V		
Security In Operating Systems:UNIX Security,UNIX Protection System,UNIX Authorization,UNIX Security Analysis,Windows Security,Windows Protection System,Windows Authorization,Windows Security Analysis,Windows Vulnerabilities,Address Space Layout Randomizations,Introduction to Security Kernels.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, "Operating System Concepts", John Wiley & Sons, Inc., 10th Edition, 2021.
2. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers series, 2008.

Reference Books:

1. Morrie Gasser, "Building A Secure Computer System", Van Nostrand Reinhold, New York,1988.
2. Charles Pfleeger, Shari Pfleeger, Jonathan Margulies, "Security in Computing", Fifth Edition, Prentice Hall, New Delhi, 2015.
3. William Stallings, "Operating Systems – Internals and Design Principles", 9th Edition, Pearson, 2017.

Online Resources/E-Learning Resources

1. https://www.ischool.berkeley.edu/courses/cyber/211
2. https://www.javatpoint.com/operating-system-security

COURSE CURRICULUM

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc(Cyber Security)</b></td><td colspan="2"><b>Semester :III</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Firewall and VPN Security</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2"><b>UBS205B/MAJE</b></td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2"><b>1.0</b></td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hours</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/Oral</b></td></tr>
<tr><td>3</td><td>-</td><td>-</td><td>3</td><td>-</td><td>40</td><td>60</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite: Basic knowledge of Networking and Security.</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Firewall and VPN Security are:
1. Define the basics of Firewall.
2. Illustrate the security risks and vulnerabilities.
3. Classify the different types of authentications and access control mechanisms.
4. Analyze the categorizations of VPNs.
5. Create ACLs to filter traffic through the firewall.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Identify and assess the need of Firewall for security.
2. List the different types of methods used in detecting the vulnerabilities.
3. Demonstrate the mechanism used for authentication and access control.
4. Outline the need for Protecting networks from internal and external threats.
5. Plan and Monitor to resolve security problems.</td></tr>
</table>

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Firewall: Introduction,Firewall vs.Antivirus,Limitations of a Firewall, Software Firewall vs a Hardware Firewall,Types of Operational Firewalls,Working of Firewall,Components of Firewall,Best Practices of Firewall,Disable Firewall.	**CLO 1**	**9**
UNIT II		
Intrusion Detection: Intrusion Detection System,Vulnerability, Assessment,Misuse Detection, Anomaly Detection, Network Based IDS, Host Based IDS, Honeypots	**CLO 2**	**9**
UNIT III		
User Authentication and Access Control: User Authentication,Password and Certificate based,Biometric Authentication,Finger/Hand prints, Retina,Patterns,Signature and writing patterns,Access Controls,Authentication Mechanism,Principle Authentication, Authorization, Audit and Policies.	**CLO3**	**9**
UNIT IV		
VPN: Introduction,Devices,Technologies and Protocols,Methods of Categorizing VPNs,Types of VPNs,Install VPN on Computer,Operational Security (OpSec) in VPN,Reliable VPN.	**CLO4**	**9**
UNIT V		
VPN Security: Introduction,Is VPN Safe,Features that make VPN secure, Protecting Digital Privacy by VPN,Encryption in VPN,Case studies.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Build Your Own VPN Server A Step by Step Guide by Lin Song
2. Cisco VPN Configuration Guide Step-By-Step Configuration of Cisco VPNs for ASA and Routers by Harris Andrea

Reference Books:

1. Mastering Openvpn by Eric Crist Network Security Expert & Open Source Contributor
2. VPNs A Beginner's Guide by John Mairs

Online Resources/E-Learning Resources

1. https://www.techradar.com/vpn
2. https://www.cisco.com/c/en_in/products/security/vpn

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester : III**		**Level: UG**	
Course Name		**Security Assessment and Risk Analysis**		**Course Code/ Course Type**		**UBS206/SEC**	
Course Pattern		**2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basics of Security and Computers.							
Course Objectives (CO):				The objectives of Security Assessment and Risk Analysis are: 1. Memorize the challenges of software systems that are secure. 2. Compare the different stages of Software Design. 3. Illustrate the models of Software assurance. 4. Examine the need of having software security in enterprise business. 5. Discuss the need of having a security development framework.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define the core concepts of computer security. 2. Explain the design patterns of software design. 3. Illustrate the best practices for designing a secure software model. 4. Select the various data encryption mechanisms used in various businesses. 5. Simplify the need of having a secured development framework.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Computer Security: Introduction,Defining computer security,Principles of secure software,Trusted computing base,Threat modeling,Techniques for mapping security requirements into design specifications,Secure software implementation, deployment and ongoing management	**CLO 1**	**9**
UNIT II		
Software Design:Introduction,Hierarchical design representations,Difference between high level and detailed design,Handling security with high-level design,General Design Notions,Security concerns designs at multiple levels of abstraction,Design patterns,Quality assurance activities and strategies that support early vulnerability detection,Trust models.	**CLO 2**	**9**
UNIT III		
Software Assurance Model: Identify project security risks & selecting risk management strategies,Risk Management Framework,Security Best practices and Known Security Flaws,Architectural risk analysis,Security Testing & Reliability (Penn testing, RiskBased Security Testing)	**CLO3**	**9**
UNIT IV		
Software Security in Enterprise Business: Identification and authentication, Enterprise Information Security,Symmetric and asymmetric cryptography, Including public key cryptography,Data encryption standard(DES),Advanced encryption standard (AES),Algorithms for hashes and message digests.	**CLO4**	**9**
UNIT V		

Security development frameworks: Security issues associated with the development and deployment of information systems,including Internet-based e-commerce,e-business and e-service systems. Case Studies on Security frameworks need to be explained.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. W. Stallings, Cryptography and network security: Principles and practice, 5 th Edition, Upper Saddle River, NJ: Prentice Hall., 2011
2. C. Kaufman, r. Perlman, & M. Speciner, Network security: Private communication in a public world, 2 nd Edition, Upper Saddle River, NJ:Prentice HalL, 2002

Reference Books:

1. M. Merkow, & J. Breithaupt, Information security: Principles and practices. Upper Saddle River, NJ:Prentice Hall,2005
2. Gary McGraw, Software Security: Building Security In, Addison-Wesley, 2006

Online Resources/E-Learning Resources

1. https://www.skillsoft.com/course/security-risks-performing-security-risk-assessments
2. https://www.coursera.org/learn/risk-management-threat-modeling

COURSE CURRICULUM

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc(Cyber Security)</b></td><td colspan="2"><b>Semester :III</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Statistical Techniques</b></td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2"><b>UBS207/BSC</b></td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>Revised 2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2"><b>1.0</b></td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hours</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical/Oral</b></td></tr>
<tr><td>2</td><td>-</td><td>-</td><td>2</td><td>-</td><td>20</td><td>30</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite: Basic Knowledge of Statistics.</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Statistical Techniques are:
1. Recall the basic concepts of statistics.
2. Illustrate the interpretations of graphs and diagrams.
3. Classify the general magnitude of the data.
4. Highlight the concepts of Probability.
5. Formulate problems based on Random variables.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students would be able to:
1. Define the meaning, scope and limitations of Statistics
2. Explain the need for primary and secondary data.
3. Illustrate the different techniques of simple bar diagram, multiple bar diagram, percentage bar diagram, pie diagram
4. Simplify the use of central tendency to solve different statistical problems.
5. Interpret the concepts of probability for solving real life problems.</td></tr>
</table>

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction to Statistics: Meaning,Scope and limitations of statistics,Basic Statistical Concepts,population,sample,variable,attribute,parameter,statistic, Collection of Data,primary and secondary,sample and census,survey(concept only),tabulation of data up to 3 characteristics(simple examples)	**CLO 1**	**6**
UNIT II		
Diagrams and graphs: Introduction,Given a diagram,interpretation of it,simple bar diagram,multiple bar diagram,percentage bar diagram,pie diagram,drawing of frequency curve,frequency polygon,histogram(class intervals of equal lengths only)	**CLO 2**	**6**
UNIT III		
Measures of Central Tendency: Arithmetic mean, weighted mean, combined mean, median,mode without grouping,quartiles(no example on missing frequency)measures of dispersion,range,quartile deviation,mean deviation from mean standard deviation and their relative measures.(concepts of shift of origin and change or scale are not to be done)	**CLO3**	**6**
UNIT IV		
Elementary Probability Theory: Concept of random experiment,trial and possible outcomes,sample space and discrete sample space,events and their types,algebra of events,mutually exclusive and exhaustive events,classical definition of probability, addition theorem (without proof),independence of events.	**CLO4**	**6**
UNIT V		
Random Variable: Probability distribution of a discrete random variable, expectation and variance,simple examples,concept of normal distribution and standard normal variate (SNV),Simple examples	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. Erwin Kreyszig, Advanced Engineering Mathematics, 10th Edition, John Wiley & Sons, 2014.
2. Ronald E Walpole, Raymond H Myers, Sharon L Myers, and Keying E Ye, "Probability and Statistics for Engineers and Scientists", Pearson Education, Delhi-9th edition, 2012.

Reference Books:

1. B.S.Grewal,Higher Engineering Mathematics,Khanna Publishers,44thEdition,2010.
2. B S Grewal,Numerical methods in engineering and science,10th Edition,Khanna publishers,2016.

Online Resources/E-Learning Resources

1. https://ocw.mit.edu/courses/18-05-introduction-to-probability-and-statistics-spring-2022/resources/lecture-notes
2. https://stattrek.com/

COURSE CURRICULUM

Name of the Program:		**B.Sc(Cyber Security)**		**Semester: III**		**Level: UG**	
Course Name		**UHV-II: Understanding Harmony**		**Course Code/ Course Type**		**ACUHV201/AC**	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	-	2	50	-	-
Pre-Requisite: Knowledge of Rights and Values.							
Course Objectives (CO):				The objectives of Universal Human Value- Understanding Harmony are: 1. To train the student for Development of a holistic perspective based on self-exploration about themselves (human being), family, society and nature/existence. 2. To comprehend (or develop clarity) the harmony in the human being, family, society and nature/existence 3. To strengthen self-reflection. 4. To infuse a sense of commitment and courage to act 5. To understand Holistic Understanding of Harmony on Professional Ethics			
Course Learning Outcomes (CLO):				Students would be able to: 1. Analyze the most important requirement for any human being 2. Apply correct appraisal of Physical needs, meaning of Prosperity in detail 3. Analyze salient values in relationship, Friends and Foes, Empathy, False Prestige. 4. Develop holistic perception of harmony at all levels of existence 5. Apply the Holistic Understanding of Harmony on Professional Ethics			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Course Introduction - Need, Basic Guidelines, Content and Process for Value Education Purpose and motivation for the course, recapitulation from Universal Human Values-I, Self-Exploration–what is it? - Its content and process; Personality Traits- Self Excellence, „Natural Acceptance“ and Experiential Validation- as the process for self-exploration, Adaptability, Belief and Understanding- Self discipline, Continuous Happiness and Prosperity- A look at basic Human Aspirations, Right understanding, Relationship and Physical Facility- the basic requirements for fulfilment of aspirations of every human being with their correct priority, Understanding Happiness and Prosperity correctly- A critical appraisal of the current scenario, Method to fulfil the above human aspirations: understanding and living in harmony at various levels.	**CLO 1**	**6**
UNIT II		

Understanding Harmony in the Human Being - Harmony in Myself: Understanding human being as a co-existence of the sentient „I‟ and the material „Body‟, Understanding the needs of Self („I‟) and „Body‟ - happiness and physical facility, Understanding the Body as an instrument of „I‟ (I being the doer, seer and enjoyer)- Habits and Hobbies, SWOT Analysis (Activity) ,Understanding the characteristics and activities of „I‟ and harmony in „I‟ – Dalai Lamas‟ Tibetan Personality Test – Dr. Menninger‟s Psychometric Test., Understanding the harmony of I with the Body: Sanyam and Health; correct appraisal of Physical needs, meaning of Prosperity in detail	**CLO 2**	**6**
UNIT III		
Understanding Harmony in the Family and Society- Harmony in Human-Human Relationship: Understanding values in human-human relationship; meaning of Justice (nine universal values in relationships) and program for its fulfilment to ensure mutual happiness; Trust and Respect as the foundational values of relationship, Understanding the meaning of Trust; Difference between intention and competence, Understanding the meaning of Respect, Difference between respect and differentiation; the other salient values in relationship, Friends and Foes, Empathy, False Prestige.	**CLO 3**	**6**
UNIT IV		
Understanding Harmony in the Nature and Existence - Whole existence as Coexistence: Understanding the harmony in the Nature and its Equanimity, Respect for all, Nature as Teacher, Interconnectedness and mutual fulfillment among the four orders of nature- recyclability and self-regulation in nature, Understanding Existence as Co-existence of mutually interacting units in all-pervasive space, Holistic perception of harmony at all levels of existence.	**CLO 4**	**6**
UNIT V		
Implications of the above Holistic Understanding of Harmony on Professional Ethics: Natural acceptance of human values, Definitiveness of Ethical Human Conduct, Basis for Humanistic Education, Humanistic Constitution and Humanistic Universal Order, Vision for the Holistic alternatives, UHVs for entrepreneurship	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. _Human Values and Professional Ethics by R R Gaur, R Sangal, G P Bagaria, Excel Books, New Delhi, 2010
2. Jeevan Vidya: Ek Parichaya, A Nagaraj, Jeevan Vidya Prakashan, Amarkantak, 1999.
3. Human Values, A.N. Tripathi, New Age Intl. Publishers, New Delhi, 2004.

Reference Books:

1. The Story of Stuff (Book).
2. The Story of My Experiments with Truth - by Mohandas Karamchand Gandhi
3. Small is Beautiful - E. F Schumacher
4. Slow is Beautiful - Cecile Andrews

Online Resources/E-Learning Resources

1. https://www.studocu.com/in/document/jss-science-and-technology-university/human-values/uhv-handout-2-harmony-in-the-human-being/
2. https://vvce.ac.in/wp-content/uploads/2021/04/Realising-Aspirations-of-NEP2020-UHV.pdf
3. https://vemu.org/uploads/lecture_notes/22_12_2022_1850871704.pdf

CIA Guidelines

Online Quiz (Based on MCQ)- 20 marks

Activity (with short Report Submission) - 20 Marks

Academic Sincerity - 10 marks

Few of suggested activities are Assignments, Debates, Poster presentations, Model making, Group presentation, Field visits and Group Discussions.

Few of suggested topics related to UHVII-Understand Harmony are:

Debate Topics

- Materialistic things make you happy
- Happiness in individualism and family
- Spirituality vs Materialistic
- Satisfaction of Body and self (Soul)

Assignment

Students maintain a reflective account of the times they felt happy and prosperous and the causes of that happiness and prosperity for them.

References:

https://www.aicte-india.org/sites/default/files/Model_Curriculum/Minor%20Degree%20in%20Universal%20Human%20Values%20(UHV).pdf

https://uhv.org.in/
https://vvce.ac.in/wp-content/uploads/2021/04/Realising-Aspirations-of-NEP2020-UHV.pdf

COURSE CURRICULUM

Name of the Program:	**B.Sc(Cyber Security)**	**Semester : III**	**Level: UG**
Course Name	**Constitution of India**	**Course Code/ Course Type**	**ACCOI201/AC**
Course Pattern	**Revised 2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	-	2	50	-	-

Prerequisite: Basic Knowledge of Constitution.

Course Objectives (CO):	The objectives of Constitution of India are: 1. To familiarize the students with the key elements of the Indian constitution. 2. To enable students to grasp the constitutional provisions and values. 3. To acquaint the students with the powers and functions of various constitutional offices and institutions. 4. To make students understand the basic premises of Indian politics. 5. To make students understand the role of constitution and citizen-oriented measures in a democracy
Course Learning Outcomes (CLO):	Students would be able to: 1. Analyze the basic structure of Indian Constitution. 2. Remember their Fundamental Rights, DPSP's and Fundamental Duties (FD's) of our constitution. 3. know about our Union Government, political structure & codes, procedures. 4. Understand our State Executive & Elections system of India. 5. Access the Amendments and Emergency Provisions, other important provisions given by the constitution

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Indian Constitution: The Necessity of the Constitution, The Societies before and after the Constitution adoption. Introduction to the Indian constitution, The Making of the Constitution, The Role of the Constituent Assembly. The Preamble of Indian Constitution & Key concepts of the Preamble. Salient features of India Constitution.	**CLO 1**	**6**
UNIT II		
FR's, FD's and DPSP's: Fundamental Rights and its Restriction and limitations in different Complex Situations. Directive Principles of State Policy (DPSP) and its present relevance in our society with examples. Fundamental Duties and its Scope and significance in Nation building	**CLO 2**	**6**
UNIT III		
Governance and Constitution: Federalism in India - Features , Local Government -Panchayats –Powers and functions; 73rd and 74th amendments, Election Commission – Composition, Powers and Functions; Electoral Reforms, Citizen oriented measures – RTI and PIL – Provisions and significance..	**CLO 3**	**6**
UNIT IV		
Union Executive: Parliamentary System, Union Executive – President, Prime Minister, Union Cabinet, Parliament - LS and RS, Parliamentary Committees, Important Parliamentary Terminologies. Supreme Court of India, Judicial Reviews and Judicial Activism.	**CLO 4**	**6**
UNIT V		

State Executive & Elections, Amendments and Emergency Provisions: State Executive, Election Commission, Elections & Electoral Process. Amendment to Constitution (How and Why) and Important Constitutional Amendments till today. Emergency Provisions.	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Text Books

1. "Constitution of India" (for Competitive Exams) - Published by Naidhruva Edutech,Learning Solutions, Bengaluru. – 2022.
2. "Engineering Ethics", M.Govindarajan, S.Natarajan, V.S.Senthilkumar, Prentice –Hall, 2004

Reference Books:

1. "SamvidhanaOdu" - for Students & Youths by Justice HN NagamohanDhas, Sahayana, kerekon.
2. "Constitution of India, Professional Ethics and Human Rights" by Shubham Singles, Charles E. Haries, and et al: published by Cengage Learning India, Latest Edition – 2019.
3. "Introduction to the Constitution of India", (Students Edition.) by Durga Das Basu (DD Basu):Prentice –Hall, 2008.
4. "The Constitution of India" by Merunandan K B: published by Merugu Publication, Second Edition, Bengaluru.

CIA Guidelines

Online Quiz (Based on MCQ)- 20 marks

Activity (with short Report Submission) - 20 Marks

Academic Sincerity - 10 marks

Few of suggested activities are Assignments, Debates, Poster presentations, Model making, Group presentation, Field visits and Group Discussions.

Few of suggested topics related to **Constitution of India** are:

Debate Topics

- Rights and duties
- Base of Reservation and need

Assignment

- Characteristics of Constitution
- Working of Constitution

COURSE CURRICULUM

Name of the Program:		BSc(Cyber Security)		Semester : III		Level: UG	
Course Name		Foundation of Big data		Course Code/ Course Type		UBS208A/OE	
Course Pattern		Revised 2024		Version		1.0	
Teaching Scheme					Assessment Scheme		
Theory	Practical	Tutorial	Total Credits	Hours	CIA (Continuous Internal Assessment)	ESA (End Semester Assessment)	Practical/Oral
2	-	-	2	-	20	30	-
Prerequisite: Basic Database knowledge.							
Course Objectives (CO):				The objectives of Foundation of Big data are: 1. Remember the basic concepts of Big Data. 2. Explain the different sources of Big Data. 3. Identify the Technologies used for Handling Big Data. 4. Examine the role of Ecosystems used in Big Data. 5. Discuss the role and type of File used in Big Data.			
Course Learning Outcomes (CLO):				Students would be able to: 1. List out the fundamentals of Big Data. 2. Classify the need and sources of Big Data. 3. Illustrate the various technologies for managing Big Data. 4. Analyze the need for the Hadoop ecosystem. 5. Evaluate the different File systems.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction to Big Data: Introduction,Types of Digital Data,Characteristics of Big Data, Evolution of Big Data, Definition of Big Data,Data Appliance, Challenges with Big Data.	CLO 1	6
UNIT II		
Big Data Sources: Introduction,Big data sources,Types of Data Sources,Open Big Data Sources,Importance of Big Data Sources,Big Data sources from various Industries,Challenges associated with Big Data sources.	CLO 2	6
UNIT III		
Technologies for Handling Big Data: Distributed Computing,Parallel Computing, Cloud Computing,Features of Cloud Computing,Cloud Deployment Models.	CLO3	6
UNIT IV		
Understanding Hadoop Ecosystem: Introduction to Hadoop,Hadoop History, Modules of Hadoop,Hadoop Architecture,Advantages of Hadoop.	CLO4	6
UNIT V		
Hadoop Distributed File System: Introduction,HDFS Architecture,Namenodes and Datanodes,Features of HDFS and MapReduce with examples.	CLO5	6
Total Hours		30

Learning resources

Textbooks:

1. Seema Acharya, Subhasini Chellappan, "Big Data Analytics", 2nd Ed., Wiley, 2019
2. Frank J. Ohlhorst, "Big Data and Analytics: Turning Big Data into Big Money", 1st Ed., Wiley and SAS Business Series,
   2013.

Reference Books:

1. BIG DATA, Black Book TM, DreamTech Press, 2016 Edition.
2. Nathan Marz and James Warren, "BIG DATA- Principles and Best Practices of Scalable Real-Time Systems", 2010

Online Resources/E-Learning Resources

1. https://www.knowledgehut.com/blog/big-data/big-data-sources
2. https://scholar.harvard.edu/files/msseo/files/1.introduction_to_bigdata

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester : III**		**Level: UG**	
Course Name		**Introduction to Digital Image Processing**		**Course Code/ Course Type**		**UBS208B/OE**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	-	20	30	-
Prerequisite: Basic Geometry Concepts.							
Course Objectives (CO):				The objectives of Introduction to Digital Image Processing are: 1. Define Image Processing fundamentals. 2. Classify the various properties of perception. 3. Illustrate the different transformation types. 4. Examine image enhancement techniques used in digital image processing. 5. Solve the process of Image degradation by using different models.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify Digital Image Concept and its elements. 2. Explain the various types of image model and its geometry. 3. Execute the Image Processing to transform in various forms. 4. Analyze the need of Image Enhancement in various domains. 5. Evaluate the processes for restoration of Image degradation.			

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Digital Image Processing: Introduction,Image conversion,Working of Digital Image Processing,Image Filtering Techniques,Elements of Digital Image Processing system.	**CLO 1**	**6**
UNIT II		
Visual Perception: Introduction,Properties of Human eye,Image representation, simple image model,Image geometry,Image demosaicing	**CLO 2**	**6**
UNIT III		
Fourier Transform: Introduction,DFT & FFT,Properties of 2D Fourier Transform, Walsh Transform,Hadamard Transform.	**CLO3**	**6**
UNIT IV		
Image Enhancement: Introduction,Enhancement in spatial domain,Enhancement through point operations,Types of point Operations.	**CLO4**	**6**
UNIT V		

Model of Image Degradation: Introduction,Restoration process,Inverse filtering, Singular value decomposition,Recursive filtering.	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

Rafael C Gonzalez, Richard E Woods, "Digital Image Processing" - 2nd Edition, Pearson Education 2003

1. Jain A.K., "Fundamentals of Digital Image Processing", Pearson education

Reference Books:

Millman Sonka, Vaclav Hlavac, Roger Boyle, Broos/Colic, "Image Processing Analysis and Machine VisThompson

Online Resources/E-Learning Resources

1. https://onlinecourses.nptel.ac.in/noc21_ee78
2. https://www.wolfram.com/wolfram-u/courses/image-signal-processing

COURSE CURRICULUM

Name of the Program:		**Foreign Language**		**Semester: III**		**Level: UG**	
Course Name		**German A1.1**		**Course Code/ Course Type**		UFL201A/AEC	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	-	-	-	2	20	30	-
Pre-Requisite:							
Course Objectives (CO):				The objectives of (German A1.1) are: 1. To remember new words and their spellings. 2. To understand the new concepts. 3. To apply the basic vocab and grammar concepts. 4. To understand the German text. 5. To create basic sentences in German.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Spell simple words in German 2. Can understand everyday expressions. 3. Able to frame simple sentences in German language. 4. Can introduce themselves and others. 5. Can answer questions about themselves.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Guten Tag : Speak about yourself and others, Speak about Countries and Languages Grammar – Sentence formation and verbs usage	**CLO 1**	**6**
UNIT II		
Freunde, Kollegen und Ich: Speak about your Hobbys, To fix a meeting, Speak about work and Profession, To create a profile on Internet.Grammar – How to use 'The' in german, Singular and plural forms of Nouns	**CLO 2**	**6**
UNIT III		
In der Stadt: To get to know about Cities and Places, how to find way and understand directions, learn international wordS.Grammar – Negations (how to use NO in German), Definite articles, indefinite articles	**CLO3**	**6**
UNIT IV		
Guten Appetit: To speak about food and food habits, to have a discussion about shopping.Grammar – introduction of cases	**CLO4**	**6**
UNIT V		
Tag für Tag & Zeit mit Freunden Clock timings, To speak about family and friends, Daily routine To speak about free time activity, to understand the specific information from the text, to order and to pay in a restaurant,Grammar – Possessivarticle, Modalverbs, use of on,at,from…till, Seprable verbs and past tence	**CLO5**	**6**
Total		**30 hrs.**

Learning resources

Textbooks:

1. Netzwerk A1, Ernst klett Verlag & Goyal Publishers & Distributors Pvt. Ltd.
2. Studio d A1, Cornelesen Verlag & Goyal Publishers & Distributors Pvt. Ltd.
3. Netzwerk Neu A1, Ernst klett Verlag & Goyal Publishers & Distributors Pvt. Ltd

Reference Books:

1. Hallo Deutsch A1,Ernst Klett Verlag, Goyal Publishers & Distributors Pvt. Ltd
2. Themen Aktuell 1, Hueber verlag
3. Maximal Ernst klett Verlag & Goyal Publishers & Distributors Pvt. Ltd.

Online Resources/E-Learning Resources:

1. Youtube : https://youtube.com/@LearnGermanwithAnja?si=BkJYDPi7TS0fT4lr
2. https://youtube.com/@deutschlernenmitheidi?si=TkICIabzioaU0roZ

Instagram : instagram.com/learngermanwithanja

COURSE CURRICULUM

Name of the Program:		**B.Sc(Cyber Security)**		**Semester: III**		**Level: UG/PG**	
Course Name		Basic Japanese language skill		**Course Code/Course Type**		UFL201B/AEC	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
2	--	--	2	30	50	--	--
Pre-Requisite: Desire to get acquainted with the Japanese language.							
Course Objectives (CO):				The objectives of Basic Japanese language skill are: 1. To meet the needs of ever-growing industry, with respect to language support. 2. To get introduced to Japanese society and culture through language. 3. To acquire competitive edge in career choices. 4. To participate effectively & responsibly in a multi-cultural world. 5. To enable learners to communicate effectively in Japanese language.			
Course Learning Outcomes (CLO):				After learning the course, the students will be able to: 1. Read and Write Hiragana script. 2. Write and speak basic sentences. 3. Comprehend and speak about time, hobbies, likes and dislikes. 4. Write basic kanji. 5. Use the Hiragana script in discussion.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction to Japanese Language – roduction of script, culture, History of script ,Speaking : Self introduction, listening : short video skit on self-introduction	**CLO 1**	**6**
UNIT II		
Introduction of Hiragana Script - Writing : Hiragana script, Speak : Basic sentences, General vocabulary : Months , Days of the week ,Basic numbers, colours	**CLO 2**	**6**
UNIT III		
Basic Sentence formation - sic sentence structure: Affirmative and Negative, General vocabulary: about family.	**CLO 3**	**6**
UNIT IV		
Time and verbs – Speaking: Talking about routine, Writing: routine using verbs and time, reading : A clock.	**CLO 4**	**6**
UNIT V		
Introduction of Katakana and basic kanji – Reading : English words, country names Writing : Basic Kanji	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Textbook:

1. Minna no Nihongo , " Japanese for everyone" ,Elementary Main Textbook , Goyal Publishers & Distributors Pvt. Ltd.

Reference books:

1. Shyoho Volume 1.
2. Genki Japan
3. Haru Vol. 1 & 2

Online Resources/E-Learning Resources:

1. U Tube links

https://www.youtube.com/watch?v=shdlEapDsP4

https://youtu.be/K-nw5EUxDz0?feature=shared

https://youtu.be/o9sP-vaCEa0?si=l8yOvVKaItBQWXNu

https://youtu.be/JnoZE51WZg4?si=9uq68USOz5plBk2n

https://youtu.be/shdlEapDsP4?si=tC6RGaMtwDJgVu2d

https://youtu.be/9paXgC2U8L0?si=btS1G4mvrkG5C9zi

2. Apps

A) Learn Japanese - Hiragana APP available on Google play.

B) Hiragana Pro

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester - IV

COURSE CURRICULUM

Name of the Program:		BSc(Cyber Security)		Semester :IV		Level: UG	
Course Name		**Operating Systems-Linux**		**Course Code/ Course Type**		**UBS209/MAJM**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basic knowledge of Operating System							
Course Objectives (CO):				The objectives of Web Application Security are: 1. Recognize the principles of Linux operating system 2. Illustrate the fundamentals of Shell, Pipes and Filters. 3. Identify the different types of operations performed in the unix file system. 4. Examine the Inter process communication used in Linux. 5. Discuss semaphore and shared memory concept.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define various Linux commands that are used to manipulate system operations. 2. Explain Shell Programming using Linux commands. 3. Execute the application to manipulate the internal kernel level Linux File System. 4. Categorize various processes for synchronization. 5. Ability to develop applications to make efficient use of resources			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction To Linux and Linux Utilities: A brief history of Linux, Architecture of Linux, Features of Linux, introduction to vi editor, Linux commands, PATH, man, echo, printf, script, passwd,uname,who,date,stty,pwd, cd,mkdir,rmdir,ls,cp,mv,rm,cat,more,wc,lp,od,tar,gzip,file handling utilities, security by file permissions, process utilities, disk utilities, networking commands	**CLO 1**	**9**
UNIT II		
Introduction to Shells: Linux Session, Standard Streams,Redirection,Pipes,Tee Command, Command Execution,Command Line Editing,Quotes,Command Substitution, Job Control,Aliases,Variables,Predefined Variables,Options,Shell Environment Customization,Filters,Filters and Pipes,Concatenating files,Display Beginning and End of files,Cut and Paste,Sorting,Translating Characters,Files with Duplicate Lines,Count Characters,Words or Lines,Comparing Files.	**CLO 2**	**9**
UNIT III		
Grep: Introduction,Operation,grep Family,Searching for File Content,Sed Scripts, Operation,Addresses,commands,Applications,grep and sed,Unix File Structure,Introduction to Unix file system,inode,file descriptors, system calls and device drivers,File Management,File Structures,System Calls for File Management,create,open,close,read,write,lseek,link,symlink	**CLO3**	**9**
UNIT IV		

Process and Signals: Introduction,Process,process identifiers,process structure,process table,viewing processes,system processes,process scheduling,starting new processes,waiting for a process,zombie processes,orphan process,fork,vfork,exit,wait,waitpid,unreliable signals,interrupted system calls,kill, raise,alarm,pause,abort,system,sleep functions,signal sets.	**CLO4**	**9**
UNIT V		
Inter Process Communication: Pipe,process pipes,the pipe call,parent and child processes and named pipes,fifos,semaphores,semget,semop,semctl,message queues,msgget,msgsnd,msgrcv,msgctl,shared memory,shmget,shmat,shmdt,shmctl.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. W. Richard. Stevens (2005), Advanced Programming in the UNIX Environment, 3rd edition, Pearson Education, New Delhi, India.
2. Unix and shell Programming Behrouz A. Forouzan, Richard F. Gilberg.Thomson

Reference Books:

1. Linux System Programming, Robert Love, O'Reilly, SPD.
2. Advanced Programming in the UNIX environment, 2nd Edition, W.R.Stevens, Pearson Education.

Online Resources/E-Learning Resources

1. https://www.coursera.org/learn/linux-fundamentals
2. https://linuxsimply.com/

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester: IV**		**Level: UG**	
Course Name		**Operating System Lab**		**Course Code/ Course Type**		UBS210/MAJM	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
-	1	-	1	2	25	-	25
Prerequisite: Basic Knowledge is required.							
Course Objectives (CO):				The objectives of using Operating System: - 1. To Understand the basic Unix Commands. 2. To apply Shell Programming. 3. To analyze Process and thread creation and termination. 4. To evaluate the CPU Scheduling. 5. To Design various synchronization mechanisms.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Understand and identify the implementation of Unix Commands. 2. Explain the shell programming. 3. Apply knowledge of processes and threads. 4. Analyze the mechanism of CPU scheduling. 5. Evaluate the synchronization mechanism.			

Course Contents/Syllabus: Practical Plan

Activity Number	Assignment/Practical/Activity Title	Week Number/Turn	Details	CLO	Hours
1	Basics of UNIX commands	Week 1	Time and Date commands Getting help in Unix Unix Shell Commands	CLO1	2
2	UNIX commands	Week 2	Unix users commands Unix file operations Text file operations in Unix Unix directory management commands	CLO1	2
3	UNIX commands	Week 3	Networking commands in Unix Process management File transfers commands	CLO1	2
4	Shell Programming	Week 4	Write a shell program to add two numbers. write a shell program to find a number is even or odd.	CLO1, CLO2	2
5	Shell Programming	Week 5	Write a shell program for fibonacci series	CLO2	2
6	Process and thread	Week 6	program for process creation and termination	CLO2	2
7	Process and thread	Week 7	program for thread creation and termination	CLO3	2
8	CPU Scheduling	Week 8	First Come First Serve (FCFS)	CLO3	2
9	CPU Scheduling	Week 9	Shortest Job First (SJF)	CLO3	2
10	synchronization.	Week 10	Producer-Consumer Problem	CLO4	2
11	synchronization	Week 11	Reader Process	CLO4, CLO5	2
12	Deadlock Prevention	Week 12	Eliminate Hold and wait Eliminate Circular Wait	CLO5	2
13	Deadlock	Week 13	Bankers algorithm	CLO5	2
14	Memory Management	Week 14	Implementation of Memory Management Algorithm Best Fit,	CLO5	2

15	Memory Management	Week 15	Implementation of Memory Management Algorithm Worst Fit	CLO5	2
Total					**30 hrs.**

Learning resources

Textbooks:

1. The Linux Programming Interface: A Linux and UNIX System Programming by Michael Kerrisk
2. How Linux Works: What Every Superuser Should Know by Brian Ward

Reference Books:

1. Linux Pocket Guide by Daniel J. Barrett Publisher O'Reilly Media
2. Linux for Beginners by Jason Cannon

Online Resources/E-Learning Resources

1. https://linuxsimply.com/
2. https://www.coursera.org/specializations/unix-and-bash-for-beginners

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester: IV**		**Level: UG**	
Course Name		**Mobile Security**		**Course Code/ Course Type**		**UBS211/MAJM**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basic knowledge of Security.							
Course Objectives (CO):				The objectives of Mobile Security are: 1. Recognize the Importance of Security in Mobile devices. 2. Classify security Issues associated with Mobile communication. 3. Categorize the levels of security needed in cellular networks. 4. Analyze the security attacks on MANETs 5. Visualize various issues of application-level security in wireless environment.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the requirement of security and various issues at wireless and mobile network. 2. Explain the threats in the wireless environment including device, networks and servers. 3. Assess the security requirement for mobile adhoc environment 4. Recognize the attacks in various environment and Report consequences of them 5. Select an appropriate solution for security measures and countermeasures.			

Course Contents/Syllabus

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Mobile Security: Introduction,Importance of Mobile Security,Threats,Components of Mobile Device Security,Types of Mobile threats,Types of Mobile Device Security,Building Blocks of Mobile security and cryptographic techniques.	**CLO 1**	**9**
UNIT II		
Security Issues in Mobile Communication: Mobile Communication History, Security Wired Vs Wireless,Security Issues in Wireless and Mobile Communication,Mobile Devices Security Requirements,Mobile Wireless network level Security, Server Level Security.	**CLO 2**	**9**
UNIT III		
Security levels in Cellular Networks: Application Level Security in Wireless Networks,Wireless Threats,Recent Security Schemes for Wi-Fi Applications,Generations of Cellular Networks,Security Issues and attacks in cellular networks, GSM,5G security for applications.	**CLO3**	**9**
UNIT IV		
Application Level Security in MANETs:MANETs Introduction,Applications of MANETs, MANET Features,Security Challenges in MANETs,Security Attacks on MANETs.	**CLO4**	**9**
UNIT V		
Wireless Sensor Network Security: Attacks on wireless sensor networks and counter measures,Prevention mechanisms,Authentication and traffic protection, centralized and passive intruder detection,Decentralized intrusion detection.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Pallapa Venkataram, Satish Babu, Wireless and Mobile Network Security, First Edition, Tata McGraw Hill,2010
2. Hakima Chaouchi, Maryline Laurent-Maknavicius, Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies, Wiley,2009

Reference Books:

1. Tara M.Swaminathan and Charles R. Eldon,Wireless Security and Privacy- Best Practices and Design Techniques, Addison Wesley, 2002.
2. Mobile Security and Privacy by Man Ho Au,Raymond Choo Syngress Publications

Online Resources/E-Learning Resources

1. https://www.cisa.gov/resources-tools/resources/
2. https://ocw.mit.edu/courses/6-858-computer-systems-security

COURSE CURRICULUM

Name of the Program:		**BSc (Cyber Security)**		**Semester:IV**		**Level: UG**	
Course Name		**Mobile Security Lab**		**Course Code/ Course Type**		UBS212/MAJM	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
-	1	-	1	2	25	-	25
Prerequisite: Basic Knowledge is required.							
Course Objectives (CO):				The objectives of using Operating System: - 1. To Identify the basic Components of Mobile phones. 2. Classify the Components of GSM Network. 3. Illustrate the need for RFID technology. 4. To Examine the selection of the network. 5. Integrate the parts of a mobile.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Understand and identify the basic components of mobile devices. 2. Explain the components of mobile phone and GSM network. 3. Illustrate the need for having RFID technology in mobile. 4. Analyze the use of wireless technology for enhancing network connectivity. 5. Evaluate the need for wireless and network connectivity for real life applications.			

Course Contents/Syllabus: Practical Plan

Activity Number	Assignment/Practical/Activity Title	Week Number/Turn	Details	CLO	Hours
1	Identify the components of a mobile phone.	Week 1	Test the different sections of mobile phone (such as Ringer section, dialer section)	CLO1	2
2	Components of mobile phone	Week 2	Test the different sections receiver section and transmitter section)	CLO1	2
3	Identify the component of GSM Network	Week 3	Perform the process of call connection	CLO1	2
4	Identify the component of GSM Network	Week 4	Call release of cellular Mobile system.	CLO1, CLO2	2
5	Transfer an Image	Week 5	Transfer an image, audio and video file using Bluetooth protocol with varying distance between two devices and analyze the performance	CLO2	2
6	Wi-Fi setting	Week 6	Configure Wi-Fi setting in mobile devices using mobile tethering to connect two devices such as mobile phone to mobile phone.	CLO2	2
7	RFID technology	Week 7	Apply RFID technology for real life applications using RFID kit.	CLO3	2
8	Wireless connectivity	Week 8	Establish seamless wireless connectivity using single access point	CLO3	2
9	Check network availability	Week 9	Check network availability manual and auto selection of network using AT commands in mobile.	CLO3	2
10	Check network availability	Week 10	Auto Selection of Network	CLO4	2
11	Direct sequence spread	Week 11	Simulate the Direct sequence spread.	CLO4, CLO5	2
12	Wireless connectivity	Week 12	Establish seamless wireless connectivity	CLO5	2

			using multiple access point		
13	Wi-Fi setting	Week 13	Configure Wi-Fi setting in mobile devices using mobile tethering to connect two devices such as phone to laptop.	CLO5	2
14	Wireless connectivity	Week 14	Authenticate Wireless Connectivity by using password	CLO5	2
15	Check network availability	Week 15	Network Availability Checking usage	CLO5	2
Total					**30 hrs.**

Learning resources

Textbooks:

1. Pallapa Venkataram, Satish Babu, Wireless and Mobile Network Security, First Edition, Tata McGraw Hill,2010
2. Hakima Chaouchi, Maryline Laurent-Maknavicius, Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies, Wiley,2009

Reference Books:

1. Tara M.Swaminathan and Charles R. Eldon,Wireless Security and Privacy- Best Practices and Design Techniques, Addison Wesley, 2002.
2. Mobile Security and Privacy by Man Ho Au,Raymond Choo Syngress Publications

Online Resources/E-Learning Resources

1. https://www.cisa.gov/resources-tools/resources/
2. https://ocw.mit.edu/courses/6-858-computer-systems-security

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester : IV**		**Level: UG**	
Course Name		**Cyber laws & Security Policies**		**Course Code/ Course Type**		**UBS213A/MAJE**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basic Knowledge of security.							
Course Objectives (CO):				The objectives of Cyber laws & Security Policies are: 1. Identify the practical aspects of Cyber Law and Security. 2. Compare the different types of security breaches and frauds. 3. Categorize various emerging trends in Cyber Law jurisprudence. 4. Examine the various provisions that have in place for cyber crimes and other aspects of Cyber Law. 5. Discuss the legal ramifications of different activities on the World Wide Web.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Define cyber security, cyber law and their roles. 2. Demonstrate cybersecurity, cybercrime and forensics. 3. Infer legal issues in cybercrime, 4. Demonstrate tools and methods used in cybercrime and security. 5. Illustrate evidence collection and legal challenges.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Cybercrime: Definition and Origins of the Word,Cybercrime and Information Security,Classifications of Cybercrimes,The Legal Perspectives, Cybercrimes:An Indian Perspective,Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes,Cybercrime Era,Survival Mantra for the Netizens, Cyber Offenses.	**CLO 1**	**9**
UNIT II		
Cybercrime: Mobile and Wireless Devices,Proliferation of Mobile and Wireless Devices,Trends in Mobility,Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices,Registry Settings for Mobile Devices,Authentication Service Security,Attacks on Mobile and Cell Phones.	**CLO 2**	**9**
UNIT III		
Tools and Methods Used in Cybercrime: Introduction,Proxy Servers and Anonymizers,Phishing,Password Cracking,Keyloggers and Spywares,Virus and Worms,Trojan Horses and Backdoors,Steganography,DoS and DDoS Attacks,SQL Injection,Buffer Overflow,Attacks on Wireless Networks,Phishing and Identity Theft,Phishing,Identity Theft (ID Theft).	**CLO3**	**9**
UNIT IV		

Understanding Computer Forensics: Introduction,Historical Background of Cyberforensics,Digital Forensics Science, The Need for Computer Forensics,Cyberforensics and Digital Evidence,Forensics Analysis of E-Mail,Digital Forensics Life Cycle,Chain of Custody Concept, Network Forensics,Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing.	**CLO4**	**9**
UNIT V		
Introduction to Security Policies and Cyber Laws: Need for An Information Security Policy,Information Security Standards,Introducing Various Security Policies and Their Review Process,Introduction to Indian Cyber Law,Objective and Scope of the IT Act 2000,Intellectual Property Issues.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives SunitBelapure and Nina Godbole Wiley India Pvt Ltd 2013
2. Introduction to information security and cyber laws Surya PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla Dreamtech Press 2015

Reference Books:

1. Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions Thomas J. Mowbray John Wiley & Sons,
2. Cyber Security Essentials James Graham, Ryan Olson, Rick Howard CRC Press 2010

Online Resources/E-Learning Resources

1. https://onlinecourses.swayam2.ac.in/
2. https://www.javatpoint.com/cyber-security-policies

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester : IV**		**Level: UG**	
Course Name		**Cyber Threat Intelligence**		**Course Code/ Course Type**		**UBS213B/MAJM**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	-	40	60	-
Prerequisite:Basic Knowledge of security.							
Course Objectives (CO):				The objectives of Cyber threat Intelligence are: 1. Learn the foundations of Cyber Security and threat landscape 2. To equip students with the technical knowledge and skills needed to protect and defend against cyber threats. 3. Illustrate the different cyber security mechanisms to ensure the protection of information technology assets. 4. Examine the different social and ethical contexts of Cyber Security. 5. Simplify the cybercrimes and threats with solutions in a global and societal context.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Understand the Cyber Security threat landscape. 2. Explain the various types of cyberattacks, cybercrimes, vulnerabilities. 3. Illustrate the existing legal framework and laws on Cyber Security. 4. Analyze and evaluate the importance of personal data its privacy and security. 5. Plan the awareness about cyber-attack vectors and safety against cyber-frauds.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Overview of Cyber Security: Cyber Security increasing threat Landscape,Cyber Security terminologies,Cyberspace,attack,attack vector,attack surface,threat,risk, vulnerability,exploit,exploitation,Hacker,Non-state actors,Cyber terrorism, Protection of end user machine.	**CLO 1**	**9**
UNIT II		
CyberCrimes: Cyber Crimes Targeting Computer systems,Data diddling attacks,spyware,logicbombs,DoS,DDoS,APTs,virus,Trojans,Ransomware, Data breach,Online scams and frauds,email scams,Phishing,Vishing, Smishing,Online job fraud,Online sextortion,Debit/credit card fraud, Online payment fraud,Cyberbullying,website defacement,Cyber-squatting,Pharming,Cyber espionage,Cryptojacking, Darknet- illegal trades,drug trafficking, human trafficking.	**CLO 2**	**9**
UNIT III		

Cyber Law: Cybercrime and legal landscape around the world, IT Act,2000 and its amendments. Limitations of IT Act,2000,Cybercrime and punishments, Cyber Laws and Legal and ethical aspects related to new technologiesAI/ML,IoT, Blockchain, Darknet and Social media.	**CLO3**	**9**
UNIT IV		
Data Privacy and Data Security: Defining data,meta-data,big data,non personal data.Data protection,Data privacy and data security, Personal data protection bill and its compliance, Data protection principles, Big data security issues and challenges.	**CLO4**	**9**
UNIT V		
Cyber Security Management, Compliance and Governance: Cyber Security Plan,Cyber Security policy, cyber crises management plan,Business continuity, Risk assessment,Types of security controls and their goals, Cyber Security audit and compliance,National Cyber Security policy and strategy.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Cyber Crime Impact in the New Millennium, by Marine R.C,Author Press.
2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.

Reference Books:

1. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.
2. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.

Online Resources/E-Learning Resources

1. https://onlinecourses.swayam2.ac.in/
2. https://www.javatpoint.com/cyber-security-policies

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester: IV**		**Level: UG**	
Course Name		**Data Privacy**		**Course Code/ Course Type**		**UBS214/SEC**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	-	20	30	-
Prerequisite: Basic knowledge of Operating System							
Course Objectives (CO):				The objectives of Data Privacy are: 1. Describe the Need for Data Privacy. 2. Illustrate the challenges of Data Privacy and Data Security. 3. Identify the concepts and components of CIP. 4. Examine the complexity, and criticality interdependencies within the CIP. 5. Discuss the various measures for avoiding disaster.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the evolving threats in data security. 2. Explain how data privacy can prevent the critical infrastructure. 3. Apply knowledge for determining critical infrastructure for data privacy. 4. Analyze the need for essential security mechanisms. 5. Evaluate the different information security threats.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Data Privacy: Introduction,Importance,Laws that govern data privacy,Fair Information Practices,Challenges,Technologies used for Data Privacy,Importance of backup and Recovery,Physical data security.	**CLO 1**	**6**
UNIT II		
Critical infrastructure Risk Management Framework: General policy frameworks for the protection of critical infrastructure,Security goals,identify assets,networks and functions,asset risk,prioritize,effective measures	**CLO 2**	**6**
UNIT III		
Critical Infrastructure Risk in the Context of National Preparedness: Law enforcement and crime prevention,counter terrorism,national security and defense,emergency management,including the dissemination of information,business continuity planning,protective security (physical, personnel and procedural),e-security.	**CLO3**	**6**
UNIT IV		
Physical security essentials: Physical security threats,physical security prevention and mitigation measures,recovery from physical security breaches, threat assessment,planning and implementation.	**CLO4**	**6**
UNIT V		
Public information and media management: Identification of Critical Infrastructure,Disaster recovery,Measuring risk and avoiding disaster, The business impact assessment.	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. Collins, Pamela A., and Ryan K. Baggett. Homeland security and critical infrastructure protection. Praeger Security International, 2009.
2. Anil K Jain, Patrick Flynn, Arun A Ross, Handbook of Biometrics, Springer, 2008 3.Vacca, John R.Cyber security and IT infrastructure protection. Syngress, 2013

Reference Books:

1. Practical Data Privacy by Katharine Jarmul Publisher O'Reilly Media, Inc.
2. Practical Data Privacy: Enhancing Privacy and Security in Data (Grayscale Indian Edition) by Katharine Jarmul

Online Resources/E-Learning Resources

1. https://www.cloudflare.com/learning/privacy/what-is-data-privacy/
2. https://www.grantthornton.global/en/insights/

COURSE CURRICULUM

Name of the Program:		**B.Sc(Cyber Security)**		**Semester :IV**		**Level: UG**	
Course Name		**Constitution of India**		**Course Code/ Course Type**		**ACCOI201/AC**	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA** **(Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical /Oral**
2	-	-	-	2	50	-	-
Pre-Requisite: Basic Knowledge of Constitution.							
Course Objectives (CO):				The objectives of Constitution of India are: 1. To familiarize the students with the key elements of the Indian constitution. 2. To enable students to grasp the constitutional provisions and values. 3. To acquaint the students with the powers and functions of various constitutional offices and institutions. 4. To make students understand the basic premises of Indian politics. 5. To make students understand the role of constitution and citizen-oriented measures in a democracy			
Course Learning Outcomes (CLO):				Students would be able to: 1. Analyze the basic structure of Indian Constitution. 2. Remember their Fundamental Rights, DPSP's and Fundamental Duties (FD's) of our constitution. 3. know about our Union Government, political structure & codes, procedures. 4. Understand our State Executive & Elections system of India. 5. Access the Amendments and Emergency Provisions, other important provisions given by the constitution			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Indian Constitution: The Necessity of the Constitution, The Societies before and after the Constitution adoption. Introduction to the Indian constitution, The Making of the Constitution, The Role of the Constituent Assembly. The Preamble of Indian Constitution & Key concepts of the Preamble. Salient features of India Constitution.	**CLO 1**	**6**
UNIT II		
FR's, FD's and DPSP's: Fundamental Rights and its Restriction and limitations in different Complex Situations. Directive Principles of State Policy (DPSP) and its present relevance in our society with examples. Fundamental Duties and its Scope and significance in Nation building	**CLO 2**	**6**
UNIT III		
Governance and Constitution: Federalism in India - Features, Local Government -Panchayats –Powers and functions; 73rd and 74th amendments, Election Commission – Composition, Powers and Functions; Electoral Reforms, Citizen oriented measures – RTI and PIL – Provisions and significance..	**CLO 3**	**6**
UNIT IV		
Union Executive: Parliamentary System, Union Executive – President, Prime Minister, Union Cabinet, Parliament - LS and RS, Parliamentary Committees, Important Parliamentary Terminologies. Supreme Court of India, Judicial Reviews and Judicial Activism.	**CLO 4**	**6**
UNIT V		

State Executive & Elections, Amendments and Emergency Provisions: State Executive, Election Commission, Elections & Electoral Process. Amendment to Constitution (How and Why) and Important Constitutional Amendments till today. Emergency Provisions.	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Text Books

1. "Constitution of India" (for Competitive Exams) - Published by Naidhruva Edutech Learning Solutions, Bengaluru. – 2022.
2. "Engineering Ethics", M.Govindarajan, S.Natarajan, V.S.Senthilkumar, Prentice –Hall, 2004

Reference Books:

1. "SamvidhanaOdu" - for Students & Youths by Justice HN NagamohanDhas, Sahayana, kerekon.
2. "Constitution of India, Professional Ethics and Human Rights" by Shubham Singles, Charles E. Haries, and et al: published by Cengage Learning India, Latest Edition – 2019.
3. "Introduction to the Constitution of India", (Students Edition.) by Durga Das Basu (DD Basu): Prentice –Hall, 2008.
4. "The Constitution of India" by Merunandan K B: published by Merugu Publication, Second Edition, Bengaluru.

CIA Guidelines

CIA Guidelines

Online Quiz (Based on MCQ)- 20 marks

Activity (with short Report Submission) - 20 Marks

Academic Sincerity - 10 marks

Few of suggested activities are Assignments, Debates, Poster presentations, Model making, Group presentation, Field visits and Group Discussions.

Few of suggested topics related to **Constitution of India** are:

Debate Topics

- Rights and duties
- Base of Reservation and need

Assignment

- Characteristics of Constitution
- Working of Constitution

COURSE CURRICULUM

Name of the Program:		**B.Sc(Cyber Security)**		**Semester: IV**		**Level: UG**	
Course Name		**UHV-II: Understanding Harmony**		**Course Code/ Course Type**		**ACUHV201/AC**	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	-	2	50	-	-
Pre-Requisite:							
Course Objectives (CO):				The objectives of Universal Human Value- Understanding Harmony are: 1. To train the student for Development of a holistic perspective based on self-exploration about themselves (human being), family, society and nature/existence. 2. To comprehend (or develop clarity) the harmony in the human being, family, society and nature/existence 3. To strengthen self-reflection. 4. To infuse a sense of commitment and courage to act 5. To understand Holistic Understanding of Harmony on Professional Ethics			
Course Learning Outcomes (CLO):				Students would be able to: 1. Analyze the most important requirement for any human being 2. Apply correct appraisal of Physical needs, meaning of Prosperity in detail 3. Analyze salient values in relationship, Friends and Foes, Empathy, False Prestige. 4. Develop holistic perception of harmony at all levels of existence 5. Apply the Holistic Understanding of Harmony on Professional Ethics.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Course Introduction - Need, Basic Guidelines, Content and Process for Value Education Purpose and motivation for the course, recapitulation from Universal Human Values-I, Self-Exploration–what is it? - Its content and process; Personality Traits- Self Excellence, „Natural Acceptance‟ and Experiential Validation- as the process for self-exploration, Adaptability, Belief and Understanding- Self discipline, Continuous Happiness and Prosperity- A look at basic Human Aspirations, Right understanding, Relationship and Physical Facility- the basic requirements for fulfilment of aspirations of every human being with their correct priority, Understanding Happiness and Prosperity correctly- A critical appraisal of the current scenario, Method to fulfil the above human aspirations: understanding and living in harmony at various levels.	**CLO 1**	**6**
UNIT II		
Understanding Harmony in the Human Being - Harmony in Myself: Understanding human being as a co-existence of the sentient „I‟ and the material „Body‟, Understanding the needs of Self („I‟) and „Body‟ - happiness and physical facility, Understanding the Body as an instrument of „I‟ (I being the doer, seer and enjoyer)- Habits and Hobbies, SWOT Analysis (Activity) ,Understanding the characteristics and activities of „I‟ and harmony in „I‟ – Dalai Lamas‟ Tibetan Personality Test – Dr. Menninger‟s Psychometric Test., Understanding the harmony of I with the Body: Sanyam and Health; correct appraisal of Physical needs, meaning of Prosperity in detail	**CLO 2**	**6**
UNIT III		
Understanding Harmony in the Family and Society- Harmony in Human-Human Relationship: Understanding values in human-human relationship; meaning of Justice (nine universal values in	**CLO 3**	**6**

relationships) and program for its fulfilment to ensure mutual happiness; Trust and Respect as the foundational values of relationship, Understanding the meaning of Trust; Difference between intention and competence, Understanding the meaning of Respect, Difference between respect and differentiation; the other salient values in relationship, Friends and Foes, Empathy, False Prestige.		
UNIT IV		
Understanding Harmony in the Nature and Existence - Whole existence as Coexistence: Understanding the harmony in the Nature and its Equanimity, Respect for all, Nature as Teacher, Interconnectedness and mutual fulfillment among the four orders of nature- recyclability and self-regulation in nature, Understanding Existence as Co-existence of mutually interacting units in all- pervasive space, Holistic perception of harmony at all levels of existence.	**CLO 4**	**6**
UNIT V		
Implications of the above Holistic Understanding of Harmony on Professional Ethics: Natural acceptance of human values, Definitiveness of Ethical Human Conduct, Basis for Humanistic Education, Humanistic Constitution and Humanistic Universal Order, Vision for the Holistic alternatives, UHVs for entrepreneurship	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. _Human Values and Professional Ethics by R R Gaur, R Sangal, G P Bagaria, Excel Books, New Delhi, 2010
2. Jeevan Vidya: Ek Parichaya, A Nagaraj, Jeevan Vidya Prakashan, Amarkantak, 1999.
3. Human Values, A.N. Tripathi, New Age Intl. Publishers, New Delhi, 2004.

Reference Books:

1. The Story of Stuff (Book).
2. The Story of My Experiments with Truth - by Mohandas Karamchand Gandhi
3. Small is Beautiful - E. F Schumacher
4. Slow is Beautiful - Cecile Andrews

Online Resources/E-Learning Resources

https://www.studocu.com/in/document/jss-science-and-technology-university/human-values/uhv-handout-2-harmony-in-the-human-being/

https://vvce.ac.in/wp-content/uploads/2021/04/Realising-Aspirations-of-NEP2020-UHV.pdf

https://vemu.org/uploads/lecture_notes/22_12_2022_1850871704.pdf

CIA Guidelines

Online Quiz (Based on MCQ)- 20 marks

Activity (with short Report Submission) - 20 Marks

Academic Sincerity - 10 marks

Few of suggested activities are Assignments, Debates, Poster presentations, Model making, Group presentation, Field visits and Group Discussions.

Few of suggested topics related to UHVII-Understand Harmony are:

Debate Topics

- Materialistic things make you happy
- Happiness in individualism and family

Spirituality vs Materialistic

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester : IV**		**Level: UG**	
Course Name		**Search Engine Optimization**		**Course Code/ Course Type**		**UBS216A/OE**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	-	20	30	-
Prerequisite: Basic Knowledge of Web is required.							
Course Objectives (CO):				The objectives of Search Engine Optimization are: 1. Remember the basics of Google search and other search engines. 2. Illustrate the various types of SEO's 3. Identify the Importance of Technical SEO. 4. Examine the role of Keyword research for various types of search techniques. 5. Discuss On-page and off-page optimization.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the various types of SEO's. 2. Explain the types of tags associated with optimization of technical SEO. 3. Apply knowledge of SEO for competitive analysis on a webpage. 4. Analyze the data to see which content gets the most shares. 5. Create a report of findings and recommendations for SEO.			

Course Contents/Syllabus

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Search Engine Optimization: Introduction,Working of SEO,Need for SEO,History for SEO,Google Crawler,Types Of SEO technique,Google's SEO Algorithm,strategies for SEO,SEO tools and why we need it.	**CLO 1**	**6**
UNIT II		
Technical SEO: Technical SEO,Type of meta tags and their effect on SEO,Site architecture Optimization,Breadcrumbs,Permalinks optimization,canonicalization, Fixing Broken Links and Errors.	**CLO 2**	**6**
UNIT III		
Keyword Research: Introduction,Importance of Keyword Research,Different types of keywords,Analysis of keywords using Free & Paid Tools,Keywords related to your website and business,Analysis of Keyword Using Chrome Extension.	**CLO3**	**6**
UNIT IV		
Content Planning and Creation: Content Research,Content Structure,Content Planning With Keywords,How to make SEO friendly content using AI tools	**CLO4**	**6**
UNIT V		

On Page SEO: On page SEO checklist,Title Optimization,Content optimization, Cases to be discussed.	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. SEO For Beginners: An Introduction To SEO Basics
2. Entity SEO: Moving from Strings to Things

Reference Books:

1. Search Engine Optimization by Andreas Veglis,Dimitrios Giomelakis
2. SEO For Beginners: An Introduction To SEO Basics.

Online Resources/E-Learning Resources

1. https://mdpi-res.com/bookfiles/book/3418/Search_Engine_Optimization.pdf?v=1713229263
2. https://ahrefs.com/

COURSE CURRICULUM

Name of the Program:		**BSc(Cyber Security)**		**Semester: IV**		**Level: UG**	
Course Name		**Introduction to WordPress**		**Course Code/ Course Type**		**UBS216B/OE**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	-	20	30	-
Prerequisite: Basic Knowledge of Web is required.							
Course Objectives (CO):				The objectives of Introduction to WordPress are: 1. Remember the basics of CMS. 2. To Recognize the need for WordPress. 3. Identify the types of themes in WordPress. 4. Analyze the working of widgets for creating a website. 5. Creating a Webpage by adding Widgets along with Content.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Identify the need for having a CMS. 2. Explain the different types of tools available for creating a CMS. 3. Demonstrate the working of themes in a web page. 4. Integrate the themes, Widgets and Content for creating a web page. 5. Create a Web page by adding widgets and plugins.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Content Management System: Introduction,ECM,WCM,Components of CMS, Features of CMS,Advantages,Disadvantages,Cases.	**CLO 1**	**6**
UNIT II		
WordPress: Introduction,Features,WordPress Advantages,Wordpress.org, WordPress.com,WordPress Admin,Creating Users,User Rights & Roles.	**CLO 2**	**6**
UNIT III		
Themes: Free Theme Vs Paid Theme,Theme Selection Process,Adding/installing Themes,Changing Themes,Preview & Activating Themes	**CLO3**	**6**
UNIT IV		
Working with Widgets: Installing widgets in sidebar,Installing widgets in footer Creating menus,Activating Plugin & managing plugins,Upgrading plugins	**CLO4**	**6**
UNIT V		
Working with Content: Posts Vs Pages,Adding Hyperlinks,Playing with Media content,Previewing and Editing Posts,Previewing and Editing Pages.	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. WordPress For Dummies by Lisa Sabin-Wilson
2. Professional WordPress: Design and Development by Brad Williams, David Damstra, and Hal Stern

Reference Books:

1. Teach Yourself VISUALLY WordPress by George Plumley.
2. Professional WordPress: Design and Development by Brad Williams, David Damstra, and Hal Stern

Online Resources/E-Learning Resources

1. https://www.slainstitute.com/
2. https://www.wpbeginner.com/beginners-guide/beginners-guide-on-how-to-add-a-link-in-wordpress/

COURSE CURRICULUM

Name of the Program:		**B.Sc.(Cyber Security)**		**Semester: IV**		**Level: UG**	
Course Name		**Japanese language skill - L2**		**Course Code/Course Type**		UFL201B/AEC	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	--	--	2	2	20	30	--
Pre-Requisite: Desire to get acquainted with the Japanese language. Basic knowledge of Hiragana and							
Course Objectives (CO):				The objectives of Basic Japanese language skill are: 1. To meet the needs of ever-growing industry, with respect to language support. 2. To get introduced to Japanese society and culture through language. 3. To promote multilingualism in exposing students to different cultures 4. Fostering respect for linguistic diversity. 5. Learning additional language to develop a better memory, talent for problem solving, ability to concentrate.			
Course Learning Outcomes (CLO):				After learning the course, the students will be able to: 1. Read & write words that have been borrowed from other language. 2. Comprehend and speak basic conversation with basic particles 3. Speak and write about Routine. 4. Basic sentence patterns incorporated into short dialogues indicating how they are used in actual conversation. 5. To understand grammatical structure, and improve communication abilities.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Japanese Language: Introduction of script, culture, History of script ,Speaking : Self introduction, listening : short video skit on self-introduction	**CLO 1**	**6**
UNIT II		
Introduction of Hiragana Script: Writing, Hiragana script, Speak : Basic sentences, General vocabulary : Months , Days of the week ,Basic numbers, colours	**CLO 2**	**6**
UNIT III		
Basic Sentence formation: Basic sentence structure:Affirmative and Negative , General vocabulary: about family.	**CLO 3**	**6**
UNIT IV		

Time and verbs: Speaking: Talking about routine, Writing: routine using verbs and time, reading : A clock	**CLO 4**	**6**
UNIT V		
Introduction of Katakana and basic kanji –Reading : English words, country names,Writing : Basic Kanji	**CLO 5**	**6**
Total Hours		**30**

Learning resources

Textbook:

1. Minna no Nihongo , " Japanese for everyone" ,Elementary Main Textbook , Goyal Publishers & Distributors Pvt. Ltd.

Reference books:

1. Shyoho Volume 1.
2. Genki Japan
3. Haru Vol. 1 & 2

Online Resources/E-Learning Resources:

U Tube links

1. **https://www.youtube.com/watch?v=shdlEapDsP4**
2. **https://youtu.be/K-nw5EUxDz0?feature=shared**
3. **https://youtu.be/o9sP-vaCEa0?si=l8yOvVKaItBQWXNu**
4. **https://youtu.be/JnoZE51WZg4?si=9uq68USOz5plBk2n**
5. **https://youtu.be/shdlEapDsP4?si=tC6RGaMtwDJgVu2d**
6. **https://youtu.be/9paXgC2U8L0?si=btS1G4mvrkG5C9zi**

3. Apps

C) Learn Japanese - Hiragana APP available on Google play.

D) Hiragana Pro

COURSE CURRICULUM

Name of the Program:		**Foreign Language**		**Semester: IV**		**Level: UG**	
Course Name		**German A1.2**		**Course Code/Course Type**		**UFL 202 A/AEC**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	**-**	**-**	**-**	**2**	**20**	**30**	**-**
Pre-Requisite: Can understand and use familiar, everyday expressions and very simple sentences aimed at satisfying specific needs.							
Course Objectives (CO):				The objectives of (German A1.2) are: 1. To get along with a basic vocab. 2. To understand German day to day culture. 3. Can communicate in routine situations. 4. To be able to have a direct exchange of information about familiar matters. 5. To describe own surroundings.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Communicate in the areas of immediate importance. 2. Able to frame simple sentences in formal conversation. 3. Translate simple sentences from English to the German language and vice-versa. 4. Construct a dialogue, in the German language, for basic human interactions in a social context. 5. Take part in an interaction relating to basic conversation			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Kontakte:planning of letter writing, ramification of Letter, ,writing and understanding, discussion about language learning, find information from texts, understand conversations on various topics, texts related to office life.Grammar – Usage of Articles and Prepositions	**CLO 1**	**6**
UNIT II		
MeineWohnung: Understand home advertisements, describe house, how to reply invitations, how to express 'likes and dislikes', speak about different forms of living, how to write a text on houseGrammar – Adjectives	**CLO 2**	**6**
UNIT III		
AllesArbeit: Talk about daily routine, talk about past, understand job advertisements, understand blogs on jobs, express opinions about jobs, prepare telephonic dialogues, speak about jobs Grammar – Past tense, Sentence connectors	**CLO3**	**6**
UNIT IV		
Kleidung und Mode:-Speak about cloths and shopping, lead a discussion during cloths shopping, discussion in departmental store, understand and research information about Berlin Grammar – Separable and non-separable verbs	**CLO4**	**6**
UNITV		
Gesund und munter&Ab in den Urlaub: Learn body parts, Health related dialogue, City orientation, Travel reports, discussion regarding different travel destinations and weather Grammar – Imperative, Time adverbs	**CLO5**	**6**
Total Hours		**30**

Learning resources

Textbooks:

1. Netzwerk A1, Ernst klettVerlag&Goyal Publishers & Distributors Pvt. Ltd.
2. Studio d A1, CornelesenVerlag&Goyal Publishers & Distributors Pvt. Ltd.
3. NetzwerkNeu A1, Ernst klettVerlag&Goyal Publishers & Distributors Pvt. Ltd

Reference Books:

1. Hallo Deutsch A1,ErnstKlettVerlag, Goyal Publishers & Distributors Pvt. Ltd
2. ThemenAktuell 1, Hueberverlag
3. Maximal Ernst klettVerlag&Goyal Publishers & Distributors Pvt. Ltd.

Online Resources/E-Learning Resources:

Youtube:

https://youtube.com/@LearnGermanwithAnja?si=BkJYDPi7TS0fT4lr

https://youtube.com/@deutschlernenmitheidi?si=TkICIabzioaU0roZ

Instagram :instagram.com/learngermanwithanja

Name of the Program:	**B.Sc. (Cyber Security)**	**Semester: Exit Policy**	**Level: UG Certificate**
Course Name	**Cyber Crime Investigation and Digital Forensics**	**Course Code/ Course Type**	UCEXBS101/VSC
Course Pattern	**Revised 2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	50	-	-

Prerequisite: Students should have basic Knowledge of Cyber.

Course Objectives (CO):	The objectives of Cyber Crime Investigation and Digital Forensics are: 1. To identify security risks and take preventive steps 2. Explain the different types of Cyber Crime Issues. 3. To understand the evidence capturing process. 4. To understand the preservation of digital evidence 5. To elaborate the role of CRET in cyber security.
Course Learning Outcomes (CLO):	Students will be able to: 1. Acquire the definition of computer forensics fundamentals. 2. Describe the types of computer forensics technology. 3. Analyze various computer forensics systems. 4. Illustrate the methods for data recovery, evidence collection and data seizure 5. Summarize duplication and preservation of digital evidence.

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property, Cyber Crime	**CLO 1**	6
UNIT II		
Cyber Crime Issues: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.	**CLO 2**	**6**
UNIT III		
Investigation: Introduction to Cyber Crime Investigation, Investigation Tools, e-Discovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking	**CLO3**	**6**
UNIT IV		
Digital Forensics: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.	**CL04**	**6**
UNIT V		
Role of CRET-In Cyber Security: Computer Security Incident Response (Reactive), Computer Security Incident Prevention (Proactive), Security Quality Management Services, CERT-In Security Guidelines- Web server, database server, Intrusion Detection system, Routers, Standard alone system, networked System, IT Security polices for government and critical sector organizations.	**CLO5**	**6**

Total	30 Hrs

Learning Resources

Textbooks:

1. Nihad A. Hassan, ―Digital Forensics Basics: A Practical Guide Using Windows OS Paperback‖, February 26, 2019.

Reference Books:

1. Nelson Phillips and EnfingerSteuart, ―Computer Forensics and Investigations‖, Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, ―Incident Response and Computer Forensics―, Tata McGraw-Hill, New Delhi, 2006.
3. Robert M Slade, Software Forensics‖, Tata McGraw - Hill, New Delhi, 2005

Online Resources/E-Learning Resources:

1. https://www.cert-in.org.in/

COURSE CURRICULUM

Name of the Program:		**B.Sc.(Cyber Security)**		**Semester: Exit Policy**	**Level: UG Diploma**		
Course Name		**Cyber Defense**		**Course Code/ Course Type**	UDIEXBS201/VSC		
Course Pattern		**2024**		**Version**	1.0		
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	50	-	-
Prerequisite: Students should have basic Knowledge of Cyber.							
Course Objectives (CO):				The objectives of Cyber Defence are: 6. To remember the basics about security. 7. Understand the need for classical encryption techniques. 8. To Identify the basic concepts and algorithms used in number theory and finite fields. 9. To analyse the need of Design principles and their modes. 10. To elaborate the various principles of Pseudorandom Number generation.			
Course Learning Outcomes (CLO):				Students will be able to: 6. List out the basics of security and its services. 7. Explain the different classical encryption techniques. 8. Apply the concept of number theory in varied fields of security. 9. Analyse the design principles for the implementation of AES. 10. Demonstrate the use of Pseudorandom Number generation using block cipher.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Security: Security Concepts, Security Attacks, Antivirus bypassing, Password Attacks and Web browser exploitation, Security Services and Mechanisms, Security Model.	**CLO 1**	6
UNIT II		
Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Block Ciphers and DES, Traditional Block Cipher Structure.	**CLO 2**	**6**
UNIT III		
Basic concepts in Number Theory and Finite Fields: Introduction, Division Algorithms, Euclidean Algorithm, Modular Algorithm, Groups, Rings and Fields, Polynomial Arithmetic	**CLO3**	**6**
UNIT IV		
Block Cipher Design Principles: Finite Field Arithmetic, AES Structure, AES Transformation Functions, AES Example, AES implementation. Block Cipher Operation, Multiple Encryption and Triple DES,Modes of Operation.	**CL04**	**6**
UNIT V		
Principles and Pseudorandom Number Generation: Pseudorandom Number, Generators, Pseudorandom Number Generation using a Block Cipher, Stream, Ciphers, RC4, Fermats and Euler's Theorem,	**CLO5**	**6**
Total		**30 Hrs**

Learning Resources

Textbooks:

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015.

Reference Books:

1. Applied Cryptography for Cyber Security and Defense
2. Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

Online Resources/E-Learning Resources:

1. Udacity- Introduction to Information Security- https://www.udacity.com/course/intro-to-information-security--ud459
2. https://www.coursera.org/professional-certificates/sscp-training

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester - V

Name of the Program:	**B.Sc.(Cyber Security)**	**Semester: V**	**Level: UG**
Course Name	Ethical Hacking	**Course Code and Course Type**	UBS301/MAJ
Course Pattern	**Revised 2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
3	-	-	3	3	40	60	-

Prerequisite:	
Course Objectives (CO):	The objectives of: 1. Gain knowledge of security principles, ethical hacking concepts, security testing, and legal considerations in cybersecurity. 2. Identify and gather critical information about target systems, including network scanning, OS fingerprinting, and enumeration. 3. Understand different types of malware, such as viruses, worms, Trojans, and spyware, and learn countermeasures against these threats. 4. Explore techniques for hacking web applications, databases, and wireless networks while understanding mobile security risks. 5. Understand the role of Intrusion Detection Systems (IDS), firewalls, honeypots, and other security mechanisms to defend against cyber threat
Course Learning Outcomes (CLO):	Students will be able to: 1. Understand the core foundations of ethics in regards to computer security 2. Perform the foot printing and scanning. 3. Demonstrate the techniques for system hacking. 4. Characterize the malware and their attacks and detect and prevent them. 5. Detect and prevent the security attacks in different environments

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I		
An Introduction to ethical Hacking: Security Fundamental, Security testing, Hacker and Cracker, Descriptions, Test Plans-keeping It legal, Ethical and Legality, Information Security Controls – Penetration Testing Concepts.	**CLO 1**	9
UNIT II		
Footprinting and scanning: Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface, Enumeration, System Hacking.	**CLO 2**	9
UNIT III		
Malware Threats, Sniffers, Session Hijacking and Denial of Service: Viruses and Worms, Trojans, Covert Communication, Keystroke Logging and Spyware, Malware Counter measures, Sniffers, Session Hijacking, Denial of Service and Distributed Denial of Service.	**CLO3**	9
UNIT IV		
Web Server Hacking & Wireless Technologies: Web Server Hacking, Web Application Hacking, Database Hacking, Wireless Technologies, Mobile Device Operation and Security, Wireless LANs.	**CLO4**	9
UNIT V		
IDS, Firewalls and Honeypots : Intrusion Detection Systems, Firewalls, Honeypots, Physical Security, Social Engineering, Cloud Computing, Botnets.	**CLO5**	9
Total Hours		**45**

Learning resources

Textbooks:

1. Beginners Guide to Ethical Hacking & Cybersecurity, Abhinav Ojha
2. Mastering Hacking, Harsh Bothra

Reference Books:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification
2. Hacking the Hacker, Roger Grimes, Wiley

Online Resources and E-Learning Resources

1. https://hackaday.com
2. https://breakthesecurity.cysecurity.org
3. https://www.hackthissite.org

Name of the Program:	**BSc (Cyber Security)**	**Semester - V**	**Level: UG**
Course Name	Ethical Hacking Lab	**Course Code/ Course Type**	UBS302/MAJM
Course Pattern	**Revised 2024**	**Version**	**1.0**

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**(Continuous Internal Assessment)**	**Semester Assessment)**	**Practical/Oral**
-	**1**	**-**	**1**	**2**	**25**	**-**	**25**

Prerequisite:	
Couse Objective (CO)	The objectives of Ethical Hacking lab are: 1. Understand and apply information-gathering techniques such as footprinting, reconnaissance, and email tracing to assess system vulnerabilities. 2. Utilize network scanning, enumeration, and intrusion detection tools to detect and report security threats effectively. 3. Demonstrate practical knowledge in identifying, analyzing, and mitigating malware threats including viruses, worms, trojans, and password attacks. 4. Perform various types of cyberattacks such as DoS, ARP poisoning, SQL injection, and session hijacking to understand attacker methodologies. 5. Explore cryptographic methods including encryption, decryption, and steganography to ensure data security and integrity.
[illegible]	Students will be able to: 1. Demonstrate the ability to gather and analyze information using footprinting and reconnaissance techniques. 2. Apply scanning and sniffing techniques to detect vulnerabilities in networks using tools like port scanners, IDS, and packet sniffers. 3. Identify and exploit common system vulnerabilities through malware, DoS attacks, ARP poisoning, and use of system utilities for security assessment. 4. Develop and evaluate malware such as keyloggers, viruses, and trojans; exploit web application vulnerabilities through attacks like SQL injection and session hijacking

Course Contents/Syllabus:

Activity Number	Assignment/Practical/Activity Title	Number/Turn	Details	CLO	Hours
1	Footprinting and Reconnaissance	Week 1/ Turn 1 and 2	Performing footprinting using Google Hacking, website information, information about an archived website, to extract contents of a website	CLO1	2

2		Week 2/ Turn 1 and 2	trace any received email, to fetch DNS information	CLO1	2
3	Scanning networks, Enumeration and sniffing	Week 3/ Turn 1 and 2	Use port scanning. network scanning tools,	CLO2	2
4		Week 4/ Turn 1 and 2	Use IDS tool, sniffing tool and generate reports	CLO2	2
5	Malware Threats: Worms, viruses, Trojans:	Week 5/ Turn 1 and 2	Use Password cracking, Dictionary attack., Encrypt and decrypt passwords,	CLO3	2
6		Week 6/ Turn 1 and 2	DoS attack, ARP poisoning in windows,	CLO3	2
7		Week 7/ Turn 1 and 2	Ifconfig, ping, netstat, traceroute,	CLO3	2
8		Week 8/ Turn 1 and 2	Steganography tools.	CLO3	2
9	Developing and implementing malwares	Week 9/ Turn 1 and 2	Creating a simple keylogger in python	CLO4	2
10		Week 10/ Turn 1 and 2	creating a virus	CLO4	2

11		Week 11/ Turn 1 and 2	creating a trojan	CLO4	2
12	Hacking web servers, web applications	Week 12/ Turn 1 and 2	Hacking a website by Remote File Inclusion, Disguise as Google Bot to view hidden content of a website, to use Kaspersky for Lifetime without Patch	CLO4	2
13	sql injection and Session hijacking	Week 13/ Turn 1 and 2	SQL injection for website hacking, session hijacking.	CLO4	2
14		Week 14/ Turn 1 and 2	SQL injection for session hijacking.	CLO4	2
15	Wireless network hacking, cloud computing security, cryptography	Week 15/ Turn 1 and 2	Using Cryptool to encrypt and decrypt password, implement encryption and decryption using Ceaser Cipher	CLO4	2
Total					**30**

Learning resources

Textbooks:

Beginners Guide to Ethical Hacking & Cybersecurity, Abhinav Ojha
Mastering Hacking, Harsh Bothra

Reference Books:

Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification

Hacking the Hacker, Roger Grimes, Wiley

Online Resources and E-Learning Resources

https://hackaday.com
https://breakthesecurity.cysecurity.org
https://www.hackthissite.org

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2">BSc(CS)</td><td colspan="2"><b>Semester:</b> V</td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2">Malware Analysis &amp; Reverse Engineering</td><td colspan="2"><b>Course Code/ Course Type</b></td><td colspan="2">UBS303/MAJM</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>Revised 2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hours</b></td><td><b>CIA</b>
<b>(Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical and Oral</b></td></tr>
<tr><td>3</td><td>-</td><td>-</td><td>3</td><td>45</td><td>40</td><td>60</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite:</b></td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of Malware analysis and reverse engineering are:
1. To understand the fundamental concepts of malware, its types, and its impact on computer systems and networks
2. To demonstrate knowledge of tools and techniques used in static and dynamic malware analysis.
3. To develop skills in reverse engineering malware to identify its behavior, functionality, and potential vulnerabilities.
4. To apply strategies to detect, analyze, and mitigate malware in real-world scenarios.
5. To gain awareness of ethical and legal aspects of malware analysis and reverse engineering practice</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students will be able to:
1. Define and explain the key concepts of malware analysis, including virus, worms, ransomware, and spyware.
2. Identify and use industry-standard tools such as IDA Pro, Olly Dbg, and Wireshark to perform malware analysis.
3. Analyze malicious code using reverse engineering techniques to extract information about its behavior and structure.
4. Implement methodologies to create secure environments for safely testing and analyzing malware.
5. Demonstrate an understanding of global cyber laws and ethical guidelines related to malware analysis and reverse engineering.</td></tr>
</table>

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I Introduction to Malware Analysis		
Overview of Malware - Definition, types (viruses, worms, Trojans, ransomware, spyware, rootkits, adware, etc.), and their impact; Malware Evolution - History of malware and	**CLO 1**	9

emerging trends in cyber threats; Malware Analysis Techniques - Static analysis, dynamic analysis, and hybrid approaches; Introduction to Malware Life Cycle - Delivery, installation, execution, persistence, and propagation; **Basic** Malware Indicators: Hashes, file signatures, and behavior analysis		
UNIT II Static Analysis of Malware		
Basics of Static Analysis - What is static analysis?, Analyzing file properties (file type, size, and structure), Extracting basic information (file metadata and strings), Tools for Static Analysis - Introduction to tools like PE Explorer, Strings, and VirusTotal, Limitations of Static Analysis - Packed, encrypted, or obfuscated malware	**CLO 2**	9
UNIT III Dynamic Malware Analysis		
Basics of Dynamic Analysis - What is dynamic analysis, observing malware Behavior in a controlled environment; Key Indicators of Malware Behavior - File system changes, registry modifications, and processes created, Monitoring network activity; Dynamic Analysis Tools - Process Monitor, Process Explorer, TCPView, and Wireshark;	**CLO3**	9
UNIT IV Introduction to Reverse Engineering		
What is Reverse Engineering - Role of reverse engineering in malware analysis; Assembly Language Basics: Overview of x86 architecture; Registers, instructions, and simple control flow; Reverse Engineering Tools - Introduction to IDA Free, Ghidra, and x64dbg., Analyzing simple programs or malware samples	**CLO4**	9
UNIT V Case Studies and Reporting		
Case Studies - Analysis of simple malware samples, Examples of common malware families; Reporting and Documentation - How to create a basic malware analysis report, Sharing findings like IOCs (Indicators of Compromise); Ethical and Legal Aspects - Ethical considerations in malware analysis, Legal frameworks and responsible disclosure	**CLO5**	9
Total Hours		45

Learning resources

Textbooks:

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig
2. "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code by Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard.
3. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory" by Michael Hale Ligh, Andrew Case, Jamie Levy, and AAron Walters

Reference Books:

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software"
2. The Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code

Online Resources and E-Learning Resources

1. **https://www.reddit.com/r/Malware/**
2. **https://www.reddit.com/r/ReverseEngineering/**

Name of the Program:	**BSc (Cyber Security)**	**Semester - V**	**Level: UG**
Course Name	Malware Analysis & Reverse Engineering Lab	**Course Code/ Course Type**	UBS304/MAJM
Course Pattern	**Revised 2024**	**Version**	**1.0**
	Teaching Scheme	**Assessment Scheme**	

Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**(Continuous Internal Assessment)**	**Semester Assessment)**	**Practical/Oral**
-	1	-	1	2	25	-	25

Prerequisite:	
Couse Objective (CO)	The objectives of Malware analysis and reverse engineering lab are: 1. To understand different types of malwares and their characteristics. 2. To explore various techniques for identifying and analyzing malware files 3. To develop hands-on skills in reverse engineering and debugging executables 4. To apply static and dynamic analysis techniques to detect malicious behavior 5. To generate comprehensive malware analysis reports, including Indicators of Compromise (IOCs) and mitigation strategies
	Students will be able to: 1. Identify and classify different types of malwares based on their characteristics and behavior 2. Utilize hashing, file signatures, and metadata extraction tools to verify and analyze malware files 3. Perform static and dynamic analysis using appropriate tools to inspect malware behavior and impact 4. Apply reverse engineering techniques using disassemblers, decompiles, and debuggers to analyze malware. 5. Create detailed malware analysis reports, documenting findings, behavior patterns, and security recommendations.

Course Contents/Syllabus:

Activity Number	Assignment/Practical/Activity Title	Number/Turn	Details	CLO	Hours
1	Identifying Malware Types	Week I/ Turn 1 and 2	Collect and analyze different malware samples (harmless ones like EICAR), Categorize them as viruses, worms, Trojans, etc.	CLO1	2
2	Hashing and File Signatures	Week 2/ Turn 1 and 2	Compute MD5/SHA-256 hashes for files to check integrity, identify file signatures using Binwalk or Hex editors.	CLO1	2
3	Detecting Malware with VirusTotal	Week 3/ Turn 1 and 2	Upload sample files to VirusTotal and analyze the results.	ClO1	2
4	Extracting File Metadata	Week 4/ Turn 1 and 2	Use PE Explorer or exiftool to extract metadata from executables	CLO2	2
5	Analyzing Strings in Executables	Week 5/ Turn 1 and 2	Use strings command or Strings Utility in Sysinternals to find readable text in a malware sample	CLO3	2
6	Checking for Packed Malware	Week 6/ Turn 1 and 2	Use PEiD or Detect It Easy (DIE) to check if a file is packed or obfuscated	CLO2	2
7	Identifying Imports and Exports of an Executable	Week 7/ Turn 1 and 2	Use Dependency Walker or PE Explorer to list imported/exported functions.	CLO2	2

8	Dynamic Malware Analysis	Week 8/ Turn 1 and 2	Run a test executable in a sandbox and track changes using Process Monitor.	CLO3	2
9	Analyzing Registry Modifications	Week 9/ Turn 1 and 2	Use Regshot before and after running a sample to detect registry changes.	CLO3	2
10	Observing Process Behavior	Week 10/ Turn 1 and 2	Use Process Explorer to monitor newly created processes and their resource usage.	CLO3	2
11	Capturing Network Traffic of Malware	Week 11/ Turn 1 and 2	Run a benign sample and analyze network traffic using Wireshark.	CLO3	2
12	Disassembling an Executable with Ghidra	Week 12/ Turn 1 and 2	Open a simple program in Ghidra and analyze its assembly code.	CLO4	2
13	Finding Hardcoded Strings in IDA Free	Week 13/ Turn 1 and 2	Load a sample file in IDA Free and find hardcoded file paths, domains, or IPs.	CLO4	2
14	Basic Debugging with x64dbg	Week 14/ Turn 1 and 2	Step through a simple executable and observe function calls	CLO4	2
15	Creating a Basic Malware Report	Week 15/ Turn 1 and 2	Document findings of a simple malware analysis, including behavior, IOCs, and mitigation strategies	CLO5	2
Total					30

Learning Resources

Textbooks:

1. Michael Sikorski & Andrew Honig – Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software
2. Bruce Dang, Alexandre Gazet, Elias Bachaalany – Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, and Reversing Tools

Reference Books:

1. "Practical Malware Analysis" by Michael Sikorski and Andrew Honig
2. "Malware Analyst's Cookbook and DVD" by Michael Hale Ligh, Steven Adair, Blake

Online/e learning resources:

a. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation

b. Introduction to Reverse Engineering Software from OpenSecurityTraining.info | NICCS

Name of the Program:		**BSc(CS)**		**Semester: V**		**Level: UG**	
Course Name		**Applied Cryptography**		**Course Code and Course Type**		**UBS306**	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme: Theory					**Assessment Scheme:**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
3	-	-	3	3	40	60	-
Prerequisite:							
Course Objectives (CO):				**The objectives of:** 1. Understand cryptographic principles and their role in securing communication. 2. Learn symmetric and asymmetric cryptographic techniques and their applications. 3. Explore cryptographic protocols for authentication, digital signatures, and key exchange. 4. Analyze real-world cryptographic systems and their security implications. 5. Implement cryptographic algorithms and protocols in practical applications.			
Course Learning Outcomes (CLO):				**Students will be able to:** 1. Explain the principles of cryptographic security and cryptanalysis techniques. 2. Apply symmetric and asymmetric cryptographic algorithms for secure communication. 3. Implement cryptographic protocols for authentication and key management. 4. Analyze vulnerabilities in cryptographic systems and suggest countermeasures. 5. Design and develop secure applications using modern cryptographic techniques.			

Course Contents and Syllabus:

Descriptors and Topics	CLO	Hours
UNIT I - Introduction to Cryptography		9
Foundations of Cryptography: Security goals (confidentiality, integrity, authenticity, non-repudiation). Threats and attacks (brute-force, man-in-the-middle, side-channel attacks). Mathematical Background: Number theory (modular arithmetic, prime numbers, GCD, Euler's theorem). Probability and randomness in cryptographic systems.	**CLO 1**	
UNIT II - Symmetric Key Cryptography		9
Classical Encryption Techniques: Caesar cipher, Vigenère cipher, Playfair cipher. One-time pad and its security implications. Modern Block Ciphers: Data Encryption Standard (DES), Triple DES. Advanced Encryption Standard (AES): Structure, key expansion, security. Modes of Operation: ECB, CBC, CFB, OFB, GCM. Stream Ciphers: RC4, ChaCha20.	CLO 2	
UNIT III - Asymmetric Key Cryptography		9
Public Key Cryptography Principles: Key pairs, encryption and decryption process. RSA Algorithm: Key generation, encryption, decryption, security analysis. Diffie-Hellman Key Exchange: Concept and security considerations. Elliptic Curve Cryptography (ECC): Advantages over RSA, applications.	CLO3	
UNIT IV - Cryptographic Protocols and Applications		9
Cryptographic Hash Functions: Properties (collision resistance, preimage resistance). MD5, SHA-1, SHA-2, SHA-3, BLAKE2. Message Authentication Codes (MACs) & HMAC. Digital Signatures: RSA Digital Signatures. DSA and ECDSA. Key Management and Distribution: PKI, certificate authorities, SSL/TLS.	CLO4	
UNIT V - Applications and Advanced Topics		9
Cryptanalysis Techniques: Brute-force, frequency analysis, differential cryptanalysis. Secure Communication: HTTPS, VPN, email encryption (PGP, S/MIME). Blockchain and Cryptocurrency: Bitcoin, Ethereum, cryptographic principles in blockchain. Post-Quantum Cryptography: Threats and emerging cryptographic techniques.	CLO5	
Total Hours		45

Learning resources

Textbooks:

1. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, Wiley, 2015.
2. William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson, 2017.
3. Behrouz A. Forouzan, *Cryptography and Network Security*, McGraw-Hill, 2011.

Reference Books:

1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
2. Douglas R. Stinson, *Cryptography: Theory and Practice*, 4th Edition, CRC Press, 2018.

3. Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, 3rd Edition, CRC Press, 2020.
4. Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994.
5. Christof Paar, Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.

Online Resources and E-Learning Resources:

E-Learning Platforms

- **Coursera Courses**:
  - Cryptography I by Stanford University (Coursera)
  - Applied Cryptography by University of Colorado (Coursera)
- **edX Courses**:
  - Cybersecurity Fundamentals by Rochester Institute of Technology (edX)
- **Khan Academy**:
  - Cryptography and Security Basics (Khan Academy)
- **MIT OpenCourseWare**:
  - Computer Science and Applied Cryptography (MIT OCW)
- **YouTube Channels**:
  - Computerphile (Security & Cryptography)
  - Cryptography by NPTEL
  - Whiteboard Cryptography
  -

E-Leaning and Practice Apps

- **Coursera Courses**:
  - Cryptography I by Stanford University (Coursera)
  - Applied Cryptography by University of Colorado (Coursera)
- **edX Courses**:
  - Cybersecurity Fundamentals by Rochester Institute of Technology (edX)
- **Khan Academy**:
  - Cryptography and Security Basics (Khan Academy)
- **MIT OpenCourseWare**:
  - Computer Science and Applied Cryptography (MIT OCW)
- **YouTube Channels**:
  - Computerphile (Security & Cryptography)
  - Cryptography by NPTEL
  - Whiteboard Cryptography

Name of the Program:	**BSc (CS)**	**Semester: V**	**Level: UG**
Course Name	**Cyberspace Operations and Design**	**Course Code and Course Type**	**UBS305A/MAJE**
Course Pattern	**Revised 2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA** **(Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
3	-	-	3		40	60	
Prerequisite:							

Course Objectives (CO):	1. To understand basics of full-spectrum cyberspace operations. 2. Understand cyberspace environment, as well as planning, organizing, and integrating cyberspace operations. 3. Consists of presentations and exercises about operations. 4. To develop a cyber-operations design and bring it to fruition 5. To analyze, plan for, and execute cyberspace operations.
Course Learning Outcomes (CLO):	Students will be able to: 1. Understand the Cyberspace Environment and Design. 2. Cyberspace Operational Approaches, Cyberspace Operations, and cyberspace integrations. 3. Apply knowledge to building Cyber Warriors and Warrior Corps. 4. Analyze to Designing Cyber Related Command. 5. Examine Training and Readiness for Cyber Related Commands.

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I		
Introduction: Definition**,** Cyberspace as a Domain of Warfare, Objective of cyberspace operations and design, Scope of Cyberspace Operations and Design, Cyberspace environment and its characteristics, Developing a design approach, Planning for cyberspace operation.	**CLO1**	**9**
UNIT II		
Understanding the Cyberspace Environment and Design: Components of a Secure Cyberspace Infrastructure, Cyberspace Operational Approaches- Foundational approaches that utilize cyberspace capabilities to support organizational missions, The pros, and cons of the different approaches, Incident Response and Digital Forensics, Foundational approaches that utilize cyberspace capabilities to support organizational	**CLO2**	**9**

missions.		
UNIT III		
Cyberspace Operations and Integrations: Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defense and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations, Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application exercise.	**CLO3**	**9**
UNIT IV		
Building Cyber Warriors and Warrior Corps: The warrior and warrior corps concept as applied to cyber organizations, The challenges of training and developing a cyber-workforce from senior leadership to the technical workforce.	**CLO4**	**9**
UNIT V		
Designing Cyber Related Commands: Mission statements, Essential tasks, Organizational structures, Tables of organizations Training and Readiness for Cyber Related Commands Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Paulo Shakarian et al. "Introduction of Cyber Warfare: A Multidisciplinary Approach," syngress, Elsevier 2013.
2. Jeffery carr et al, "Inside Cyber Warfare: Mapping the Cyber Underworld," O'Reilly Publication December 2012.

Reference Books:

1. Jason Andress et al. "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners" Syngress, Elsevier 2013.
2. R. A. Clarke, Robert Knake "Cyber War: The Next Threat to National Security and What to Do About It" Haper Collins Publisher 2010.

Online Resources and E-Learning Resources

1. https://www.globalknowledge.com/us-en/course/86761/introduction-to-cyber-warfare-and-operations-design
3. https://www.coursera.org/courses?query=cybersecurity

Name of the Program:		**B.Sc. Computer Science (Cyber Security)**		**Semester : V**		**Level: UG**	
Course Name		**Secure Software Design and Development**		**Course Code/ Course Type**		**UBS305B/MAJE**	
Course Pattern		**Revised 2024**		**Version**		**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA** **(Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	-	40	60	-
Prerequisite: Basic knowledge of Computer Network and Java.							
Course Objectives (CO):				The objectives of Mobile Security are: 1. To understand the importance of integrating security practices into the software development lifecycle (SDLC). 2. To explore threat modeling techniques and risk assessment methods for secure software design. 3. To learn secure coding standards and best practices for developing robust and secure applications. 4. To gain practical exposure to security testing tools and techniques for identifying vulnerabilities in software systems. 5. To develop an understanding of compliance requirements and secure deployment strategies for software applications.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Demonstrate knowledge of Secure Software Development Life Cycle (SDLC) and its significance. 2. Identify security requirements and apply threat modeling techniques to assess risks in software projects. 3. Apply secure coding standards to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), etc. 4. Conduct security testing using automated tools and manual techniques to detect software vulnerabilities. 5. Recommend and implement best practices for secure deployment, configuration management, and incident response.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction to Secure Software Development Lifecycle (SDLC): Basics of Software Development Life Cycle (SDLC), Need for Secure Software Development, Introduction to Secure SDLC Models: Waterfall, Agile, DevSecOps, Security Principles in Software Design: Least Privilege, Defense in Depth, Fail Secure, Secure Defaults, Common Software Vulnerabilities and OWASP Top 10 Overview, Case Studies on Real-World Software Security Breaches	**CLO 1**	**9**
UNIT II		
Secure Requirements Engineering & Threat Modeling: Importance of Security Requirements in SDLC, Techniques to Gather Security Requirements, STRIDE Model for Threat Modeling, Attack Surface Analysis, Risk Assessment and Mitigation Planning, Tools for Threat Modeling: Microsoft Threat Modeling Tool, Case Study: Threat Modeling for a Web or Mobile Application**.**	**CLO 2**	**9**
UNIT III		
Secure Design Principles & Secure Coding Practices: Secure Design Patterns and Architectural Considerations, Principles for Secure Application Design, Common Secure Coding Guidelines: Input Validation and Output Encoding, Proper Error Handling, Secure Session Management, Secure Cryptographic Practices, Secure Coding Standards: CERT Secure Coding, Language-specific Secure Coding (C/C++, Java, Python, PHP), Static and Dynamic Analysis Tools (SAST/DAST).	**CLO3**	**9**
UNIT IV		
Secure Testing & Vulnerability Assessment: Importance of Security Testing in SDLC, Types of Security Testing: Penetration Testing, Code Review, Fuzz Testing, Introduction to Automated Security Testing Tools (Checkmarx, SonarQube), Security Testing Techniques for Web Applications, APIs, Mobile Applications, Common Vulnerabilities: SQL Injection, XSS, CSRF, Broken Authentication, Reporting and Documenting Vulnerabilities.	**CLO4**	**9**
UNIT V		
Secure Deployment, Maintenance & Compliance: Security Considerations During Deployment, Configuration Management and Hardening Techniques, Monitoring and Logging for Security Events, Patch Management and Secure Updates, Post-deployment Security: Continuous Monitoring and Incident Response, Compliance with Security Standards: ISO 27001, OWASP ASVS, NIST, GDPR, Case Study on Secure Deployment in Cloud Environments	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. **Michael Howard and Steve Lipner,** *The Security Development Lifecycle*, Microsoft Press
2. **Mark G. Graff, Kenneth R. van Wyk,** *Secure Coding: Principles and Practices*, O'Reilly Media
3. **Gary McGraw,** *Software Security: Building Security In*, Addison-Wesley
4. **OWASP Foundation,** *OWASP Software Assurance Maturity Model (SAMM)* (freely available)

Reference Books:

1. **Robert C. Seacord,** *Secure Coding in C and C++*, Addison-Wesley
2. **Ben Laurie, Richard Clayton, and Andrew Whitaker,** *Security Engineering: A Guide to Building Dependable Distributed Systems*, Ross Anderson, Wiley
3. **Neal Ford,** *Fundamentals of Software Architecture: An Engineering Approach*, O'Reilly Media
4. **Andrew Hoffman,** *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*, O'Reilly Media
5. **OWASP Top Ten Project Documentation** (Latest Edition)

Online Resources/E-Learning Resources:

1. **OWASP Official Website** - https://owasp.org
2. **Microsoft Security Development Lifecycle (SDL)** - https://www.microsoft.com/en-us/securityengineering/sdl
3. **NIST Secure Software Development Framework (SSDF)** - https://csrc.nist.gov/publications/detail/sp/800-218/final
4. **CERT Secure Coding Practices** - https://www.sei.cmu.edu/our-work/cert-secure-coding/
5. **Coursera / edX Courses on Secure Software Development and Secure Coding**
6. **Checkmarx Secure Coding Resources** - https://checkmarx.com/resources
7. **OWASP Threat Modeling Cheat Sheet** - https://cheatsheetseries.owasp.org
8. **GitHub - Secure Coding Practices Repositories**

Name of the Program:		**B.Sc.(Cyber Security)**	**Semester: V**			**Level: UG**	
Course Name		**Security in Wireless Ad hoc Network**	**Course Code and Course Type**			**UBSM107**	
Course Pattern		**Revised 2024**	**Version**			**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA** **(Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
-	-	-	2	2	25	-	25
Prerequisite:							
Course Objectives (CO):			The objectives of: 1. To provide a foundational understanding of computer networks, including addressing, switching, and common protocols. 2. To examine network security threats, models, and infrastructure components used to protect against cyber-attacks. 3. To develop knowledge and skills for managing network security through monitoring, auditing, and secure administration practices. 4. To introduce the concept, structure, and operational workflow of a Security Operations Centre (SOC) and its critical role in cybersecurity. 5. To explore global cybersecurity challenges, threat actors, motivations, and their impacts on individuals and organizations, and their impacts on individuals and organizations.				
Course Learning **Outcomes (CLO):**			Students will be able to: 1. Describe the fundamentals of computer networks and key security protocols involved in network communication. 2. Identify and classify common network threats, vulnerabilities, and protective technologies used in network security infrastructure. 3. Apply security administration techniques and demonstrate monitoring and auditing processes in wireless and cloud networks. 4. Evaluate SOC deployment models, services, tools, and assess their effectiveness in real-time threat detection and response. 5. Analyze the impact of cybersecurity threats and explain the motivations and consequences of hacking in the global digital landscape.				

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I Computer Networks		
Networking Fundamentals, IP Addressing and Switching, Network Protocols, Network Security Technique	**CLO 1**	6
UNIT II Network Security		
Network concepts and Models, Common Network Threats and Attacks, Network Security Infrastructure, Network Security Review	**CLO 2**	6
UNIT III Managing Network Security		
Cybersecurity Technology Administration, Wireless and Cloud Networks, Cybersecurity Network Auditing, Monitoring and Logging, Wrap up for Managing Network Security	**CLO3**	6
UNIT IV Security Operations Centre (SOC)		
Introduction to Security Operations Centre, Security Operations Centre Processes and Services, SOC Deployment Models and Types, Staffing an Effecting SOC Team, Security Event Data and SOC Analyst Tools, Developing Key Relationship with Internal and External Stakeholders, Understanding the SOC Metrics, Understanding SOC Workflow and Automation	**CLO4**	6
UNIT V Cybersecurity for Everyone		
Defining Cybersecurity, Cybersecurity Problems, Evolution of Internet, Global Telecommunications Architecture and Governance, Threat Actors and Their Motivations, The Hacking Process, End Process-Direct and Indirect Consequences	**CLO5**	6
Total Hours		**30**

Learning resources

Textbooks:

1. "Security in Wireless Ad Hoc and Sensor Networks" by Erdal Çayırcı and Chunming Rong
2. "Ad Hoc Wireless Networks: Architectures and Protocols" by C. Siva Ram Murthy and B.S. Manoj
3. "Wireless Sensor Networks: Technology, Protocols, and Applications" by Kazem Sohraby, Daniel Minoli, and Taieb Znati

Reference Books:

1. "Wireless Ad Hoc and Sensor Networks: Theory and Applications" by Rajesh M. Shrestha and Dharma P. Agrawal
2. "Security for Wireless Sensor Networks" by Frank Stajano (Editor), B. S. Manoj
3. "Cryptography and Network Security: Principles and Practice" by William Stallings

Online Resources and E-Learning Resources
1. NPTEL – National Programme on Technology Enhanced Learning- https://nptel.ac.in/courses/106105160
2. edX- https://www.edx.org
3. Udemy -*Wireless Network Security Made Simple*- https://www.udemy.com

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester – VI
SCHEME-A

Name of the Program:		**BSc.(CS)**		**Semester: VI**		**Level: UG**	
Course Name		Blockchain Technology		**Course Code and Course Type**		UBS308	
Course Pattern		**2024**		**Version**		1.0	
Teaching Scheme: Theory					**Assessment Scheme:**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
2	-	-	2	2	20	30	-
Prerequisite:							
Course Objectives (CO):				**The objectives of:** 1. To provide foundational knowledge of blockchain technology and its components. 2. To develop an understanding of distributed ledger technology and consensus mechanisms. 3. To familiarize students with blockchain platforms and smart contract development. 4. To explore blockchain applications in various industries. 5. To equip students with the ability to analyze, design, and implement blockchain-based solutions.			
Course Learning Outcomes (CLO):				**Students will be able to:** 1. Explain the basic principles and architecture of blockchain technology. 2. Understand and apply cryptographic techniques in blockchain systems. 3. Analyze the working of consensus mechanisms in blockchain. 4. Develop smart contracts using blockchain platforms. 5. Evaluate real-world blockchain applications and design blockchain-based solutions.			

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I - Introduction to Blockchain Technology		6
History and evolution of blockchain technology, Key characteristics: Decentralization, immutability, and transparency, Blockchain architecture and components: Blocks, chains, nodes, and transactions, Types of blockchains: Public, private, and consortium blockchains.	**CLO 1**	
UNIT II - Cryptography and Blockchain Security		6
Cryptographic foundations: Hash functions, digital signatures, and public-key cryptography, Merkle trees and their role in blockchain, Blockchain security: Consensus	**CLO 2**	

models and attack resistance, Case studies: Bitcoin and Ethereum blockchain security.		
UNIT III - Consensus Mechanisms		6
Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS), Byzantine Fault Tolerance (BFT) and Practical Byzantine Fault Tolerance (PBFT), Scalability issues and Layer 2 solutions.	**CLO3**	
UNIT IV - Smart Contracts and Blockchain Platforms		6
Introduction to smart contracts and their importance, Writing smart contracts with Solidity on Ethereum, Comparison of blockchain platforms: Ethereum, Hyperledger, Binance Smart Chain, and Polkadot, Case studies: Applications of smart contracts.	**CLO4**	
UNIT V - Blockchain Applications and Future Trends		6
Blockchain applications: Supply chain, finance, healthcare, and governance, Challenges: Scalability, energy consumption, and regulatory concerns, Emerging trends: Interoperability, blockchain in IoT, and Web3, Ethical considerations in blockchain adoption.	**CLO5**	
Total Hours		30

Learning resources

Textbooks:

1. **"Mastering Blockchain" by Imran Bashir**
    - Edition: 3rd
    - Publisher: Packt Publishing
    - Focus: Comprehensive introduction to blockchain technology, cryptographic principles, consensus mechanisms, and smart contracts.
2. **"Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher**
    - Edition: 1st
    - Publisher: Apress
    - Focus: Simplified understanding of blockchain concepts for beginners.
3. **"Ethereum and Solidity: The Complete Guide to Blockchain Programming" by Henning Diedrich**
    - Edition: 1st
    - Publisher: CreateSpace Independent Publishing Platform
    - Focus: Detailed guide on Ethereum, smart contract development, and Solidity programming.

Reference Books:

1. **"Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World" by Don Tapscott and Alex Tapscott**
    - Edition: 1st
    - Publisher: Portfolio
    - Focus: Application of blockchain technology in business and its impact on industries.
2. **"Bitcoin and Cryptocurrency Technologies" by Arvind Narayanan et al.**
    - Edition: 1st
    - Publisher: Princeton University Press
    - Focus: Cryptographic foundations, Bitcoin, and blockchain's role in cryptocurrencies.

3. **"Hyperledger Blockchain Solutions: A Guide to Enterprise Blockchain Platforms" by Nitin Gaur, Luc Desrosiers, and Venkatraman Ramakrishna**
   - Edition: 1st
   - Publisher: Addison-Wesley Professional
   - Focus: Hyperledger framework and its applications in enterprise blockchain solutions.

Online Resources and E-Learning Resources:

1. **Coursera - "Blockchain Specialization" by University at Buffalo & The State University of New York**
   - URL: Blockchain Specialization
   - Description: Comprehensive course covering blockchain basics, smart contracts, and applications.
2. **edX - "Blockchain Fundamentals" by UC Berkeley**
   - URL: Blockchain Fundamentals
   - Description: Beginner-friendly program to learn blockchain principles and use cases.
3. **GitHub - Blockchain Development Resources**
   - URL: Blockchain Resources
   - Description: A curated list of tutorials, tools, and guides for learning blockchain development.

E-Learning Resources

1. **IBM Blockchain Platform Tutorials**
   - URL: IBM Blockchain Tutorials
   - Description: Hands-on tutorials and resources to learn and implement blockchain solutions.
2. **Solidity Documentation**
   - URL: Solidity Docs
   - Description: Official documentation and tutorials for programming smart contracts on Ethereum.
3. **Blockchain at Berkeley - YouTube Channel**
   - URL: Blockchain at Berkeley
   - Description: Educational videos on blockchain, cryptocurrencies, and decentralized systems.

Name of the Program:		**BSc(CS)**		**Semester:** VI		**Level: UG**	
Course Name		Research Methodologies and Techniques(MOOC)		**Course Code/ Course Type**		UBSM109	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	-	2	25		25
Prerequisite: Anyone can take this course with basic knowledge of English communication							
Course Objectives (CO):				The objectives of Applied Communication are: 1. Provide fundamental knowledge of research methodologies. 2. Develop analytical skills for conducting systematic research. 3. Enhance understanding of qualitative and quantitative research techniques. 4. Introduce research ethics, literature review, and citation methods. 5. Enable students to apply research tools for problem-solving and decision-making.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Explain the concept, purpose, and significance of research. 2. Apply research techniques in academic and professional settings. 3. Conduct literature reviews and apply proper citation methods. 4. Differentiate between qualitative and quantitative research methodologies. 5. Develop and present a structured research proposal.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction to Research Methodology: Definition and importance of research, Types of research (exploratory, descriptive, analytical, applied), Research process and characteristics of good research.	**CLO 1**	**6**
UNIT II		
Research Design and Sampling Techniques: Research design types, Formulating research problems, Hypothesis development, Sampling methods and data collection techniques.	**CLO 2**	**6**
UNIT III		
Literature Review and Citation Techniques: Importance of literature review, Searching academic sources, Referencing and plagiarism, Citation styles (APA, MLA, IEEE)	**CLO3**	**6**
UNIT IV		
Qualitative & Quantitative Research Methods: Overview of qualitative and quantitative approaches, Data analysis techniques, Survey design, Interview techniques	**CLO4**	**6**
UNIT V		
Research Proposal and Ethical Considerations: Writing a research proposal, Ethical principles in research, Institutional Review Boards (IRB), Presenting research findings effectively	**CLO5**	**6**
Total Hours		**30 hrs.**

Learning resources

Textbooks:

1. **Research Methodology: A Step-by-Step Guide for Beginners** – Ranjit Kumar
2. **Business Research Methods** – Donald R. Cooper & Pamela S. Schindler

Reference Books:

1. **The Craft of Research** – Wayne C. Booth, Gregory G. Colomb, Joseph M. Williams
2. **Qualitative Inquiry and Research Design: Choosing Among Five Approaches** – John W. Creswell

Online Resources:

- **Coursera:** Research Methods
- **MIT OpenCourseWare:** Introduction to Research Methods
- **Google Scholar:** https://scholar.google.com/

Name of the Program:		**BSc(CS)**		**Semester: VI**		**Level: UG**	
Course Name		**Mobile Forensics(MOOC)**		**Course Code/ Course Type**		**UBSM110**	
Course Pattern		**Rev. 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	25	25	-
Prerequisite: Students should have a basic concept Security in Mobile Devices.							
Course Objectives (CO):				The objectives of Mobile Forensics are: 1. To identify the concepts used in Mobile Forensics. 2. To describe the practical approaches used in Android Forensics. 3. To demonstrate the various forensic techniques used in iOS. 4. To examine the different security mechanism used in Android. 5. Assess the different Traffic Analysis security mechanisms.			
Course Learning Outcomes (CLO):				Students would be able to: 1. To recall the ethical considerations in mobile forensics. 2. To discuss common tools and techniques used in Android Forensics. 3. To make use of various terms associated with iOS Forensics. 4. To categorize the security systems used in Android. 5. To formulate the Traffic analysis of Android Devices.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Mobile Forensics: Mobile forensics, Challenges in mobile forensics the mobile phone evidence extraction, components Inside Mobile devices, Crimes using mobile phones, SIM Card, SIM Security, Mobile forensics, Mobile forensic & its challenges, Mobile phone evidence Extraction process.	**CLO1**	**6**
UNIT II		
Android Forensics: Understanding Android, Android model, Android security- Secure kernel, Security- Enhanced Linux, Full Disk Encryption, Trusted Execution Environment, Android Forensic Setup and Pre-Data Extraction Techniques, Android Data Extraction Techniques, Android Data Analysis and Recovery, Android data recovery, Android App Analysis.	**CLO2**	**6**
UNIT III		

iOS Forensics: Introducing iOS Application Security, Basics of iOS and application development, developing your first iOS app, Running apps on iDevice, iOS MVC design, iOS security model, iOS secure boot chain.	**CLO3**	**6**
UNIT IV		
Android Security: Sandboxing and the permission model, Application signing, Android startup process, Setting up the development environment, Creating an Android virtual device, Useful utilities for Android Pentest, Android Debug Bridge, Burp Suite, APKTool.	**CLO4**	**6**
UNIT V		
Traffic Analysis: Traffic Analysis for Android Devices, Android traffic interception. Ways to analyze Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception.	**CLO5**	**6**
Total		**30 hrs**

Books and References:
Text Books

1. Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma and Heather Mahalikunder Packet Publishing.

2. Digital Forensic by Dr. Nilakshi Jain - John Wiley Publication

Reference Books

1. Aditya Gupta, “Learning Pentesting for Android Devices”, Packt Pub Ltd; Illustrated edition, 2014.
2. SwaroopYermalkar, “Learning iOS Penetration Testing Paperback”, Packt Publishing, 2004.

NPTEL Web Course:

- https://youtu.be/GoryZkLhBLo

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester – VI
(SCHEME - B)

Name of the Program:	BSc(Cyber Security)	**Semester: VI**	**Level:**
Course Name	Blockchain Technology (MOOC)	**Course Code and Course Type**	UBSM111
Course Pattern	**Revised 2024**	**Version**	1.0

Teaching Scheme: Theory					**Assessment Scheme:**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
2	-	-	2	2	20	-	30

Prerequisite: Fundamental knowledge of computer science, networking, and data structures.

Course Objectives (CO):	The objectives of Block Chain Technology • Explain blockchain's structure and operational principles. • Analyze consensus mechanisms and their role in decentralized systems. • Work with modern blockchain platforms and tools. • Identify and assess the use of blockchain in various real-world domains. • Address technical and regulatory challenges in blockchain deployment.
Course Learning Outcomes (CLO):	**Students will be able to:** • To Understand the fundamental concepts and components of blockchain technology. • To Analyze blockchain architecture, transactions, and consensus models. • To Demonstrate the use of blockchain platforms like Ethereum and Hyperledger.. • To Explore real-world applications of blockchain in various industries. • To Evaluate emerging blockchain trends, scalability, privacy, and interoperability challenges..

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I - **Introduction to Cryptography**		6
Classical Cryptography (Caesar Cipher, Vigenère), Symmetric vs Asymmetric Encryption, Hash Functions: SHA-256, Merkle Trees, Digital Signatures and Public Key Infrastructure	**CLO 1**	
UNIT II - **Blockchain Fundamentals**		6
Introduction to Blockchain, Structure of a Block and Blockchain, Distributed Ledger Technology, Cryptographic Hashes and Immutable Records	**CLO 2**	
UNIT III - **Consensus Mechanisms & Smart Contracts**		6
Proof of Work (PoW), Proof of Stake (PoS), Byzantine Fault Tolerance, Smart Contracts and Ethereum Basics, Solidity Programming Introduction	**CLO3**	
UNIT IV - **Blockchain Applications Across Industries**		6

Financial services (cryptocurrencies, DeFi), Supply chain management, Healthcare data sharing, Digital identity, voting systems, real estate, and IoT	**CLO4**	
UNIT V - Challenges, Trends, and Future Scope		6
Scalability solutions: Layer 1 & Layer 2, Interoperability and cross-chain communication, Privacy-enhancing technologies (ZKPs, mixers), Legal, regulatory, and ethical considerations, Web3 and the future of decentralized internet	**CLO5**	
Total Hours		30

Learning resources

Textbooks & Reference Books:

- **"Blockchain Basics"** by Daniel Drescher
- **"Blockchain Revolution"** by Don & Alex Tapscott
- **"Mastering Blockchain"** by Imran Bashir
- **"Blockchain Applications"** by Arshdeep Bahga & Vijay Madisetti

Online Resources and E-Learning Resources

Platform	Sample Courses
Coursera	- Blockchain Specialization (University at Buffalo) - Blockchain Revolution (INSEAD)
edX	- Blockchain Fundamentals (UC Berkeley) - Blockchain for Business (Linux Foundation)
Udemy	- Blockchain A-Z: Learn How to Build Your First Blockchain - Ethereum and Solidity Developer Bootcamp
NPTEL (Swayam)	- Blockchain Architecture Design and Use Cases - Fundamentals of Blockchain Technology
IBM SkillsBuild / FutureSkills Prime	- Blockchain Essentials - Blockchain Foundation Developer Path

Name of the Program:		**BSc(CS)**		**Semester:** VI		**Level: UG**	
Course Name		Research Methodologies and Techniques(MOOC)		**Course Code/ Course Type**		UBSM109	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	-	2	25		25
Prerequisite: Anyone can take this course with basic knowledge of English communication							
Course Objectives (CO):				The objectives of Applied Communication are: 1. Provide fundamental knowledge of research methodologies. 2. Develop analytical skills for conducting systematic research. 3. Enhance understanding of qualitative and quantitative research techniques. 4. Introduce research ethics, literature review, and citation methods. 5. Enable students to apply research tools for problem-solving and decision-making.			
Course Learning Outcomes (CLO):				Students would be able to: 1. Explain the concept, purpose, and significance of research. 2. Apply research techniques in academic and professional settings. 3. Conduct literature reviews and apply proper citation methods. 4. Differentiate between qualitative and quantitative research methodologies. 5. Develop and present a structured research proposal.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Research Methodology: Definition and importance of research, Types of research (exploratory, descriptive, analytical, applied), Research process and characteristics of good research.	**CLO 1**	**6**
UNIT II		
Research Design and Sampling Techniques: Research design types, Formulating research problems, Hypothesis development, Sampling methods and data collection techniques.	**CLO 2**	**6**
UNIT III		
Literature Review and Citation Techniques: Importance of literature review, Searching academic sources, Referencing and plagiarism, Citation styles (APA, MLA, IEEE)	**CLO3**	**6**
UNIT IV		
Qualitative & Quantitative Research Methods: Overview of qualitative and quantitative	**CLO4**	**6**

approaches, Data analysis techniques, Survey design, Interview techniques		
UNIT V		
Research Proposal and Ethical Considerations: Writing a research proposal, Ethical principles in research, Institutional Review Boards (IRB), Presenting research findings effectively	**CLO5**	**6**
Total Hours		**30 hrs.**

Learning resources

Textbooks:

3. **Research Methodology: A Step-by-Step Guide for Beginners** – Ranjit Kumar
4. **Business Research Methods** – Donald R. Cooper & Pamela S. Schindler

Reference Books:

3. **The Craft of Research** – Wayne C. Booth, Gregory G. Colomb, Joseph M. Williams
4. **Qualitative Inquiry and Research Design: Choosing Among Five Approaches** – John W. Creswell

Online Resources:

- **Coursera:** Research Methods
- **MIT OpenCourseWare:** Introduction to Research Methods
- **Google Scholar:** https://scholar.google.com/

Name of the Program:		**BSc(CS)**		**Semester: VI**		**Level: UG**	
Course Name		**Mobile Forensics(MOOC)**		**Course Code/ Course Type**		**UBSM110**	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	25	25	-
Prerequisite: Students should have a basic concept Security in Mobile Devices.							
Course Objectives (CO):				The objectives of Mobile Forensics are: 1. To identify the concepts used in Mobile Forensics. 2. To describe the practical approaches used in Android Forensics. 3. To demonstrate the various forensic techniques used in iOS. 4. To examine the different security mechanism used in Android. 5. Assess the different Traffic Analysis security mechanisms.			
Course Learning Outcomes (CLO):				Students would be able to: 1. To recall the ethical considerations in mobile forensics. 2. To discuss common tools and techniques used in Android Forensics. 3. To make use of various terms associated with iOS Forensics. 4. To categorize the security systems used in Android. 5. To formulate the Traffic analysis of Android Devices.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Mobile Forensics: Mobile forensics, Challenges in mobile forensics the mobile phone evidence extraction, components Inside Mobile devices, Crimes using mobile phones, SIM Card, SIM Security, Mobile forensics, Mobile forensic & its challenges, Mobile phone evidence Extraction process.	**CLO1**	**6**
UNIT II		
Android Forensics: Understanding Android, Android model, Android security- Secure kernel, Security- Enhanced Linux, Full Disk Encryption, Trusted Execution Environment, Android Forensic Setup and Pre-Data Extraction Techniques, Android Data Extraction Techniques, Android Data Analysis and Recovery, Android data recovery, Android App Analysis.	**CLO2**	**6**
UNIT III		
iOS Forensics: Introducing iOS Application Security, Basics of iOS and application development, developing your first iOS app, Running apps on iDevice, iOS MVC design, iOS security model, iOS secure boot chain.	**CLO3**	**6**
UNIT IV		

Android Security: Sandboxing and the permission model, Application signing, Android startup process, Setting up the development environment, Creating an Android virtual device, Useful utilities for Android Pentest, Android Debug Bridge, Burp Suite, APKTool.	**CLO4**	**6**
UNIT V		
Traffic Analysis: Traffic Analysis for Android Devices, Android traffic interception. Ways to analyze Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception.	**CLO5**	**6**
Total		**30 hrs**

Books and References:

Text Books

1. Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma and Heather Mahalikunder Packet Publishing.

2**.** Digital Forensic by Dr. Nilakshi Jain - John Wiley Publication

Reference Books

Aditya Gupta, "Learning Pentesting for Android Devices", Packt Pub Ltd; Illustrated edition, 2014.
SwaroopYermalkar, "Learning iOS Penetration Testing Paperback", Packt Publishing, 2004.

NPTEL Web Course:

https://youtu.be/GoryZkLhBLo

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester – VII

Name of the Program:		**BSc(CS)**		**Semester: VII**		**Level: UG**	
Course Name		**Vulnerability Assessment & Penetration Testing**		**Course Code/ Course Type**		UBS401	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hrs.**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
3	-	-	3	3	40	60	-
Prerequisite: Students should have a basic concept Security.							
Course Objectives (CO):				The objectives of Vulnerability Assessment and Penetration Testing are: 1. To Introduce Vulnerability Assessment and Penetration Testing. 2. To describe the various types of Penetration Attacks. 3. To get an exposure of managing penetration testing. 4. To gain knowledge on Web Application Security Vulnerabilities. 5. To assess Vulnerabilities in Client-Side Browsers.			
Course Learning Outcomes (CLO):				Students would be able to 1. To List the key concepts and terminology related to vulnerability assessment. 2. To Explain the need and importance of vulnerability assessment and penetration attacks. 3. To manage the execution of various penetration testing for security. 4. To examine the need for Web Application Security Vulnerabilities. 5. To assess the severity of identified vulnerabilities and recommend appropriate mitigation strategies.			

Course Contents/Syllabus:

Descriptors/Topics	**CLO**	**Hours**
UNIT I		
Introduction to Ethics of Ethical Hacking: Why You Need to Understand Your Enemy's Tactics, Recognizing the Gray Areas in Security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a Social Engineering Attack Works, Common Attacks Used in Penetration Testing, Preparing Yourself for Face-to-Face Attacks, Defending Against Social Engineering Attacks	**CLO1**	**9**
UNIT II		
Penetration Attacks: Physical Penetration Attacks: Need of Physical Penetration, Conducting a Physical Penetration, Common Ways into a Building, Defending Against Physical Penetrations, Conducting an Insider Attack, Defending Against Insider Attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch	**CLO2**	**9**

Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's.		
UNIT III		
Managing Penetration Testing: Planning a Penetration Test, Structuring a Penetration Testing, Agreement, Execution of a Penetration Test, Information Sharing During a Penetration Test, Reporting the Results of a Penetration Test, Understanding Windows Memory Protections.	**CLO3**	**9**
UNIT IV		
Web Application Security Vulnerabilities: Overview of Top Web Application Security Vulnerabilities, Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities, SQL Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities.	**CLO4**	**9**
UNIT V		
Client-Side Browser Exploits: Why Client-Side Vulnerabilities are Interesting, Internet Explorer Security Concepts, History of Client- Side Exploits and Latest Trends, Finding New Browser-Based Vulnerabilities, Heap Spray to Exploit, Protecting Yourself from Client-Side Exploit.	**CLO5**	**9**

Books and References:

Text Books

1. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan

Reference Books

The Web Application Hacker's Hand Book - Discovering and Exploiting Security flaws, Dafydd Suttard, Marcuspinto,1st Edition, Wiley Publishing.

Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No Starch Press.

The Pen Tester Blueprint - Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly,1st Edition, Wiley Publications.

Web links and Video Lectures (e-Resources):

https://www.youtube.com/watch?v=fgdcE4kfQBc

https://www.youtube.com/watch?v=bQh-nhhYcS4

https://www.youtube.com/watch?v=i5GLg9XWJg4

https://qualysec.com/penetration-testing-and-vulnerability-assessment/

COURSE CURRICULUM

Name of the Program:	**BSc (Cyber Security)**	**Semester: VII**	**Level: UG**
Course Name	**Vulnerability Assessment & Penetration Testing-Lab**	**Course Code/ Course Type**	UBS402
Course Pattern	**2024**	**Version**	1.0

Teaching Scheme				**Assessment Scheme**			
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
-	1	-	1	2	25	-	25

Prerequisite: Basic Knowledge is required.

Course Objectives (CO):	The objectives of Vulnerability Assessment & Penetration Testing Lab are:- 1. Introduce Vulnerability Assessment and Penetration Testing 2. To be familiar with the Penetration Testing and Tools 3. To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit 4. To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis. 5. To assess Vulnerabilities in Client-Side Browsers.
Course Learning Outcomes (CLO):	Students would be able to: 1. Explain the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools. 2. Analyze social engineering, physical penetration and insider attacks using automating penetration testing processes. 3. Identify report penetration tests effectively to develop and execute Linux and Windows exploits, bypassing memory protections. 4. Illustrate web application security vulnerabilities to conduct vulnerability analysis. 5. Inspect protection against client-side browser exploits.

Course Contents/Syllabus: Practical Plan

Activity Number	Assignment/Practical/Activity Title	Week Number/Turn	Details	CLO	Hrs
1	Monitoring Network Traffic	Week 1/ Turn 1 and 2	To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.	1	2
2	Monitoring Network Traffic	Week 2/ Turn 1 and 2	To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.	1	2
3	Host & Services Discovery using Nmap	Week 3/ Turn 1 and 2	To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.	2	2
4	Host & Services Discovery using Nmap	Week 4/ Turn 1 and 2	To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.	2	2
5	Vulnerability Scanning using OpenVAS	Week 5/ Turn 1 and 2	To perform a systematic assessment of networked systems using OpenVAS to identify potential vulnerabilities that could be exploited by attackers.	2	2
6	Vulnerability Scanning using OpenVAS	Week 6/ Turn 1 and 2	To perform a systematic assessment of networked systems using OpenVAS to identify potential vulnerabilities that could be exploited by attackers.	3	2
7	Internal Penetration Testing	Week 7/ Turn 1 and 2	Mapping To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques	3	2
8	Internal Penetration	Week 8/	Scanning	3	2

	Testing	Turn 1 and 2	To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques		
9	External Penetration Testing	Week 9/ Turn 1 and 2	Evaluating External Infrastructure	3	2
10	External Penetration Testing	Week 10/ Turn 1 and 2	Evaluating External Infrastructure	4	2
11	Different Types of Vulnerability Scanning	Week 11/ Turn 1 and 2	To explore and compare various vulnerability scanning techniques and tools.	4	2
12	Different Types of Vulnerability Scanning	Week 12/ Turn 1 and 2	To explore and compare various vulnerability scanning techniques and tools.	4	2
13	Vulnerability Scanning with Nessus	Week 13/ Turn 1 and 2	To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation	4	2
14	Vulnerability Scanning with Nessus	Week 14/ Turn 1 and 2	To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation	5	2
15	Web Application Assessment with Nikto & Burp Suite	Week 15/ Turn 1 and 2	To evaluate web applications for security vulnerabilities using Nikto and Burp Suite, identifying issues such as misconfigurations and common vulnerabilities in web applications.	5	2
Total Hrs.					30

Learning resources

1. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 3rd Edition, Tata McGraw-Hill.

Reference Books:

1. The Web Application Hacker's Hand Book - Discovering and Exploiting Security flaws, Dafydd Suttard, Marcuspinto,1st Edition, Wiley Publishing.
2. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No 21102024 5 Starch Press.
3. The Pen Tester Blueprint - Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly,1st Edition, Wiley Publications

Name of the Programme:		B.Sc.(Cyber Security)		**Semester: VII**		**Level: UG**	
Course Name		Python Programming		**Course Code and Course Type**		UBS403 / MAJM	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
3	-	-	3	3	40	60	-
Prerequisite:							
Course Objectives (CO):				The Objectives of Python Programming are: 1. Understand the fundamental concepts of Python programming and its environment. 2. Illustrate data structures like lists, tuples, sets, and dictionaries for real-world applications. 3. Develop structured and modular Python programs using functions, modules, and exception handling. 4. Analyse object-oriented programming principles and GUI development in Python. 5. Design and optimize Python programs for data handling, file operations, and database integration.			
Course Learning Outcomes (CLO):				Students will be able to: 1. Explain Python programming concepts, syntax, and constructs. 2. Illustrate built-in data structures for handling and processing data efficiently. 3. Apply control structures, loops, and functions to solve computational problems. 4. Develop object-oriented programs and graphical user interfaces using Python libraries. 5. Evaluate and integrate file handling and database connectivity in Python applications.			

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I		
Introduction to Python Programming: Introduction to Python, Features, Installation, and Python IDEs**;** Basic Syntax, Variables, Data Types, and Operators; Input/Output operations and Type Conversion; Control Statements- Conditional Statements (if-else), Loops (for, while)**;** Loop manipulation using pass, continue, break and else.	**CLO 1**	**9**

UNIT II		
Data Structures in Python: Lists- Definition, Slicing, Methods, List Comprehensions**;** Tuples- Definition, Operations, and Applications; Sets- Definition, Operations, and Use Cases**;** Dictionaries- Creating, Manipulating, and Dictionary Comprehensions; Iterators and Generators.	**CLO 2**	**9**
UNIT III		
Functions, Modules, and Exception Handling: Introduction to Functions- Built-in Functions & User-defined Functions**;** Defining and Calling Functions, Function Arguments, and Recursion**;** Anonymous Functions**;** Modules and Packages- Importing and Creating Modules**;** Exception Handling- try, except, finally, raise**;** Decorator.	**CLO3**	**9**
UNIT IV		
Object-Oriented Programming (OOP) & GUI in Python: Classes and Objects, Constructors & Destructors; Inheritance, Polymorphism, and Method Overriding; Encapsulation and Data Abstraction; GUI Programming using Tkinter (Widgets, Layouts, Event Handling); Introduction to PyQt.	**CLO4**	**9**
UNIT V		
File Handling and Database Connectivity: File Handling- Reading and Writing Files (Text, CSV, JSON), File Operations: Append, Modify, Delete; Database Connectivity using SQLite & MySQL; Performing CRUD Operations.	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

1. Mark Lutz, *Learning Python*, O'Reilly Media, 5th Edition.
2. Paul Barry, *Head First Python*, O'Reilly Media, 2nd Edition.
3. Reema Thareja, *Python Programming: Using Problem Solving Approach*, Oxford University Press.

Reference Books:

1. Allen B. Downey, *Think Python: How to Think Like a Computer Scientist*, 2nd Edition, O'Reilly Media.
2. Wesley Chun, *Core Python Applications Programming*, Pearson, 3rd Edition.
3. David Beazley & Brian K. Jones, *Python Cookbook*, O'Reilly Media.

Online & E-Learning Resources:

1. **Official Python Documentation:** https://docs.python.org/3/
2. **Python for Beginners (W3Schools):** https://www.w3schools.com/python/
3. **Python Course (GeeksforGeeks):** https://www.geeksforgeeks.org/python-programming-language/

MOOCs & Online Courses:

1. Coursera: ‘Python for Everybody’ by University of Michigan
2. Udemy: ‘Complete Python Bootcamp: From Zero to Hero’
3. edX: ‘Introduction to Python’ by Microsoft

Name of the Program:	BSc(CS)	Semester: VII	Level: UG
Course Name	**Python Programming Lab**	**Course Code/ Course Type**	UBS404/MAJM
Course Pattern	**Revised 2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/ Oral**
-	1	-	1	2	25	-	25

Prerequisite: Basic Knowledge of Computers are required.

Course Objectives (CO):	The Objectives of Python Programming are: 1. To introduce students to Python programming basics, including syntax, data types, and control structures. 2. To enable students to write modular and reusable programs using functions, recursion, and exception handling. 3. To familiarize students with Python's built-in data structures (lists, tuples, dictionaries, sets) and their applications. 4. To expose students to object-oriented programming concepts such as classes, objects, inheritance, and polymorphism using Python. 5. To provide hands-on experience in file handling, GUI development using Tkinter, and database connectivity using SQLite.
Course Learning Outcomes (CLO):	Students would be able to: 1. Demonstrate proficiency in writing Python programs using variables, data types, control structures, and loops. 2. Apply Python functions, recursion, and exception handling to develop modular and error-resilient programs. 3. Implement and manipulate Python's data structures (lists, tuples, dictionaries, sets) to solve programming problems 4. Design object-oriented solutions using Python classes, objects, inheritance, and polymorphism. 5. Develop Python applications incorporating file handling, GUI elements using Tkinter, and database operations using SQLite.

Course Contents/Syllabus: Practical Plan

Activity Number	Assignment/Practical/Activity Title	Week Number	Details	CLO	Hours
1	Introduction to Python	Week 1	• Writing basic Python scripts • Understanding variables, data types, and I/O operations	CLO1	2

2	Control Structures	Week 2	• Implementing if-else, elif, and nested conditions.	CLO1	2
3	Control Structures	Week 3	• Using loops (for, while) with break, continue, pass	CLO1	2
4	Working with Lists and Tuples	Week 4	• Performing operations on lists (slicing, sorting, list comprehension) • Implementing tuples for immutable data storage.	CLO2	2
5	Dictionaries and Sets	Week 5	• Implementing dictionaries for key-value data storage • Using sets for unique data handling and mathematical operations	CLO2	2
6	Iterators, Generators	Week 6	• Using iter() and next() for iteration • Creating generators with yield	CLO2	2
7	Functions	Week 7	• Implementing user-defined functions and recursion • Anonymous function	CLO3	2
8	Exception Handling	Week 8	• Using try-except-finally for error handling	CLO3	2
9	Modules and Packages	Week 9	• Creating custom modules and importing built-in libraries • Using standard modules like math, random, datetime • Implementing decorators to modify functions	CLO3	2
10	Object-Oriented Programming	Week 9 & 10	• Implementing classes and objects • Using constructors, destructors, inheritance, and polymorphism	CLO4	4
11	GUI Development using Tkinter	Week 11	• Designing a GUI application with buttons, labels, and input fields • Handling events using Tkinter	CLO4	2
12	File Handling in Python	Week 12 & Week 13	• Reading and writing text, CSV, and JSON files • Performing file operations (append, modify, delete)	CLO5	4

13	Database Connectivity using SQLite	Week 14 & Week 15	• Connecting Python with SQLite • Performing CRUD operations on databases	CLO5	4
Total Marks					**30 hrs**

Learning resources

Textbooks:

1. Mark Lutz, *Learning Python*, O'Reilly Media, 5th Edition.
2. Paul Barry, *Head First Python*, O'Reilly Media, 2nd Edition.
3. Reema Thareja, *Python Programming: Using Problem Solving Approach*, Oxford University Press.

Reference Books:

1. Allen B. Downey, *Think Python: How to Think Like a Computer Scientist*, 2nd Edition, O'Reilly Media.
2. Wesley Chun, *Core Python Applications Programming*, Pearson, 3rd Edition.
3. David Beazley & Brian K. Jones, *Python Cookbook*, O'Reilly Media.

Online & E-Learning Resources:

1. **Official Python Documentation:** https://docs.python.org/3/
2. **Python for Beginners (W3Schools):** https://www.w3schools.com/python/
3. **Python Course (GeeksforGeeks):** https://www.geeksforgeeks.org/python-programming-language/

MOOCs & Online Courses:

1. Coursera: 'Python for Everybody' by University of Michigan
2. Udemy: 'Complete Python Bootcamp: From Zero to Hero'
3. edX: 'Introduction to Python' by Microsoft

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>BSc(CS)</b></td><td colspan="2"><b>Semester: VII</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>AI in Cyber Security</b></td><td colspan="2"><b>Course Code and Course Type</b></td><td colspan="2">UBS405/SEC</td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>Revised 2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hours</b></td><td><b>CIA</b>
<b>(Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical and Oral</b></td></tr>
<tr><td>3</td><td>-</td><td>-</td><td>3</td><td>3</td><td>40</td><td>60</td><td>-</td></tr>
<tr><td colspan="8"><b>Prerequisite:</b> Data Mining, Knowledge of probability theory, statistics, and programming</td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of:
1. Understand the fundamentals of Artificial Intelligence (AI) and its role in Cyber Security.
2. Learn how AI techniques such as Machine Learning and Deep Learning are applied in threat detection and prevention.
3. Develop knowledge of AI-driven security systems, anomaly detection, and automated response mechanisms.
4. Gain hands-on experience in implementing AI models for Cyber Security use cases.
5. Explore ethical considerations, challenges, and future trends in AI for Cyber Security.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students will be able to:
1. To Understand the basics of Machine Learning and Deep Learning.
2. To Implement anomaly detection for threat identification.
3. To Utilize AI for automated cyber security threat detection and response
4. To Identify and implement defense mechanisms against AI-based cyber attacks.
5. To Explore real-world AI applications in Cyber Security.</td></tr>
</table>

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**HRS**
UNIT I		
Introduction to AI in Cyber Security: Applying AI in cyber security, The evolution from expert systems to data mining and AI,The different forms of automated learning, The characteristics of algorithm training and optimization, Beginning with AI via Jupyter Notebooks, Introducing AI in the context of cyber security.	**CLO 1**	9
UNIT II		

Machine Learning for Threat Detection: - Supervised, Unsupervised, and Reinforcement Learning in Cyber Security, AI-based Intrusion Detection and Prevention Systems (IDPS), Anomaly Detection using Machine Learning, Feature Engineering for Cyber Security Data, AI Techniques for Malware Analysis and Classification, Hands-on: Implementing a Simple Machine Learning Model for Threat Detection	**CLO 2**	9
UNIT III		
AI-Driven Security and Automated Response: - How to detect spam with Perceptrons, Image spam detection with support vector machines (SVMs),Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes, Spam detection adopting NLP	**CLO3**	9
UNIT IV		
Adversarial AI and Challenges: - Adversarial Machine Learning and AI Manipulation, Attack Techniques on AI Models, Defensive Mechanisms Against Adversarial Attacks, Explainable AI (XAI) in Cyber Security, Ethical Considerations and Bias in AI Models	**CLO4**	9
UNIT V		
Protecting Sensitive Information and Assets: - Authentication abuse prevention, Account reputation scoring, User authentication with keystroke recognition, Biometric authentication with facial recognition. **Fraud Prevention with Cloud AI Solutions**: How to leverage machine learning (ML) algorithms for fraud detection, How bagging and boosting techniques can improve an algorithm's effectiveness, How to analyze data with IBM Watson and Jupyter Notebook, How to resort to statistical metrics for results evaluation	**CLO5**	9
Total Hours		45 hrs

Learning resources

Textbooks:

1. Russell, S. and Norvig, P, Artificial Intelligence: A Modern Approach, Third Edition, PrenticeHall, 2010
2. Dr. Nilakshi Jain (2019). Artificial Intelligence, As per AICTE: Making a System Intelligent,Wiley Publication
3. Alessandro Parisi .(2019). Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies, Packt Publication

Reference Books:

1. Artificial Intelligence, Elaine Rich, Kevin Knight, Shivasankar B. Nair, The McGraw Hill publications, Third Edition, 2009. 2. George F. Luger, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Pearson Education, 6th ed., 2009

Name of the Program:	BSc(Cyber Security)	**Semester: VII**	**Level: UG**
Course Name	Security in Wireless Ad Hoc Networks	**Course Code and Course Type**	UBS406/VSC
Course Pattern	**Revised 2024**	**Version**	1.0

Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
3	-	-	3	45	40	60	-

Prerequisite:

Course Objectives (CO):	The objectives of: 1. Understand the fundamental concepts of wireless Ad Hoc networks, including their characteristics, types, and applications. 2. Analyze various security challenges in wireless Ad Hoc networks, including attacks, vulnerabilities, and trust models. 3. Apply cryptographic techniques, key management strategies, and secure routing mechanisms to protect Ad Hoc networks. 4. Evaluate security protocols, energy-efficient security mechanisms, and intrusion detection techniques for communication security in wireless Ad Hoc networks. 5. Explore emerging trends, including blockchain, AI/ML, and quantum cryptography, to enhance the security of next-generation wireless Ad Hoc networks.
Course Learning Outcomes (CLO):	Students will be able to: 1. Explain the fundamental concepts, types, and applications of wireless Ad Hoc networks. 2. Identify various security threats, vulnerabilities, and attack models in Ad Hoc networks. 3. Implement cryptographic techniques and secure routing mechanisms to protect Ad Hoc networks. 4. Assess wireless security protocols, intrusion detection techniques, and energy-efficient security strategies. 5. Investigate emerging security technologies such as blockchain, AI-based intrusion detection, and quantum cryptography for securing wireless Ad Hoc networks.

Course Contents and Syllabus:

Descriptors and Topics	CLO	Hours
UNIT I : Introduction to Wireless Ad Hoc Networks		
Overview of Wireless Networks: Introduction to Wireless Networks, Introduction to wireless communication and networks, Introduction to Infrastructure-based and Ad Hoc networks, Differences between Infrastructure-based and Ad Hoc networks, Applications: Military, healthcare, disaster recovery, IoT, Ad Hoc Networks Basics: Characteristics, limitations, and challenges, Types of Ad Hoc networks: MANETs, VANETs, FANETs, and WSNs, Importance of dynamic topology and self-organization, Routing in Ad Hoc Networks: Routing protocols: Proactive (e.g., OLSR), Reactive (e.g., DSR, AODV), and Hybrid (e.g., ZRP), Challenges in routing: Scalability, reliability, and energy constraints	**CLO1**	9
UNIT II : Security Challenges in Wireless Ad Hoc Networks		
Security Problems in Ad Hoc Networks: Attacks on routing: Wormhole, Blackhole, Grayhole, and Sybil, Denial-of-Service (DoS) attacks and their effects, Vulnerabilities in wireless communication, Requirements for Security: Importance of confidentiality, integrity, availability, and authentication, Secure routing and data integrity in wireless networks, Trust and Cooperation: What is trust?, Simple trust-building techniques, Trust models: Direct, indirect, and hybrid approaches, Reputation-based systems for secure communication, Case Studies: Analysis of real-world Ad Hoc network security incidents	**CLO 2**	9
UNIT III : Basic Security Techniques for Wireless Ad Hoc Networks		
Introduction to Cryptography: Symmetric vs. asymmetric cryptography, Lightweight cryptographic algorithms (e.g., RC5, AES). End-to-end vs. hop-by-hop encryption, Key Management: Basics of key generation and distribution, Public Key Infrastructure (PKI) and Certificate Authorities (CAs), Securing Routing Protocols:Enhancements to protocols like AODV and DSR,Cryptographic techniques for secure routing, Intrusion Detection: What is intrusion detection?, Types: Signature-based and anomaly-based detection, Cooperative intrusion detection in Ad Hoc networks	**CLO3**	9
UNIT IV : Communication Security in Wireless Ad Hoc Networks		
Wireless Security Protocols: Basics of WPA, WPA2, and WPA3, Encryption in wireless protocols (AES, TKIP), IEEE 802.11 security mechanisms, Energy-efficient Security: Designing lightweight security protocols for resource-constrained devices, Balancing energy consumption and security in IoT networks, Secure Data Aggregation: Aggregation protocols for secure data fusion, Protecting data during collection and aggregation, Ensuring data integrity and privacyCase Studies: Security implementation in smart home IoT networks	**CLO4**	9
UNIT V : Emerging Trends and Case Studies in Wireless Ad Hoc Network Security		
New Challenges: Security in IoT-based and 5G-enabled Ad Hoc networks, Role of AI and ML in detecting new threats, Blockchain for Ad Hoc Networks: Basics of blockchain technology, Decentralized trust and security using blockchain, Blockchain-enabled secure routing,Quantum Cryptography: Introduction to quantum computing, Impact of quantum cryptography on wireless security,Future Directions: Security challenges in 6G Ad Hoc networks, Integration of edge computing and Ad Hoc networks,Case Studies:Quantum-resistant algorithms for Ad Hoc networks, AI-based intrusion detection in smart cities, Case study on secure communication in a disaster management Ad Hoc network	**CLO5**	9
Total Hours		45

Learning resources

Reference Books:

1. "Ad Hoc Wireless Networks: Architectures and Protocols" by C. Siva Ram Murthy and B.S. Manoj Publisher: Pearson Education
2. "Wireless Security: Models, Threats, and Solutions" by Randall K. Nichols and Panos C. Lekkas Publisher: McGraw-Hill
3. "Security for Wireless Sensor Networks" by Ankur Dumka and Parveen Kumar Publisher: CRC Press

Online Resources and E-Learning Resources

1. IEEE Xplore Digital Library: https://ieeexplore.ieee.org/
2. SpringerLink: https://link.springer.com/
3. ResearchGate: https://www.researchgate.net/
4. NIST Cybersecurity: https://www.nist.gov/cybersecurity

Name of the Program:		**BSc(Cyber Security)**	**Semester: VII**			**Level: UG**	
Course Name		**Cyber Crime**	**Course Code and Course Type**			**UBSM111(MOOC)**	
Course Pattern		**Revised 2024**	**Version**			**1.0**	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
-	-	-	2	2	25	-	25
Prerequisite:							
Course Objectives (CO):			The objectives of: 1. Understand the Foundations of Cybercrime and Legal Frameworks. 2. Identify and Analyze Cybercrime Techniques and Tools. 3. Apply Cybercrime Investigation and Digital Forensic Techniques. 4. Evaluate Legal, Ethical, and Policy Implications of Cybercrime. 5. Explore Emerging Trends and Real-World Case Studies in Cybercrime.				
Course Learning Outcomes (CLO):			Students will be able to: 1. Describe the evolution, types, and impact of cybercrime within the context of global cyber laws and policies. 2. Identify and explain various cyberattack techniques, tools, and tactics used by cybercriminals. 3. Demonstrate the ability to conduct basic cybercrime investigations and apply digital forensic methods to analyze digital evidence. 4. Critically evaluate legal, ethical, and jurisdictional issues related to cybercrime and cybersecurity governance. 5.Analyze and interpret contemporary cybercrime trends and real-world case studies to propose informed prevention and response strategies.				

Course Contents and Syllabus:

Descriptors and Topics	CLO	Hours
UNIT I Introduction to Cybercrime and Cyber Law		
Introduction to Cybercrime: Definition and Evolution, Types and Classifications of Cybercrimes, Historical Case Studies of Major Cybercrimes, Cybercrime vs. Traditional Crime, Overview of Cyber Law: Global Perspectives, Key Cybercrime Legislation	**CLO 1**	6
UNIT II Cybercrime Techniques and Tools		
Malware and Ransomware: Mechanisms and Impact, Phishing, Spoofing, and Social Engineering, Hacking and Unauthorized Access Techniques, Denial-of-Service (DoS) and DDoS Attacks, Identity Theft and Financial Frauds, Dark Web, and Cybercrime Marketplaces	**CLO 2**	6
UNIT III Cybercrime Investigation and Forensics		
Cybercrime Investigation Process and Stakeholders, Digital Evidence: Collection, Preservation, and Chain of Custody, Network Forensics and Traffic Analysis, Mobile Device and Cloud Forensics, Tools, and Software for Cyber Forensics, Writing Cybercrime Investigation Reports	**CLO3**	6
UNIT IV Legal, Ethical, and Policy Issues		
Jurisdiction in Cyberspace, Data Protection Laws, and Privacy Regulations, Ethical Hacking vs. Criminal Hacking, Intellectual Property in Cyberspace, Cybersecurity Policies and Governance, International Cooperation in Fighting Cybercrime (e.g., INTERPOL, Budapest Convention)	**CLO4**	6
UNIT V Emerging Trends and Case Studies		
AI and Machine Learning in Cybercrime and Cybersecurity, Cyber Terrorism and Warfare, Cryptocurrency Crimes and Blockchain Forensics, Cybercrime in Social Media and Online Platforms, Real-World Case Studies, Future Challenges and Career Paths in Cybercrime and Cyber Law	**CLO5**	6
Total Hours		**30**

Learning resources

Textbooks:

1. **"Cyber Crime and Cyber Security"** by Alfred Basta, Nadine Basta, and Patrick Zgola

2. "Cybercrime and Digital Forensics: An Introduction" by Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar

3. "Cyber Law: The Law of the Internet and Information Technology" by Mark F. Grady, Francesco Parisi

Reference Books:

1. "Investigating Cyber Crime: An Introduction to the Digital Forensic Process" by Babak Akhgar, Andrew Staniforth, Francesca Bosco

2. "Scene of the Cybercrime" by Debra Littlejohn Shinder and Michael Cross

3. "Computer Forensics: Cybercriminals, Laws, and Evidence “by Marie-Helen Maras

Online Resources and E-Learning Resources

1. Coursera – Cybersecurity Specialization (by University of Maryland)

https://www.coursera.org/specializations/cyber-security

2. edX – Cybersecurity Fundamentals (by Rochester Institute of Technology)

https://www.edx.org/professional-certificate/ritx-cybersecurity-fundamentals

3. FutureLearn – Cyber Security Operations https://www.futurelearn.com/courses/cyber-security-operations

Name of the Program:		**BSc (CS)**		**Semester: VII**		**Level: UG**	
Course Name		**Threat Investigation**		**Course Code/ Course Type**		**UBSM112(MOOC)**	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical/Oral**
2	-	-	2	2	20	30	–
Prerequisite: Basic: Basic knowledge of networking, operating systems, and cybersecurity fundamentals.							
Course Objectives (CO):				The objectives of Threat Investigation are: 1. Understand the fundamentals of threat intelligence and cyber threat landscapes. 2. Identify, analyse, and interpret indicators of compromise (IOCs) and attack vectors. 3. Utilize investigative tools and techniques to detect, track, and attribute cyber threats. 4. Apply digital forensics principles in collecting and preserving evidence for threat investigation. 5. Develop and present comprehensive threat reports to support incident response and mitigation.			
Course Learning Outcomes (CLO):				Students Will be able to: 1. Explain the key concepts of cyber threat intelligence and the evolving threat landscape 2. Detect and interpret indicators of compromise (IOCs) and assess different types of cyber threats and attack vectors. 3. Apply appropriate tools and techniques to investigate and trace the origin and behavior of cyber threats. 4. Demonstrate the ability to collect, preserve, and analyze digital evidence in accordance with forensic standards. 5. Produce structured threat investigation reports and communicate findings effectively to stakeholders.			

Course Contents/Syllabus:

Descriptors/Topics	CLO	Hours
UNIT I		
Introduction to Cyber Threat Intelligence: What is Cyber Threat Intelligence (CTI), Types and sources of cyber threats (internal, external, nation-state, etc.), Threat actors and their motivations, Cyber kill chain and MITRE ATT&CK framework, The evolving global threat landscape	**CLO 1**	**6**
UNIT II		
Indicators of Compromise (IOCs) and Attack Vectors: What are IOCs? (IP addresses, hashes, domains, etc.); Types of attack vectors (phishing, malware, ransomware, etc.); Identifying and classifying threats using IOCs; IOC enrichment and validation using open-source tools.	**CLO 2**	**6**
UNIT III		
Threat Investigation Tools and Techniques: Overview of threat hunting and investigation; Common tools: Wireshark, Splunk, ELK stack, OSINT tools; Log analysis and network traffic inspection; Real-world threat case analysis	**CLO3**	**6**
UNIT IV		
Basics of Digital Forensics for Threat Investigation: Introduction to digital forensics; Evidence collection and chain of custody; Volatile vs non-volatile data; File system analysis and memory forensics; Forensics tools: Autopsy, FTK Imager, Volatility	**CLO4**	**6**
UNIT V		
Threat Reporting and Communication Structure of a threat investigation report; Key components: Summary, IOCs, analysis, recommendations; Communicating findings to technical and non-technical audiences; Sharing intelligence: STIX/TAXII formats, ISACs; Ethical and legal considerations in threat reporting.	**CLO5**	**6**
Total Hours		**30**

Text Books:

1. Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer & Allan Friedman.
2. "Investigating Windows Systems" by Harlan Carvey, Publisher: Syngress

Reference Books:

1. Intelligence-Driven Incident Response: Outwitting the Adversary, Scott J. Roberts, Rebekah Brown
2. The Practice of Network Security Monitoring: Understanding Incident Detection and Response, Richard Bejtlich.

Online Resources and e-learning resources:

Threat Investigation | Coursera

https://www.youtube.com/results?search_query=wireshark+tutorial

.

B.Sc.(Cyber Security) Revised 2024 PATTERN
COURSE DETAILS
Semester - VIII

Name of the Program:		**BSC(CS)**		**Semester: VIII**		**Level: UG**	
Course Name		**Google Cyber Security Professional Certificate**		**Course Code and Course Type**		**UBSM113 (MOOC)**	
Course Pattern		**Revised 2024**		**Version**		1.0	
Teaching Scheme					**Assessment Scheme**		
Theory	**Practical**	**Tutorial**	**Total Credits**	**Hours**	**CIA (Continuous Internal Assessment)**	**ESA (End Semester Assessment)**	**Practical and Oral**
3	-	-	3	3	50	-	50

Prerequisite: Computer Fundamentals and Networking.

Course Objectives (CO):	The Objectives of the Course are:- 1. To Identify and define fundamental cybersecurity concepts, including risks, threats, vulnerabilities, and security frameworks. 2. To Explain the importance of cybersecurity practices and their impact on organizations, ensuring data protection and network security. 3. To utilize industry-standard tools such as Python, Linux, and SQL to analyze security incidents and mitigate potential threats. 4. To examine security logs and network traffic to detect anomalies and potential cyber threats using Security Information and Event Management (SIEM) tools. 5. To assess cybersecurity strategies and recommend improvements to enhance security posture and prevent unauthorized access.
Course Learning Outcomes (CLO):	Students will be able to: 1. To recall key cybersecurity concepts, including risk management, threat detection, and security frameworks. 2. To explain the significance of cybersecurity measures in protecting networks, systems, and sensitive data. 3. To implement security protocols and use industry-standard tools like Python, Linux, and SIEM systems to analyze and mitigate threats. 4. To examine security incidents and assess vulnerabilities to identify patterns and potential risks. 5. To critically assess cybersecurity strategies and recommend improvements to enhance security posture and prevent cyberattacks.

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I		
Foundations of Cybersecurity:	**CLO 1**	**9**

Introduction to cybersecurity Concepts, Evolution of Cyber Security, Understanding risks, threats, and vulnerabilities, Cybersecurity frameworks (NIST, ISO 27001, CIS Controls), Cybersecurity principles: Confidentiality, Integrity, and Availability (CIA Triad),Ethical hacking and security policies, Basics of encryption and secure communication, Ethical considerations in cybersecurity		
UNIT II		
Network Security & Threat Management Fundamentals of network security and architecture, Firewalls, VPNs, and intrusion detection systems (IDS), Security Information and Event Management (SIEM) tools, Network traffic analysis and anomaly detection, Incident response and forensic analysis.	**CLO 2**	**9**
UNIT III		
Security Tools & Technologies Network Security Tools, Intrusion Detection & Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs), Network traffic analysis tools (Wireshark), Endpoint Security Tools, Identity & Access Management (IAM), Security Information & Event Management (SIEM).	**CLO3**	**9**
UNIT IV		
Cyber Threat Detection & Response Identifying and mitigating cyber threats, Security monitoring and log analysis, Advanced persistent threats (APT) and attack vectors, Responding to security incidents effectively, Cybersecurity Compliance and regulatory requirements.	**CLO4**	**9**
UNIT V		
Cybersecurity Strategy & Risk Assessment Understanding cybersecurity frameworks, Aligning cybersecurity strategy with business objectives, Implementing security governance and leadership, Identifying and categorizing cyber threats, Conducting vulnerability assessments and penetration testing, Risk analysis techniques (quantitative vs. qualitative), AI and machine learning in cybersecurity risk management, Zero-trust architecture and adaptive security models, Cybersecurity risk assessment in cloud environments	**CLO5**	**9**
Total Hours		**45**

Learning resources
Textbooks:

Cybersecurity Essentials – Charles J. Brooks, Christopher Grow, Philip Craig, & Donald Short Publisher: Wiley
The Web Application Hacker's Handbook" – Dafydd Stuttard & Marcus Pinto:Wiley
Cybersecurity and Cyberwar: What Everyone Needs to Know" – P.W. Singer & Allan Friedman: Oxford University Press.

Reference Books:
1**.** Computer Security: Principles and Practice" – William Stallings & Lawrie Brown-Pearson.
2. "Hacking: The Art of Exploitation" – Jon Erickson: No Starch Press

Online Resources and E-Learning Resources

https://github.com/9QIX/Google-Cybersecurity-Certification-Notes

https://www.cisa.gov/
https://owasp.org/

https://www.nist.gov/cyberframework

<table>
<tr><td colspan="2"><b>Name of the Program:</b></td><td colspan="2"><b>B.Sc.(CS)</b></td><td colspan="2"><b>Semester: VIII</b></td><td colspan="2"><b>Level: UG</b></td></tr>
<tr><td colspan="2"><b>Course Name</b></td><td colspan="2"><b>Security Analyst Fundamentals Specialization</b></td><td colspan="2"><b>Course Code and Course Type</b></td><td colspan="2"><b>UBSM114 (MOOC)</b></td></tr>
<tr><td colspan="2"><b>Course Pattern</b></td><td colspan="2"><b>Revised 2024</b></td><td colspan="2"><b>Version</b></td><td colspan="2">1.0</td></tr>
<tr><td colspan="5"><b>Teaching Scheme</b></td><td colspan="3"><b>Assessment Scheme</b></td></tr>
<tr><td><b>Theory</b></td><td><b>Practical</b></td><td><b>Tutorial</b></td><td><b>Total Credits</b></td><td><b>Hours</b></td><td><b>CIA (Continuous Internal Assessment)</b></td><td><b>ESA (End Semester Assessment)</b></td><td><b>Practical and Oral</b></td></tr>
<tr><td>3</td><td>-</td><td>-</td><td>3</td><td>3</td><td>50</td><td>-</td><td>50</td></tr>
<tr><td colspan="8"><b>Prerequisite:</b> Computer Fundamentals and Networking.</td></tr>
<tr><td colspan="4">Course Objectives (CO):</td><td colspan="4">The objectives of the Course are: -
1. To introduce the core concepts of penetration testing and threat intelligence.
2. To develop a strong understanding of cryptographic principles and techniques.
3. To Build competence in incident response and digital forensics
4. To enhance practical problem-solving abilities through hands-on projects.
5. To analyze the different cases of Digital Forensic.</td></tr>
<tr><td colspan="4">Course Learning Outcomes (CLO):</td><td colspan="4">Students will be able to:
1. Demonstrate knowledge of penetration testing methodologies.
2. Identify and utilize threat hunting and intelligence techniques.
3. Apply cryptographic principles to secure information.
4. Perform basic vulnerability assessments and penetration testing tasks.
5. Understand and implement incident response procedures.</td></tr>
</table>

Course Contents and Syllabus:

Descriptors and Topics	**CLO**	**Hours**
UNIT I		
Penetration Testing, Threat Hunting, and Cryptography: Penetration Testing -Planning & Discovery Phase, Attack Phase , Reporting Phase, Threat Hunting and Threat Intelligence,	**CLO 1**	**9**

UNIT II		
Cryptography: Principle & Techniques, Final Project & Wrap-up- Final Project: Submission and Evaluation, Final Project: Part 2 - Secure Information Using Symmetric Encryption Final Project: Part 1 - Perform Vulnerability Analysis and Penetration Testing	**CLO 2**	**9**
UNIT III		
Incident Response and Digital Forensics: What is Incident Response?, Incident Response: Preparation, Incident Response: Detection and Analysis , Containment, Eradication, and Recovery , Post-incident Activities, **Digital Forensics-** Data Collection and Examination , Analysis and Reporting , Forensic Data: Data Files	**CLO3**	**9**
UNIT IV		
Cybersecurity Case Studies- Course Introduction, Overview of Phishing Scams, Phishing Case Study: Google and Facebook, Vishing Case Study: South Korean Doctor, Analyzing POS and Insider Breach Case studies, Analyzing AI related Breaches & Ransomware case studies	**CLO4**	**9**
UNIT V		
Cybersecurity Case Studies : Analyzing Incident Response & Digital Forensic Case studies, Analyzing Penetration Testing and Compliance case studies, Final Project work-wrap-up	**CLO5**	**9**
Total Hours		**45**

Learning resources

Textbooks:

- "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman
- "Incident Response & Computer Forensics" by Jason Luttgens, Matthew Pepe, and Kevin Mandia
- Computer Security: Principles and Practice" by William Stallings & Lawrie Brown

Reference Books:

Cybersecurity Case Studies" by Josiah Dykstra