BCA (Semester- 6)

Teaching Schedule

030010608: SEC1 Fundamentals of Cyber Security

Objective: To imbibe the fundamentals of cybersecurity and its legal perspectives as well as examine the need of cryptography and digital forensics for securing information in the cyber world.

Course Outcomes: Upon completion of the course, the student shall be able to

CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types.
CO2: Classify various types of cyber attacks.
CO3: Classify and relate methods used in cybercrime along with security mechanism.
CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security.
CO5: Identify the need for cyber laws, especially in the Indian context.
CO6: Describe the fundamentals of digital forensics with its phases, rules and techniques.

Unit	Sub Unit	No. of Lecture(s)	Topics	Reference Chapter/Additional Reading	Teaching Methodology to be used	Evaluation Parameters
Unit 1 : CyberSecurity						
1	1.1	1	Basic Terminologies: Cybercrime, Cybersecurity, Cyberspace, Cybersquatting, Cyberpunk, Cyberwarfare, and Cyberterrorism	NG #1 Page no. 02 – 04 https://www.coursera.org/learn/cyber-conflicts/lecture/Pp5sI/introduction-to-cyberwarfare	Presentation, Audio-visual	
	1.2	1	Needs of Cyber Security	NG #1 Page no. 13	Presentation	
	1.3		Cyber Criminals : Introduction and Types	NG #1 Page no. 16 - 17	Presentation	
	1.4	1	Planning Cyber Attacks: Phases and Types	NG #2 Page no. 49 – 61 https://www.courser	Chalk and talk and Audio-visual	

				a.org/learn/cyber-conflicts/lecture/69Ikc/cyber-attacks-in-a-global-context		
	1.5	2	Cybercrimes Classifications	NG #1 Page no. 17 - 22	Presentation	
Unit 2 : Cyber Offences						
2	2.1	2	Social Engineering: Overview and Classifications	NG #2 Page no. 61 - 63	Presentation	Quiz
	2.2		Cyberstalking: Types and Working	NG #2 Page no. 65 - 66		
	2.3	1	Botnet: Introduction	NG #2 Page no. 71 - 72	Open text book study	
	2.4		Attack Vector: Overview and Working	NG #2 Page no. 73 - 75		
	2.5	1	Mobile Devices Attacks	https://www.itproportal.com/news/cyber attacks-against-mobile-devices-on-the-rise/ https://www.devry.edu/blog/2017/04/mobile-devices-are-vulnerable.html	Presentation	
Unit 3 : Cybercrime Methods and Security Mechanisms						
3	3.1	1	Phishing : Introduction, Techniques and Prevention	NG #5 Page no. 187, 193, 202,203	Presentation	
	3.2	1	Identity Theft: Types, Techniques and Prevention	NG #5 - Page No. 206 – 221	Presentation and	Unit Test-1

					Demonstration	
	3.3	1	DoS Attack : Classification, Types and Prevention	NG #4 - Page No. 158 – 162	Chalk and talk	
	3.4	2	DDoS Attack : Introduction and Prevention	NG #4 - Page No. 162 – 164		
	3.5	1	SQL Injection : Introduction and Prevention	NG #4 - Page No. 164– 167	Presentation	
Unit – 4: Cryptography and Digital Signature						
4	4.1	1	CIA: Confidentiality, Integrity and Availability	VK #1 Page No-2	Chalk and talk	
	4.2	1	Overview of Symmetric-Key Cryptography	VK #2 Page No-15-17 https://www.coursera.org/learn/basic-cryptography-and-crypto-api/lecture/1W0Os/course-overview	Presentation	
	4.3	1	Overview of Asymmetric-Key Cryptography		Demonstration and Audio-visual	
	4.4	1	Hash Functions: Overview and Usage	VK #9 Page No-222-223	Presentation	
	4.5	1	Digital Signature: Introduction and Importance	VK #10 Page No-241-243		Open Book Test
Unit – 5: Legal Perspectives of Cyber Security						
5	5.1	1	Need of Cyber Laws : Reasons for Enactment of Cyber Laws in India	NG #6 - Page No. 253– 254 https://www.coursera.org/learn/cyber-security-domain/lecture/GfKZj/legal-regulations-investigations-and-compliance	Open textbook study and Audio-visual	
	5.2		Indian ITA : ITA Sections	NG #6 - Page No. 254 –		

				263		
	5.3	1	Digital Signature and ITA: Public Key Certificate	NG #6 - Page No. 273	Chalk and talk	
	5.4	1	Representation of Digital Signatures in ITA	NG #6 - Page No. 274 – 275 http://nptel.ac.in/courses/110106064/41	Presentation and Audio-visual	
	5.5		Cryptographic Perspective of ITA	NG #6 - Page No. 279 – 281	Presentation	
Unit – 6: Cyber Forensics Fundamentals						
6	6.1	1	Needs	NG #7- Page No. 323– 327	Classroom discussion	Unit Test-2
	6.2		Computer Forensics and Digital Forensics		Presentation	
	6.3	1	Role of Digital Forensics	NG #7 - Page No. 320 – 323	Presentation	
	6.4	1	Rules of Evidence	NG #7 - Page No. 327 – 331		
	6.5	1	Digital Forensics Phases	NG #7 - Page No. 339 – 353	Presentation	Internal Exam
	6.6	1	Digital Forensics Techniques	NG #7 - Page No. 402 – 403	Presentation	
References : 1. Nina Godbole, Sunit Belapure - Cyber Security – Understanding Cyber Crimes, Computer Forensics and Legal Perspectives - Wiley. [NG] 2. Marjie T. Britz - Computer Forensics and Cyber Crime: An Introduction - Prentice Hall. [MB] 3. George M. Mohay - Computer and Intrusion Forensics - Artech House. [GM] 4. V. K. Pachghare, Cryptography and Information Security, 2nd Edition, PHI Learning. [VK] Note: # denotes chapter number.						

Course Objectives and Course Outcomes Mapping:

- To imbibe the fundamentals of cybersecurity and its legal perspectives: CO1, CO2, CO3, CO5
- Examine the need of cryptography and digital forensics for securing information in the cyber world: CO4, CO5,CO6

Course units and Course outcome mapping:

Unit No.	Unit	Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Cyber Security	√	√				

2	Cyber Offences	√	√				
3	Cybercrime Methods and Security Mechanisms		√	√			
4	Cryptography and Digital Signature				√		
5	Legal Perspectives of Cyber Security		√		√	√	
6	Digital Forensics Fundamentals		√				√

Programme Outcomes:

PO1: Ability to understand the concepts of key areas in computer science.

PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society.

PO3: Effective communication and presentation skill.

PO4: Ability to understand professional and ethical responsibility.

PO5: Recognition of the need for life-long learning.

Programme Outcomes and Course Outcomes mapping:

Programme Outcome	**Course Outcomes**					
	CO1	CO2	CO3	CO4	CO5	CO6
PO1	✓	✓	✓			
PO2			✓	✓		
PO3	✓	✓	✓	✓	✓	✓
PO4					✓	✓
PO5					✓	✓

Modes of Transaction (Delivery):

Unit No	**Topic Detail**	**Teaching Approach**	**PO mapped**

2	1.5 Classification of Cybercrime 2.1 Social Engineering	Open textbook study (Students shall be given questions based on scenario and they have to find the answers from the book)	PO1
4	3.1 Phisphing 3.2 Identify Theft	Group discussion: Group will be form by teacher. Student shall discuss on Phishing and Identity Theft.	PO1, PO3

Activities/Practicum:

The following activities shall be carried out by the students:

- Describe key points of countermeasures against cyber attacks.
- Depict basics of VIRUS.

The following activities shall be carried out by the teacher:

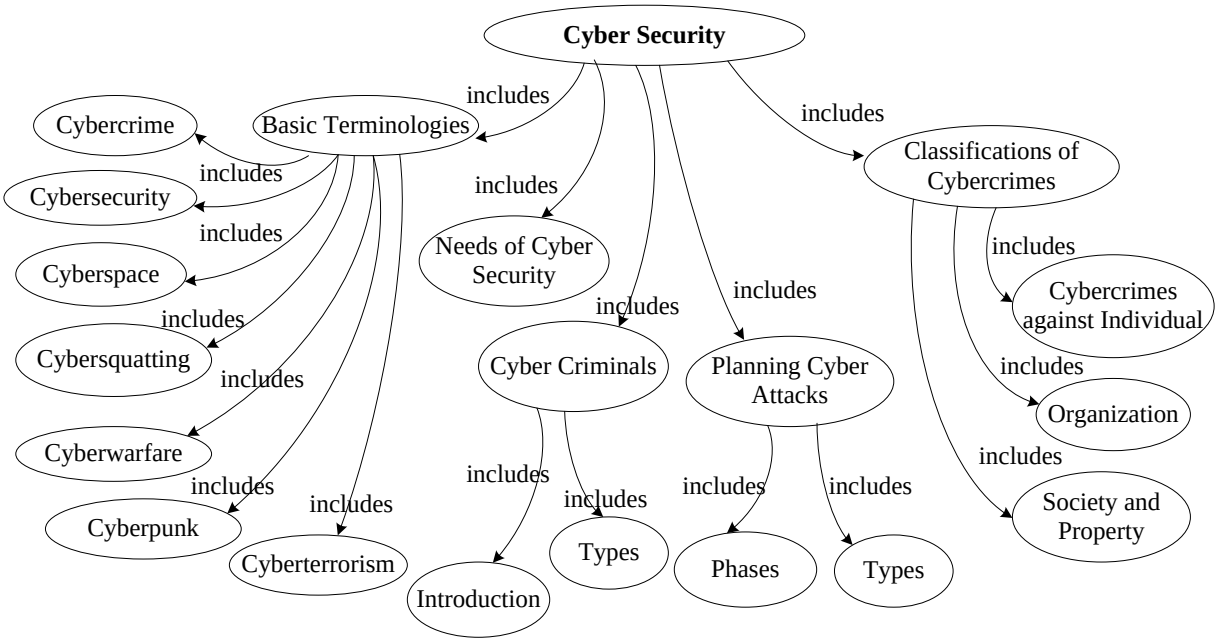
Learner	Activities to be done	PO mapped
For slow learners	After completion of every unit, a bowl containing chits with question(s) for all the topics from that unit is given by teacher. The student selected by teacher shall pick a chit of his choice from bowl and discuss answer for the question(s) available in chit in classroom.	PO1, PO3
For advanced learners	Offering various case studies for analysis.	PO1, PO3

For all	Discussion of recent trends in Cyber Security.	PO1, PO2,PO3,PO4

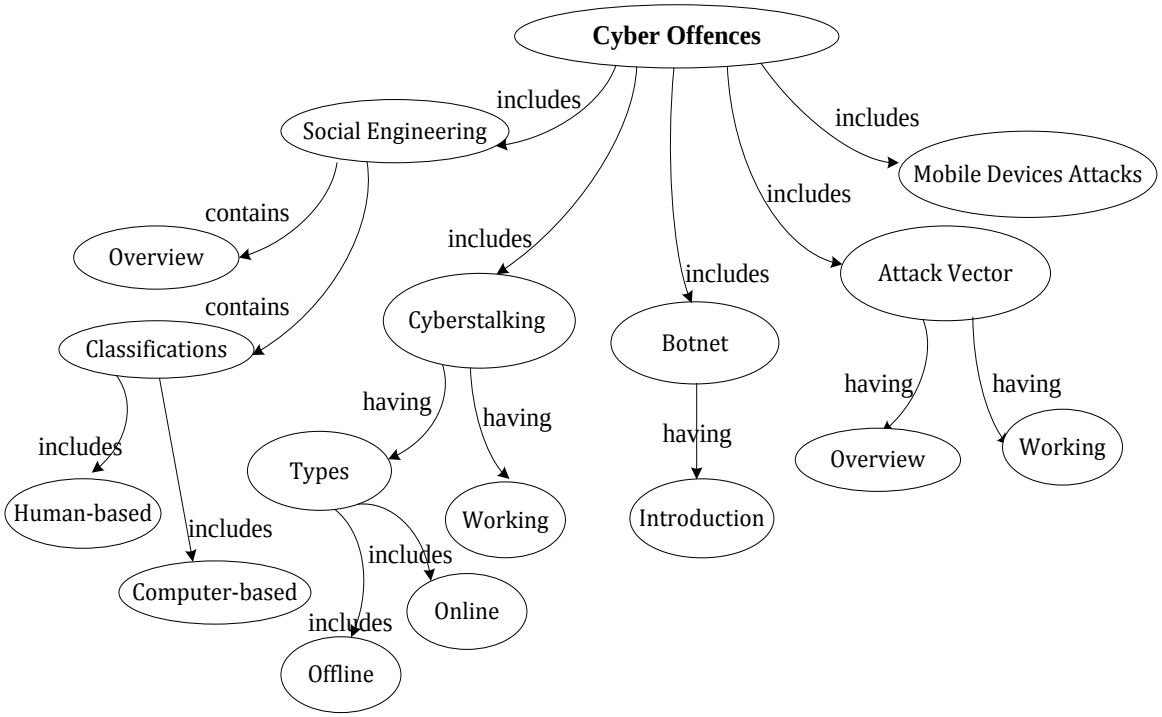
Concept map:

It is a hierarchical / tree based representation of all topics covered under the course. This gives direct / indirect relationship /association among topics as well as subtopics.

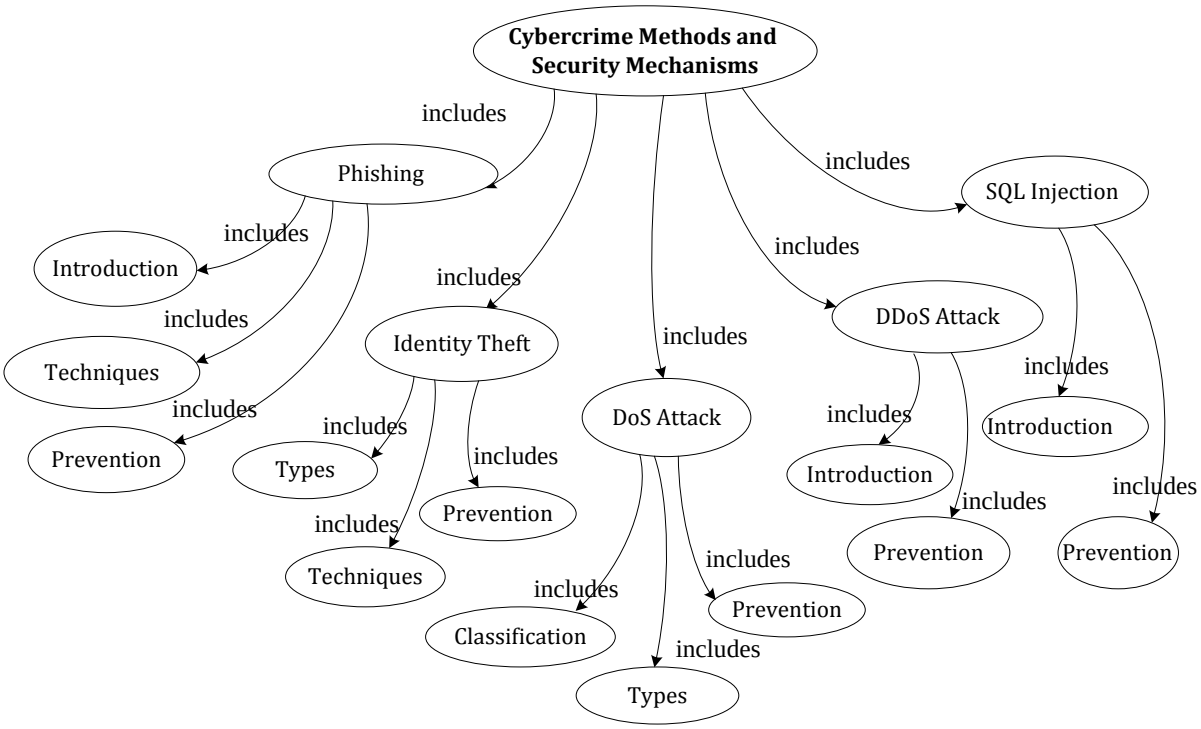
Unit-1: `Cyber Security



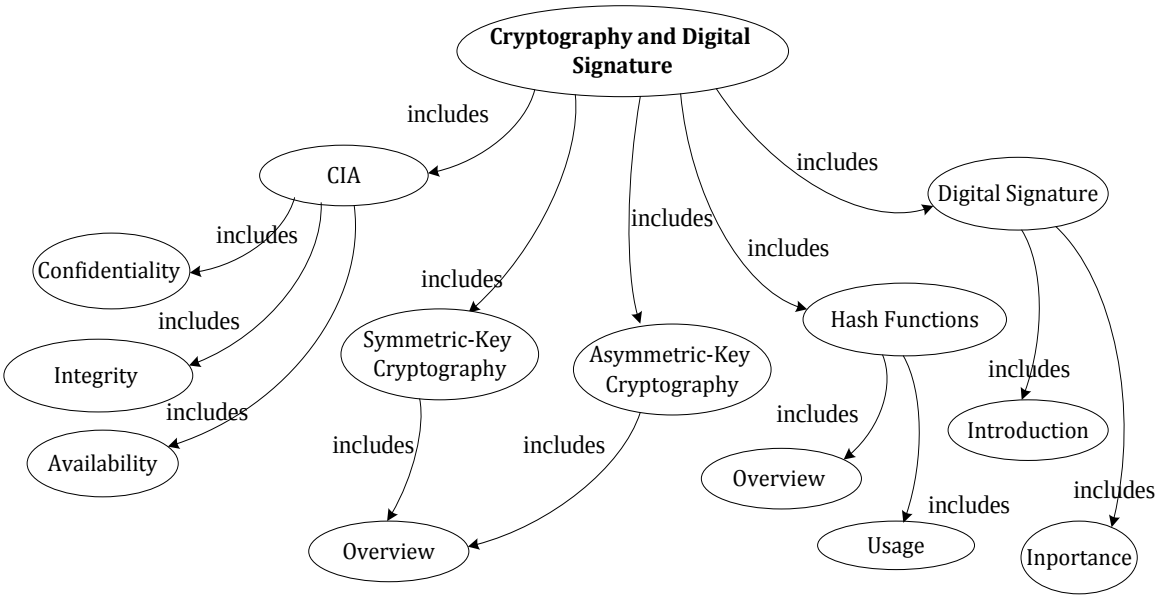
Unit-2: Cyber Offenses



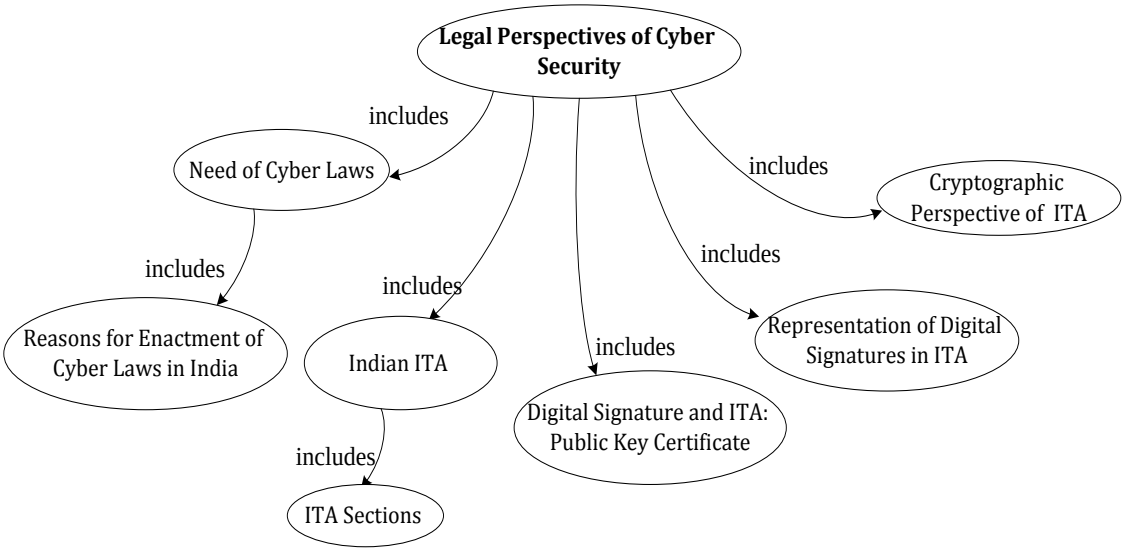
Unit-3: Cyber Crime Methods and Security Mechanisms



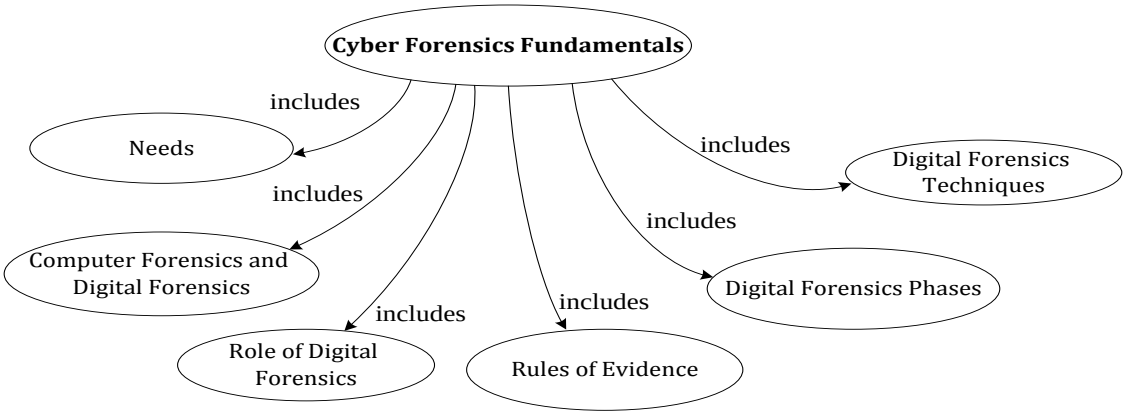
Unit-4: Cryptography and Digital Signature



Unit-5: Legal Perspectives of Cyber Security



Unit-6: Cyber Forensics Fundamentals



UFM:

- If two or more submitted answer papers are too similar for coincidence, a penalty shall be imposed that shall usually be the same for the student who did the original as for the one copying from it.
- Any ascertained fact of breaking institute policy shall be associated with one or all of the following: (i) zero marks for the work; (ii) report to the Program Coordinator; (iii) report to the Director