MCA (4th Semester)

Teaching Schedule

040010420: Information Security and Digital Forensics

Prior Topic Learning: Number Theory, Modular Arithmetic, Discrete and logarithms.

Course Objective: To develop skills to describe the usage of cryptography algorithms, digital signature, authentication and authorization for securing data. Also determine the kinds of cybercrimes and associate aspects of digital forensics.

Course Outcomes: Upon completion of the course, the student shall be able to
CO1: Describe security attacks and principles, cryptosystem related terminologies and techniques.
CO2: Apply security to data using symmetric key cryptography, asymmetric key cryptography, hash functions and digital signature.
CO3: Apply authentication and authorization methods to securing information.
CO4: Comprehend and recognize the implications of cybercrimes and related security mechanisms.
CO5: Describe the fundamentals of digital forensics with its phases, rules and techniques.

Programme Outcomes:
PO1: Proficiency in and ability to identify problems related to computer science as well as design and apply computational knowledge to solve them.
PO2: Ability to design, develop, test and maintain system, component, product or process as per needs and specification.
PO3: Understanding of professional and ethical role and responsibility.
PO4: Recognition of the need for and an ability towards life-long learning
PO5: Knowledge of programming languages, database systems, operating systems, software engineering, Web & Mobile technology and relevant modern issues.
PO6: Ability to demonstrate the use of modern tools, models and languages to solve problems related to software development
PO7: An ability to communicate and present knowledge effectively.

Programme Educational Objectives:
PEO1: To provide sound foundation in the fundamentals of computer application for life-long learning through quality education.
PEO2: To provide solid foundation knowledge to comprehend, analyze, design, test and create problem solving attitude and research aptitude.
PEO3: To provide technical skill of tools and technologies to succeed in profession as technocrat, entrepreneur, researcher and/or academician.
PEO4: To inculcate professional and ethical attitude alongwith teamwork, presentation, effective report writing and communication to become leaders in service to industry and society.

Semester Objectives:
SO1: Enhance reading skill

SO2: Enhance technical writing skill
SO3: Enhance communication skill
SO4: Promote class participation

Unit-1: Introduction to Information Security				
Course Outcome: CO1				
Programme Outcome: PO1, PO2, PO3, PO6				
Programme Educational Objectives: PEO1, PEO2				
Semester Objectives: SO1, SO2, SO3				
Sub Unit	**Lesson Duration (Hour)**	**Summary of Topic**	**Study Material**	**Teaching Approach**
-	1	Introduction of subject - Objective and role of course in professional carrier - Discussion on Lesson Plan & Assessment Policy	-	Discussion
1.1	1	Terminologies: Cryptology, Cryptography, Cryptanalysis, Plain Text, Cipher Text, Encryption, Decryption, Stream Cipher and Block Cipher	VK#1- Page no: 7-9 DNS #2 Page no. 12	Presentation
1.2	1	Security Principles: - Confidentiality - Integrity - Availability - Authentication - Non-repudiation	VK#1- Page no: 2-3, AK#1- Page no: 8-11, DNS #1 Page no. 2	Presentation
1.3	1	Security Attacks: - Introduction - Types: - Passive Attack - Active Attack	VK#1- Page no: 9-12	Discussion and Chalk & Talk
1.4	2	Cryptography Techniques: - Simple Substitution Cipher: Definition , usage and example - Double Transposition Cipher: Definition , usage and example - One-Time Pad: Definition , usage and example	VK#2- Page no: 17-18, 28-32 DNS #2 Page no. 13 – 21 https://nptel.ac.in/courses/106/105/106105162/	Chalk & Talk , Audio Visual and Case Study
1.5		Steganography: - Definition and usage - Applications: • Confidential communication and secret data storing • Protection of data	VK#1- Page no: 34-35 NS#4- Page No: 155-156	Reading (Open book study) & Discussion

		alteration		

Learner Activities:

Slow Learner Activity: After completion of unit students have to write the answers of two questions as a homework given by the course teacher. Students have to submit assignment to course teacher within 2 days of assign.

Average Learner Activity: After the completion of topic "1.4 Cryptography Techniques", students have to do case analysis on problem definition as a homework given by course teacher and submit the same to the course teacher within 3 days of assign.

Advanced Learner Activity: After completion of unit students have to study inbuilt "Hermetic Stego" tool. One week shall be given to student for study after that viva shall be conducted by course teacher during laboratory session for the same.

Assessment Parameters: Quiz, Unit Test-1&2 and Internal Examination

Unit-2: Cryptography

Course Outcome: CO1, CO2

Programme Outcome: PO1, PO2 ,PO3, PO5, PO6

Programme Educational Objectives: PEO1, PEO2, PEO3

Semester Objectives: SO2, SO3

Sub Unit	Lesson Duration (Hour)	Summary of Topic	Study Material	Teaching Approach
2.1	1	Cryptography Types: - Symmetric/Private key cryptography: Definition , usage and application - Asymmetric/Public key cryptography: Definition , usage and application - Hash Functions: Definition , usage and application	VK#2- Page no: 14-17, DNS #2 Page no. 28-29 https://www.coursera.org/lecture/basic-cryptography-and-crypto-api/basic-cryptography-n2A4v	Discussion and Audio Visual
2.2	2	Symmetric key cryptography algorithms: - DES: Introduction, usage and application - AES: Introduction, usage and application	DNS #3 Page no. 39 – 48, AK#3 Page no:92-104, 130-137	Chalk & Talk, Audio Visual & Case Study
2.3	2	Asymmetric key cryptography algorithms: - RSA: Introduction, usage and application - Elliptic Curve Cryptography: Introduction, usage and	VK#7&8 Page no: 162-164, 169-172, 182-186, 193-195, AK#4 Page no: 148-154, DNS #4 Page no. 66 -75,	

		application - Diffie-Hellman Key Exchange: Introduction, usage and application	https://nptel.ac.in/courses/106/105/106105162/ https://pdfs.semanticscholar.org/d592/d1cea5d1e125996903090d8d18773ede235f.pdf	
2.4	2	Hash Functions: - Definition and usage - USHA-1: Introduction, usage and application - HMAC: Introduction, usage and application	VK#9 Page no: 218-224, AK#4 Page no: 185-189, DNS #5 Page no. 85 – 86, 95-96, WS#11 Page no. 328	Presentation

Learner Activities:

Average Learner Activity: After the completion of topics "2.1 Cryptography Types & 2.2 Symmetric key cryptography algorithms", students have to do case analysis on problem definition as homework given by course teacher and submit the same to the course teacher within 3 days of assign.

All Learner Activity: After the completion of unit, each student shall write solution of given 2 exercises based on topic 2.3 and 2.4 as homework and submit to the course teacher within 3 days of assign.

Assessment Parameters: Unit Test-1&2 and Internal Examination

Unit-3: Digital Signature

Course Outcome: CO2

Programme Outcome: PO1, PO2 ,PO3, PO5, PO6

Programme Educational Objectives: PEO1, PEO2, PEO3

Semester Objectives: SO1, SO2, SO3, SO4

Sub Unit	Lesson Duration (Hour)	Summary of Topic	Study Material	Teaching Approach
3.1	1	Digital Signature: - Needs - Applications: • Email System • E-commerce System • Online Auction	VK#10 - Page No: 241-245, 250-251	Reading (Open book study) & Discussion
3.2		Digital Signature Certificate: Needs and usage	NS#6 - Page No: 273	
3.3	1	Signing and Verification Process	VK#10 - Page No: 243-245, 250-251, http://searchsecurity.techtarget.com/definition/digital-signature	Presentation, Chalk & Talk & Case study

3.4	3	Digital Signature Schemes: - RSA: Introduction, usage and application - ElGamal Digital Signature: Introduction, usage and application - Elliptic Curve DSA: Introduction, usage and application	VK#10 - Page No: 245-249 https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf	
3.5	1	Digital Signature for Mobile Devices	http://www.wirelessdevnet.com/articles/cysive/digitalsig.html	Presentation
Learner Activities: **Slow Learner Activity:** After the completion of reading (Open book study) for the topic 3.1 & 3.2 course teacher shall select slow learner student(s) to discuss that topic in classroom. **All Learner Activity**: After the completion of unit, each student shall write solution of given 2 exercises based on topic 3.4 as homework and submit to the course teacher within 3 days of assign.				
Assessment Parameters: Unit Test-1&2 and Internal Examination				

Unit-4: Authentication and Authorization				
Course Outcome: CO3				
Programme Outcome: PO1, PO2 ,PO3, PO5, PO6, PO7				
Programme Educational Objectives: PEO1, PEO2, PEO3, PEO4				
Semester Objectives: SO2, SO3, SO4				
Sub Unit	**Lesson Duration (Hour)**	**Summary of Topic**	**Study Material**	**Teaching Approach**
4.1	1	Authentication Methods: - Password-based - Two-factor - Multifactor - Biometrics	VK#9 - Page No: 204 - 208, DNS #7 - Page no. 153-172	Presentation
4.2	1	Access Control Metrics: Needs and usage	DNS #8 Page no. 178 - 181	Presentation
4.3	1	Multilevel Security: Needs and usage	DNS #8 Page no. 181 – 184	
4.4		Firewall: - Needs - Types: • Packet filtering firewall • Application level gateway • Circuit level gateway	DNS #8 Page no. 191 – 195, VK#16 - Page No: 362 – 366	Reading (Open book study) & Discussion
4.5	2	Intrusion Detection: - Needs - Types:	DNS #8 Page no. 196 – 202, VK#14 - Page No: 324 – 327	

		• Network intrusion detection system • Host instruction detection system - Techniques: • Anomaly-based detection • Misuse-based detection		
4.6	1	Distributed Intrusion Detection	NS#7 - Page No: 329	

Learner Activities:

Slow Learner Activity: After completion of unit students have to write the answers of two questions as a homework given by the course teacher. Students have to submit assignment to course teacher within 2 days of assign.

Advanced Learner Activity: After the completion of topic "4.1 Authentication Methods", students have to prepare one small demo of Authentication using any of the learned method (in topic 4.1) in any technology and present to course teacher. Five days shall be given to students to prepare demo.

Assessment Parameters: Unit Test-2 and Internal Examination

Unit-5: Cyber Crimes and Cyber Security

Course Outcome: CO4, CO5

Programme Outcome: PO1, PO2 ,PO3, PO5, PO6, PO7

Programme Educational Objectives: PEO1, PEO2, PEO3

Semester Objectives: SO2, SO3, SO4

Sub Unit	Lesson Duration (Hour)	Summary of Topic	Study Material	Teaching Approach
5.1	1	Cybercrimes Classifications: - Cybercrime against individuals - Cybercrime against property - Cybercrime against organization - Cybercrime against society - Crimes emanating from UseNet Newsgroup	NS#1 - Page No: 17 – 31	Presentation
5.2	1	Cybercrime Methods: - Virus - Worms - Trojan Horses - Backdoors - Keyloggers - Spywares - Password Cracking - Botnet	NS#2 - Page No: 71-72 NS#4 - Page No: 132 - 153 VK#15 - Page No: 340 – 349	
5.3	2	An overview of Social Engineering, Cyber Stalking, Cyber Defamation, Phishing, Identity Theft, Hacking, DoS, DDoS	NS#2 - Page No: 61 - 67 NS#4 - Page	Presentation, case study based

		attacks and SQL Injection	No: 158 -167	discussion and demonstration of SQL Injection attack and its prevention
5.4	1	Mobile attacks and Wireless Devices attacks	NS#3 - Page No: 99-104	
5.5	1	Cyber Laws: Need and Indian ITA	NS#6 - Page No: 254-259 https://www.coursera.org/lecture/cyber-security-domain/legal-regulations-investigations-and-compliance-GfKZj	Group Discussion
Learner Activities: **All Learner Activity:** For the topic “5.5 Cyber Laws: Need and Indian ITA”, group of four students will be assigned the cyber crime and the group need to determine and discuss the cyber law applicable to that cyber crime in classroom.				
Assessment Parameters: Unit Test-2 and Internal Examination				

Unit-6: Fundamentals of Digital Forensics

Course Outcome: CO4, CO5

Programme Outcome: PO1, PO2 ,PO3, PO5, PO6, PO7

Programme Educational Objectives: PEO1, PEO2, PEO3

Semester Objectives: SO3, SO4

Sub Unit	Lesson Duration (Hour)	Summary of Topic	Study Material	Teaching Approach
6.1	1	Computer Forensics and Network Forensics: Definition and needs	NS#7 - Page No: 320-321,327-329	Presentation
6.2		Rules of Evidence and Evidence Collection	NS#7 - Page No: 329-331	
6.3	1	Digital Forensics Phases	NS#7 - Page No: 341-355	Group Discussion
6.4	1	Digital Forensics Data Mining Techniques: - Entity Extraction - Clustering - Association Rule Mining	NS#7 - Page No: 402-403	Discussion and Chalk & Talk
6.5	1	Hand Held Devices and Digital Forensics : - Mobile Phone	NS#8 - Page No: 431-444	Presentation

		- PDA - Printers - Scanners - Smartphones		and Discussion
6.6	1	Forensics Auditing: Definition and usage	NS#7 - Page No: 403-404	

Learner Activities:
All Learner Activity: For the topic "6.3 Digital Forensics Phases", group of four students will be assigned the case study and the group need to determine and discuses the cyber crime(s) and forensics phases applicable to that crime(s) in classroom.

Assessment Parameters: Internal Examination

Study Material

- **Text Books:**

  1. V. K. Pachghare, Cryptography and Information Security, Second Edition, PHI Learning. [VK]
  2. Nina Godbole, Sunit Belapure, Cyber Security – Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wile.[NS]

- **Other References:**

  1. Deven Shah, Mark Stamp's Information Security Principles and Practice, Wiley-India.[DNS]
  2. Atul Kahate, Cryptography and Network Security, McGraw Hill.[AK]
  3. William Stallings, Cryptography and Network Security Principles and Practices, Pearson[WS]
  4. https://swayamprabha.gov.in/index.php/program/archive/10
  5. https://nptel.ac.in/courses/106/105/106105162/
  6. https://pdfs.semanticscholar.org/d592/d1cea5d1e125996903090d8d18773ede235f.pdf
  7. https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf

Note: # denotes chapter number.

Concept Linkage

Concept Linkage: Unit/Sub-Unit	Prior concept linkage	Contemporary Linkage	Post concept linkage
Unit-4 (4.1)	040010318: Web Programming Paradigm: Unit-5(5.1 & 5.2)		
Unit- 6 (6.4)	-	040010426: Fundamental of Data Science: Unit - 1(1.3), 3(3.2)	040010527: Basics of Web Analytics Unit-5(5.6)