

Branch Name:	Artificial Intelligence & Data Science
Program Code:	108
Course Name:	Data and Internet Security
Course Code:	1ET1080505
Pre-requisite Course:	Computer Networks

Course Objectives:

1. To understand the basics of Cryptography and Network Security.
2. To be able to secure a message over an insecure channel by various means.
3. To learn about how to maintain the Confidentiality, Integrity and Availability of data.
4. To understand various protocols for network security to protect against the threats in the networks.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
03	-	02	04	70	30	30	20	150

Subject Contents:

Sr. No	Topic	Total Hours	Weightage (%)
1	Introduction and Security Threats: Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare, Avenues of Attack, steps in attack, Security Basics – Confidentiality, Integrity, Availability Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware : Viruses, Logic bombs	03	04
2	Introduction to Cryptography: Introduction to security attacks, services and mechanism, introduction to cryptography, CIA Model Conventional Encryption: Conventional encryption model, classical encryption techniques, substitution ciphers and transposition ciphers, cryptanalysis, steganography	04	10
3	Block Ciphers	05	12

	Stream and blockciphers, Modern Block Ciphers: Block ciphers principals, Shannon's theory of confusion and diffusion, fiestal structure, data encryption standard(DES), strength of DES, differential and linearcrypt analysis of DES, block cipher modes of operations, triple DES, AES.		
4	Confidentiality and Modular Arithmetic Confidentiality using conventional encryption - traffic confidentiality - key distribution - random number generation - Introduction to graph - ring and field - prime and relative prime numbers - modular arithmetic - Fermat's and Euler's theorem - primality testing - Euclid's Algorithm - Chinese Remainder theorem - discrete algorithms.	05	17
5	Modes of Operations: Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	03	04
6	Public key cryptography and Authentication requirements Principles of public key crypto systems - RSA algorithm - security of RSA - key management – Diffie-Hellman key exchange algorithm - introductory idea of Elliptic curve cryptography – Elgamel encryption - Message Authentication and Hash Function: Authentication requirements - authentication functions - message authentication code - hash functions - birthday attacks – security of hash functions and MACS.	08	20
7	Integrity checks and Authentication algorithms MD5 message digest algorithm - Secure hash algorithm (SHA) Digital Signatures: Digital Signatures - authentication protocols - digital signature standards (DSS) - proof of digital signature algorithm - Authentication Applications: Kerberos and X.509 - directory authentication service - electronic mail security-pretty good privacy (PGP) - S/MIME.	08	12
8	IP Security and Key Management IP Security: Architecture - Authentication header - Encapsulating security payloads - combining security associations - key management.	04	09
9	Web and System Security Web Security: Secure socket layer and transport layer security - secure electronic transaction (SET) - System Security: Intruders - Viruses and related threads - firewall design principles – trusted systems.	05	12

Text Books:

1. William Stallings, "Cryptography and Network security Principles and Practices", Pearson/PHI.
2. Wade Trappe, Lawrence C Washington, " Introduction to Cryptography with coding theory", Pearson.

Reference Books:

1. W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing – Prentice Hall of India.

Video Lecture

1. <http://nptel.ac.in/courses/106105031/lecture> by Dr. DebdeepMukhopadhyayIIT Kharagpur
2. <https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-033-computer-system-engineering-spring-2009/video-lectures/> lecture by Prof. Robert Morris and Prof. Samuel Madden MIT.

LAB/Practical

1. Draw Diagram of DoS, backdoors, trapdoors.
2. Draw diagrams of sniffing, spoofing, man in the middle & replay attacks.
3. Draw diagram for Confidentiality, Integrity & Availability.
4. Implement Caesar cipher encryption-decryption.
5. Implement Monoalphabetic cipher encryption-decryption.
6. Implement Playfair cipher encryption-decryption.
7. Implement Polyalphabetic cipher encryption-decryption.
8. Implement Hill cipher encryption-decryption.
9. To implement Simple DES or AES.
10. Implement Diffi-Hellmen Key exchange Method.
11. Implement RSA encryption-decryption algorithm.
12. Write a program to generate SHA-1 hash.
13. Implement a digital signature algorithm.
14. Perform various encryption-decryption techniques with cryptool.

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Acquire fundamental knowledge on the concepts of finite field and number theory.	1 Remembering 2 Understanding
CLO2	Acquire the ability to apply number theory concepts in Cryptography	2 Understanding
CLO3	Utilize the principles of public key cryptosystems, hash function and digital signature	3 Applying
CLO4	Acquire the ability to apply the concept of IP security and architecture	3 Applying
CLO5	Apply the knowledge gained other various methods of password management and protocols to maintain system security	3 Applying

Mapping of CLOs with POs & PSOs

Course	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	L	L					L		L		M	M		
CLO2	M	L	M		L								M	M		

CLO3	M	L	L						L				M	M		
CLO4	M	L	L	L	L						L		M	M		
CLO5	H	M	M			L			L				M	M		

H:High, M:Medium, L:Low