

Subject Code: 1ET2030102	Subject Title: INFORMATION SECURITY
Pre-requisite	Computer Networks

Course Objective: The core objective of this course is to make the students aware and have some expertise with various facets of digital security mechanism such as confidentiality, integrity, authentication, access control, non-repudiation and availability. This course aims to present various cryptographic mechanisms, security protocols, message digest, digital signatures, and key distributions techniques used for security. This course shall act as platforms for the students wishing to carry out further research in cybercrime/security or forensic investigation.

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture	Tutorial	Practical	Credit	Theory		Practical		Total
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
2	-	2	4	60	40	30	20	150

Subject Contents			
Sr. No	Topic	Total Hours	Weight (%)
1	Introduction and Classical Encryption: Conventional Encryption Model, Cryptography, Cryptanalysis and Attacks, Steganography, Classical Encryption Techniques: Substitution and Transposition techniques	02	05
2	Block Ciphers: Principles, Fiestal Structures, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES) - Structure, Transformation functions, key expansion, example and implementation, Other Modern Block ciphers	04	15
3	Modes of Operations: Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	01	05
4	Public Key Cryptography: Principles of Public-Key Cryptography, RSA algorithm, Key Management, Elliptic Curve Cryptography, Diffie-Hellman Key Exchange, Man-in-Middle attack	03	12
5	Cryptographic Hash Functions and Message Authentication Codes: Applications, its requirements and security, Simple hash functions, Secure Hash Algorithm (SHA), Hash functions based on Cipher Block Chaining, MAC based on Hash Function, Macs based on Block Ciphers	05	15
7	Digital Signature: Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr)	02	08
8	Key management and distribution: symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Remote user authentication with symmetric and asymmetric encryption	03	10
9	Network Security Protocols: IPSec: Authentication Header and Encapsulation Security Payload, Secure Socket Layer/Transport Layer Security, SecureElectronic Transactions, Pretty Good Privacy	04	15
10	Number Theory: Prime and Relative Prime Numbers, Modular Arithmetic, Euler's Theorem, Euclid's Algorithm, Discrete Logarithm Tics	04	15

Review Presentation: The student is expected to spend minimum 2 hours per week (as mentioned in the teaching and evaluation scheme) to refer at least two peer reviewed journal papers related to this domain/subject. The student is expected to identify issues/challenges and emerging trends in the domain/subject. Student is supposed to explore various video lectures (E.g. NPTEL) available in the domain/subject. Student is required to make a review-presentation on the work carried out for the same.

Recommended sites for journal papers are (1) dl.acm.org (2) springer.com (3) sciencedirect.com (4) elsevier.com (5) ieeexplore.ieee.org (6) scholar.google.co.in (7) scopus.com or similar of similar repute.

Course Outcome:

After learning the course, the students would be able to:

Define the concepts of Information security and their usage. Describe the principles of public and private cryptography. Understand the concepts of hashing/MAC with algorithms and apply them. Understand the concepts of digital signature and digital certificates. Understand the key management and remote authentication mechanisms

List of References:

1. Cryptography and Network Security Principles and Practices by William Stallings, Prentice Hall
2. Cryptography and Network Security Atul Kahate, TMH
3. Information Security Principles and Practice, Deven Shah, Wiley-India
4. Cryptography & Network Security, Forouzan
5. Security in Computing by Pfleeger, PHI hopadhyay, McGrawHill

E-Resources / Web Links

1. <http://williamstallings.com/ComputerSecurity/>
2. <http://williamstallings.com/Cryptography/>
3. <http://williamstallings.com/NetworkSecurity/>
4. <https://www.schneier.com/academic/>

List of Experiments:

Note: The experiment list provided beneath is for reference only. The course teacher may change/formulate it as per his/her methodology and requirement.

1. Implement Brute-Force Attack (Exhaustive Key Analysis on Caesar Cipher)
1. Write a program to implement the Substitution ciphers.
2. Write a program to implement the Transposition ciphers.
3. Perform various encryption-decryption methods using freeware encryption tool (cryptool).
4. Perform the encryption operation for given information using S-DES.
5. Implementation of simple stenographic technique.
6. Implementation of block ciphers (Blowfish) using library (API)
7. To generate a digital certificate.
8. Capture and analyse the network traffic using wireshark tool.
9. To generate SHA-1 Hash code for given message/file.
10. To implement SSL/TLS.
11. To demonstrate any advance cryptography.
12. Open Experiment (Student have to identify the problem from Research papers from reputed Journals & Conferences and try to implement it-if possible)