Faculty of Engineering and Technology

Bachelor of Technology
Effective from Academic Year: 2018-19

Branch Name:	Computer Engineering / Information Technology
Semester/Year:	Semester VI / Third Year
Subject Title:	Cryptography and Network Security
Subject Code:	1ET1030602
Pre-requisite:	Computer Networks

Course Objective:

The core objective of this course is to make the students aware and have knowledge with various facets of security mechanism such as confidentiality, integrity, authentication, access control, non-repudiation and availability. This course aims to present various cryptographic mechanisms, services, security protocols, message digest, digital signatures, and key distributions techniques used for security.

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:** Security services, mechanisms and attacks	2	5%
2	**Classical Encryption:** Conventional Encryption Model, Cryptography, Cryptanalysis and Attacks, Classical Block Ciphers (Substitution and Transposition techniques)	5	10%
3	**Block Ciphers**: Principles, Fiestal Structures, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES) Structure, Transformation functions, key expansion	6	15%
4	**Modes of Operations:** Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	2	5%
5	**Number Theory:** Prime and Relative Prime Numbers, Modular Arithmetic, Euler's Theorem, Euclid's Algorithm, Extended Euclidean Algorithm, Discrete Logarithm	3	5%
6	**Public Key Cryptography:** Public Key Cryptosystems with Applications, RSA algorithm, RSA Security, Diffie-Hellman Key Exchange**,** Man-in-Middle attack on Diffie-Hellman	5	10%
7	**Message Authentication Codes and Cryptographic Hash Functions:** Applications, its requirements and security, Macs based on Block Ciphers Simple hash functions, Secure Hash Algorithm (SHA), Hash functions based on Cipher Block Chaining, MAC based on Hash Function	6	15%
8	**Digital Signature:** Digital Signature, its properties, NIST digital Signature algorithm	2	5%

9	**Key management and distribution**: Symmetric key distribution using symmetric and asymmetric encryptions, Distribution of public keys, X.509 certificates, Remote user authentication: Kerberos	5	15%
10	**Network Layer Security Protocol:** IPSec: Authentication Header and Encapsulation Security Payload	2	5%
11	**Transport and application Layer Security Protocol:** SSL architecture and protocol, Transport layer security, HTTPS and SSH	4	10%

Course Outcome:

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

- Define the concepts of Information security and their use.
- Describe the principles of symmetric and asymmetric cryptography.
- Understand and apply the various symmetric key algorithms.
- Understand and apply the various asymmetric key algorithms.
- Understand the concepts of hashing with algorithms and apply them.
- Understand and use the message authentication and its requirement.
- Understand the concepts of digital signature and digital certificates.
- List and explain various digital signature algorithms.
- Understand and use the various key management and remote authentication mechanisms.
- Understand the concept transport layer security.

List of Text Books:

1. Cryptography and Network Security Principles and Practicesby William Stallings, Prentice Hall
2. Cryptography & Network Security, Forouzan

List of Reference Books:

1. Security in Computing by Pfleeger, PHI hopadhyay, McGrawHill
2. Cryptography and Network Security Atul Kahate, TMH
3. Information Security Principles and Practice, Deven Shah, Wiley-India

List of Suggested titles of Experiments (If Any):

1. Implement the Ceaser Cipher.
2. Implement Brute-Force Attack.
3. Implement the Hill Cipher.
4. Implement the Vernam Cipher.
5. Implement the Rail-Fence Cipher.
6. Implement the Columnar Cipher.
7. Implement the RSA algorithm.
8. Implement the Diffil-Hellman key exchange algorithm.
9. To study the structure of Digital Signature.
10. To calculate the hash code using any crypt tool.
11. To Capture the network traffic and understand the network protocol using Wireshark/packet capturing tool.
12. To study and use the crypto library for cryptography.

e-Resources (If any):

1. http://nptel.ac.in/
2. http://williamstallings.com/Cryptography/