

Branch Name:	Computer Engineering / Information Technology
Program Code:	ET103/ ET105
Course Title:	Cryptography and Computer Security [Specialization in Cyber Security]
Course Code:	2ET1030506T
Pre-requisite Course:	Computer Networks

Course Objectives:

- To introduce fundamental concepts of symmetric and asymmetric cipher models
- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity
- To introduce network security and web security protocols.

Teaching and Examination Scheme:

Teaching and Examination Scheme.														
Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)									
					Theory (Marks)				Practical (Marks)				Total (Marks)	
	L	T	P	Total	SEE		CCA		SEE		CCA			
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.		
3	3	-	-	3	24	60	16	40	-	-	-	-	100	

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Introduction: Security services, mechanisms and attacks	3	10%
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 Modes of Operations: Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	8	25%
4	Number Theory: Prime and Relative Prime Numbers, Modular Arithmetic, Euler's Theorem, Euclid's Algorithm, Extended Euclidean Algorithm, Discrete Logarithm	5	10%
5	Public Key Cryptography: Public Key Cryptosystems with Applications, RSA algorithm, RSA Security, Diffie-Hellman Key Exchange, Man-in-Middle attack on Diffie-Hellman	4	10%
6	Message Authentication Codes and Hash Functions: Digital Envelope, Digital Signature, Digital Signature Schemes, Message Digest (MD), SHA, Message Authentication.	4	15%
7	Network Security: Kerberos, Key Management, PKI, Security at the Network Layer – IPSec, Security at the Transport Layer – SSL, Security at the Application Layer- PGP and S/MIME, Firewall, Network Vulnerabilities	5	20%

Reference Books:

- Cryptography and Network Security Principles and Practices by William Stallings, Prentice Hall.
- Cryptography and Network Security, Forouzan.
- Cryptography and Network Security, Forouzan, Mukhopadhyay, McGrawHill.
- Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India.

List of Open-Source Software/learning website:

- <http://nptel.ac.in/>
- <http://williamstallings.com/Cryptography/>

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Define the concepts of Information security and their use. Describe the principles of symmetric and asymmetric cryptography.	1.Remembering 2.Understanding
COL2	Importance of Network Security and Challenges in Network Security, Understand and apply the various symmetric key and asymmetric key algorithms.	1.Remembering 2.Understanding 3. Applying
COL3	Understand the concepts of hashing with algorithms and apply them. Understand and use the message authentication and its requirement.	1.Remembering 2. Understanding
COL4	Understand the concepts of digital signature and digital certificates. List and explain various digital signature algorithms	1.Remembering 2.Understanding
COL5	Understand and use the various key management and remote authentication mechanisms. Implementing Security services in an organization	1. Remembering 3. Applying

Mapping of CLO with PO and PSO :

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)	
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO1	PSO2
CLO1	L	L		L									M	
CLO2		L				L								L
CLO3	L	H	M	H	L				L		M		M	
CLO4		M	H		L				L		H		H	H
CLO5	L		L			M								H

H: High, M: Medium, L: Low