

Branch Name:	Information and Communication Technology
Program Code:	ET208
Course Name:	Information Security (Elective-III)
Course Code:	2ET2080302T
Pre-requisite Course:	Computer Networks

Course Objective:

1. Students will be able to understand basic cryptographic algorithms, message and web authentication and security issues.
2. Ability to identify information system requirements for both of them such as client and server.
3. Ability to understand the current legal issues towards information security.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme(Marks)								Total(Marks)
					Theory(Marks)				Practical(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

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	04	12
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	12
3	Modes of Operations: Electronic Code Book, Cipher Block Chaining Mode, CipherFeedback mode, Output Feedback mode, Counter mode	03	07
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	07
5	Cryptographic Hash Functions and Message Authentication Codes: Applications, its requirements and security, Simple hash functions, SecureHash Algorithm (SHA), Hash functions based on Cipher Block Chaining, MAC based on Hash Function, Macs based on Block Ciphers	05	15

6	Digital Signature: Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	02	05
7	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	05	15
8	Network Security Protocols: IPSec: Authentication Header and Encapsulation Security Payload, Secure Socket Layer/Transport Layer Security, Secure Electronic Transactions, Pretty Good Privacy, Wireless Security, Threats in networks	05	15
9	Number Theory: Prime and Relative Prime Numbers, Modular Arithmetic, Euler's Theorem, Euclid's Algorithm, Discrete Logarithm	04	12

Text Books:

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

Reference Books:

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

List of Open Source Software/learning website:

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

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

CLO	Description	Bloom's Taxonomy Level
CLO1	Define the concepts of Information security and their use.	2 Understanding
CLO2	Describe the principles of symmetric and asymmetric cryptography.	6 Creating
CLO3	Understand and apply the various symmetric and asymmetric key algorithms.	2 Understanding, 3 Applying
CLO4	Understand the concepts of hashing with algorithms and apply them.	3 Applying, 2 Understanding
CLO5	Use message authentication and its requirement. Learn the concepts of digital signatures and digital certificates.	5 Evaluate, 4 Analyze
CLO6	List and explain various digital signature algorithms	1 Remembering, 2 Understanding
CLO7	Understand and use the various key management and remote authentication mechanisms. Understand the concept of transport layer security.	2 Understanding

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	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	M	L							L		H	M		M
CLO2	H	M	M	L	M					L			H	M		
CLO3	H	M	M	L							L		H	M	M	M
CLO4	M	L	L		H					L			M	M	M	
CLO5	H	M	M										M			M
CLO6		M	M		H					L	M	M		M	M	M
CLO7	M				H					L				M		M

H: High, M: Medium, L: Low