

Branch Name:	Computer Engineering (Software Engineering)
Program Code:	ET203
Course Title:	Information Security
Course Code:	2ET2030107T
Pre-requisite Course:	Mathematics, Programming, Database Management, Computer Science, Networking, Operating Systems

Course Objectives: After successful completion of the course, student will be able to

1. Introduce fundamental information security concepts and terminology.
2. Assess and prioritize security threats and risks.
3. Develop and implement security policies and procedures.
4. Manage access control, authentication, and authorization.
5. Understand and apply cryptographic techniques for data security.
6. Implement network security measures, including firewalls and intrusion detection.

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

Course Contents:

Unit No	Topics	Total Hours	Weightage (%)
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
6	Digital Signature: Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr)	02	08
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	03	10
8	Network Security Protocols: IPsec: Authentication Header and Encapsulation Security Payload, Secure Socket Layer/Transport Layer Security, Secure Electronic Transactions, Pretty Good Privacy	04	15
9	Number Theory: Prime and Relative Prime Numbers, Modular Arithmetic, Euler's Theorem, Euclid's Algorithm, Discrete Logarithm	04	15

Text Books / 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:

- ☐ <http://williamstallings.com/ComputerSecurity/>
- ☐ <http://williamstallings.com/Cryptography/>
- ☐ <http://williamstallings.com/NetworkSecurity/>
- ☐ <https://www.schneier.com/academic/>

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Demonstrate a deep understanding of information security principles and concepts.	Understanding (2) Applying (3)
COL2	Identify and assess security threats, both internal and external, and prioritize them	Applying (3)
COL3	Develop and implement effective security policies and procedures for organizations.	Applying (3)
COL4	Comply with relevant laws, regulations, and industry standards in information security.	Applying (3)
COL5	Configure and manage network security measures, such as firewalls and intrusion detection systems.	Applying (3)

Mapping of CLO with PO and PSO

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		M											
CLO2	H	M			M							L				
CLO3	H	M	M		M											
CLO4	M	M	M		M							L				
CLO5	M	M										L				

H: High, M: Medium, L: Low