CRYPTOGRAPHY AND NETWORK SECURITY

Course code:	**17TE7DECNS**	**Credits:**	**03**
L: P: T: S:	**3:0:0:0**	**CIE Marks:**	**50**
Exam Hours:	**03**	**SEE Marks:**	**50**

Course Objectives

1. To provide impeccable knowledge on various technical aspects of Network Security & Computer Security principles.
2. To understand the principles of cryptographic algorithms.
3. To understand modular arithmetic in public key cryptosystem.
4. To determine the level of protection and response to security incidents.

Course Outcomes : After completion of the course, the graduates will be able to

CO1 To apply the fundamental concepts of network services, attacks and mechanism to model conventional network security systems.

CO2 To develop solutions for various symmetric cipher techniques to address the different security issues using modular arithmetic.

CO3 To compose different key management techniques for public key cryptosystems.

CO4 Analyze the digital signatures and authentication protocols and Hash functions.

CO5 To assess the various security threats for a computer based network and provide secured solutions for trusted systems.

CO6 Able to design and evaluate cryptographic algorithms and analyze the strength.

Mapping of Course outcomes to Program outcomes

	PO	PO	PO	PO	PO	PO	PO	PO	PO	PO	PO	PO	PS0	PSO	PSO
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3														
CO2	3	2	3		3									2	
CO3	3	2	3											2	
CO4	3	3		3											
CO5	3	3	3			2		2						2	
CO6	3	3	3	3	3				3	3	3			2	

Course Content

Module	**Contents**	**Hours**	**CO's**
1	Services, Mechanisms, Mechanism Attacks, The OSI security architecture, a model for network Security. Symmetric Ciphers model, Substitution Techniques, Transposition Techniques.	8	CO1 CO2

2	Simplified DES, Data encryption Standard (DES),The strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and modes of operation, Evaluation Criteria for Advanced Encryption Standard, The AES Cipher.	8	CO2 CO6
3	Modular arithmetic, Euclid's algorithm, Fermat's and Euler's Theorem. Principles of public key Cryptosystem, The RSA algorithms, Key management, Diffie-Hellman Key exchange, Elliptic Curve Arithmetic.	8	CO3
4	Authentication functions and Hash functions. Digital Signatures, Authentication protocols, Digital signature standard. Web security consideration, Secure Socket layer, Transport layer security, secure electronic transaction.	8	C04
5	Intruders, Intrusion Detection, Password Management. Malicious software programs: Viruses and related Threats, Virus Countermeasures. Firewall Design Principles, Trusted Systems.	8	CO5

Self-Study Component

Module-1	Steganography
Module-2	Double DES
Module-3	Finite Fields
Module-4	Email security
Module-5	Ethics in Information Security

Note : No questions from illustrative examples and from Self-study component

Text Books

1. Cryptography and network Security. William Stalling, Pearson Education,2003.
2. Perlman - Kaufman Spenciner, "Network Security", Pearson Education/PHI, 2002,ISBN: 9971–51–345–5

References

1. Cryptography and network security, Behrouz A Forouzan,TMH ,2007.
2. Cryptography and network security,Atul kahate, TMH ,2003.

Assessment Pattern :

CIE : Continious Internal Evaluation Theory (50 Marks)

Bloom's Category	**Tests**	**Assignments**	**AAT1**	**AAT2**
Marks (Out of 50)	**30**	**10**	**05**	**05**
Remember				
Understand	5	2	1	1
Apply	10	2	1	1
Analyze	5	2	1	1
Evaluate	10	2	1	1
Create		2	1	1
				***AAT: Alternate Assessment Tool**

SEE –Semester End Examination Theory (50 Marks)

Bloom’s Category	**Marks Theory (50)**
Remember	5
Understand	5
Apply	10
Analyze	10
Evaluate	10
Create	10