CRYPTOGRAPHY AND NETWORK SECURITY

Course code: 19IS7DECNS **Credits: 03**
L: P: T: S: 3: 0: 0: 0 **CIE Marks: 50**
Exam Hours: 03 **SEE Marks: 50**
Total Hours: 40

Course Objectives:

1. To understand OSI security architecture and classical encryption techniques.
2. To acquire fundamental knowledge on the concepts IP and Email security.
3. To understand various block cipher and stream cipher models.
4. To describe the principles of public key cryptosystems, hash functions and digital signature.

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

CO1	Identify different types of attacks and encryption techniques
CO2	Design secure applications
CO3	Implement secure coding in the developed applications
CO4	Design various IP security technology.
CO5	Evaluate and apply various security services such as PGP, S/MIME, authentication, confidentiality and key management.
CO6	Design and distinguish between various symmetric and asymmetric encryption techniques.

Mapping of Course outcomes to Program outcomes:

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**	**PSO3**
CO1	2	2	2	-	-	-	-	-	-	-	-	2	-	-	2
CO2	2	3	-	-	-	-	-	-	-	-	-	1	-	2	2
CO3	3	3	2	2	-	-	-	-	-	-	-	2	-	2	2
CO4	3	3	2	2	-	-	-	-	-	-	-	2	-	2	2
CO5	3	3	-	-	-	-	-	-	-	-	-	2	-	2	1
CO6	**3**	**3**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2**	**-**	**-**	**1**

Unit	**Course Content**	**Hours**	**COs**
1	**INTRODUCTION & NUMBER THEORY** Security Attacks, Services, Mechanisms Network security model. Symmetric Cipher Model ,Substitution Techniques- Ceaser cipher, Monoalphebetic cipher, Playfair cipher , Transposition Techniques, Groups, Rings, Fields-Modular arithmetic-Euclid's algorithm-Finite fields- Polynomial Arithmetic	**8**	**CO1,CO6**
2	**Block Ciphers and the Data Encryption Standard:** Block cipher Principles, The Data Encryption Standard(DES) **Public-Key Cryptography and RSA:** Principles of Public-Key Cryptosystems, The RSA Algorithm- description of the algorithm **Other Public-Key Cryptosystems:** Diffie-hellman key exchange	**8**	**CO1,CO2,CO3**
3	**HASH FUNCTIONS AND DIGITAL SIGNATURES** Applications of Cryptographic Hash Functions . Two Simple Hash	**8**	**CO5,CO6**

	Functions, Hash Functions Based on Cipher Block Chaining,Secure Hash Algorithm (SHA), Digital Signatures , ElGamal Digital Signature Scheme, Digital Signature Standard (DSS)		
4	**Key Management and Distribution:** Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, Controlling key usage, Symmetric key distribution using Asymmetric encryption	**8**	**CO5,CO6**
5	**IP Security:** IP Security Overview; IP Security Policy; Encapsulating Security Payload; Combining Security Associations; **Firewalls:** Firewall Characteristics, Types of Firewalls, Firewall basing, Firewall Location and Configurations	**8**	**CO4**

Self study component:

Note: 1.Questions for CIE and SEE not to be set from self-study component.

2. Assignment Questions should be from self-study component only.

UNIT 1: A DES example, results, the avalanche effect, the strength of DES

UNIT 2: Elliptic curve cryptography, The algorithm, key exchange protocols, man in the middle attack

UNIT 3: Simple secret key distribution, secret key distribution with confidentiality and authentication

UNIT 4: Key Management and Distribution - User Authentication

UNIT 5: Electronic mailing service

TEXT BOOKS

1. William Stallings: Network Security Essentials: Applications and Standards, 6th Edition, Pearson Education, 2013.
2. Michael E. Whitman and Herbert J. Mattord: Principles of Information Security, 2nd Edition, Cengage Learning, 2005.

REFERENCE BOOKS

1. Behrouz A. Forouzan: Cryptography and Network Security, Special Indian Edition, Tata McGraw-Hill, 2007.
2. V k Pachghare: Cryptography and Information Security, 2013

Assessment Pattern:

CIE –Continuous Internal Evaluation Theory (50 Marks)

Bloom's Category	**Tests**	**Assignments**	**AAT1**	**AAT2**
Marks (Out of 50)	**30**	**10**	**05**	**05**
Remember	10			01
Understand	10	05	01	01
Apply	10	05	02	01
Analyze			02	
Evaluate				
Create				02

***AAT 1– Alternate Assessment Tool 1: Quiz**

AAT 2 - Alternate Assessment Tool 2: Surprise Test

SEE –Semester End Examination Theory (50 Marks)

Bloom’s Category	**Marks Theory(50)**
Remember	10
Understand	20
Apply	10
Analyze	10
Evaluate	
Create	