Course Type	Course Code	Name of Course	L	T	P	Credit
OE	CSO404	**Cryptography**	3	0	0	9

Course Objective
Understanding about topics Cryptography for information and cyber security
Learning Outcomes
Ability for the following. ● The basics of cryptographic fundamentals namely, confidentiality, integrity, and availability ● Classical and modern methods for encryption/decryption ● Public key cryptosystems ● Cryptographic hash functions ● Digital Signatures

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1.	Introduction: Security goals, Attacks, Security services and mechanisms, Security techniques	3	The basics about Security goals, Attacks, Security services and mechanisms, Security techniques
2.	Classical encryption techniques: Additive ciphers, Monoalphabetic, Playfair cipher, Polyalphabetic, Block ciphers	5	Understanding classical / traditional symmetric encryption / decryption with cryptanalysis
3.	Modern symmetric cryptosystems-DES, AES	6	Learning of DES and AES
4.	Public-key ciphers: RSA, Rabin, ElGamal, Elliptic curve cryptography	6	Understanding of public-key cryptosystems and their cryptanalysis, ECC
5.	Message authentication and cryptographic hash algorithms: MAC, MD5, SHA-1	6	Learning of MAC for message authentication and cryptographic hash functions
6.	Message integrity and authentication-Digital Signatures: RSA, ElGamal, DSS	6	Learning about different digital signature schemes
7.	Key management: Diffie-Hellman key exchange protocol, Public-Key Infrastructure(PKI)	6	Understanding of different key management techniques
8.	Zero knowledge protocols: Fiat-Shamir, Feige-Fiat Shamir	4	Learning of different entity authentication ZKP schemes

Text Books:

1. William Stallings, ‘Cryptography and Network Security- Principles and Practices’ Pearson Education.

Reference Books:

1. B.A. Forouzan, ‘Cryptography and Network Security’ Tata McGraw-Hill.