BEIT702T **COMPUTER SYSTEM SECURITY**

(Theory Credit: 05)

Teaching Scheme:	**Examination Scheme:**
Lecture: 4 Hours/week	**Theory: T (U): 80 Marks T (I): 20 Marks**
Tutorial: 1 Hour/week	**Duration of University Exam. : 03 Hours**

==========

UNIT I:

Introduction:

Need of information security, OSI security Architecture, Attacks, services, mechanism, Model of network security, Classical Encryption Techniques: Symmetric, Asymmetric, cipher model; substitution - Ceasor cipher, monoalphabetic, play fair; Transposition-Railfence, columnar; Steganography, S-DES, DES, TDES, AES; Block cipher principle, Mode, strength of DES.

UNIT II:

Differential and linear Cryptanalysis, Blowfish, RC2, RC5, IDEA, CAST-128, Characteristic of advance symmetric block cipher, Euler function, Chinese remainder theorem, Discrete logarithm, confidentiality using conventional encryption, placement of encryption function traffic, confidentiality, key distribution, random number generator.

UNIT III:

Public key cryptography- principles, RSA algorithm, key management, Diffie-Hellman key exchange, elliptic curve cryptography, Message Authentication, hash function Authentication requirements, functions, codes, hash functions, Security of hash function and MACs, Hash and MAC algorithm, MD5, Message Digest algorithm.

UNIT IV:

Secure hash algorithm (SHA-1), RIPEMD-160, HMAC, digital signatures and Authentication protocol-digital signature, authentication protocol, digital signature standard. Network Security practices, authentication applications-Kerberos, x.509 directory authentication service, Kerberos encryption technique

UNIT V:

E-mail security-Pretty Good Privacy, S/MIME, data compression using ZIP, radix-64 conversion, PGP random number generation, IP Security-Overview, Architecture, authentication header, Encapsulating security payload, combining security association, key management.

UNIT VI:

Web Security requirements, secure socket layer and transport layer security, secure electronic transaction, network management security-basic concepts of SNMP, SNMP V1, community facility, SNMP V3; System security-intruders, viruses and worms and related threads firewall-design principles, trusted system, DOS.

Text Books:

1. Forouzan, "Cryptography and Network Security", Tata-McGraw hill.
2. William Stallings, "Cryptography and Network Security: Principle and Practice", Fifth Edition, Pearson.
3. Atul Kahate, "Cryptography and Network Security", Tata-McGraw hill.

Reference Books:

1. Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry, "Fundamentals of computer Security", Springer.

******