7CS2 Information System Security Class: VII Sem.

B.Tech. Evaluation Branch: Computer Engg.

Schedule per Week Lectures: 3

Examination Time = Three (3) Hours Maximum Marks = 100 [Mid-term (20) & End-term (80)]

Units Contents of the subject

Unit I

Introduction to security attacks, services and mechanism, classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, stream and block ciphers. Modern Block Ciphers: Block ciphers principals, Shannon's theory of confusion and diffusion, fiestal structure, data encryption standard(DES), differential and linear cryptanalysis of DES, block cipher modes of operations, triple DES.

Unit II

AES, RC6, random number generation.S-box theory: Boolean Function, S-box design criteria, Bent functions, Propagation and nonlinearity, construction of balanced functions, S-box design.

Unit III

Public Key Cryptosystems: Principles of Public Key Cryptosystems,RSA Algorithm, security analysis of RSA, Exponentiation in Modular Arithmetic.Key Management in Public Key Cryptosystems: Distribution of Public Keys, Distribution of Secret keys using Public Key Cryptosystems. X.509 .Discrete Logarithms, Diffie-Hellman Key Exchange.

Unit IV

Message Authentication and Hash Function: Authentication requirements, authentication functions, message authentication code, hash functions, birthday attacks, security of hash functions and MAC, MD5 message digest algorithm, Secure hash algorithm(SHA).

Digital Signatures: Digital Signatures, authentication protocols,digital signature standards (DSS), proof of digital signature algorithm.Remote user Authentication using symmetric and Asymmetric Authentication

Unit V

Pretty Good Privacy.IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulation Security Payload in Transport and Tunnel mode with multiple security associations (Key Management not Included).Strong Password Protocols: Lamport's Hash, Encrypted Key Exchange.

Syllabus Covered (In Bold fonts)

Unit I

Introduction to security attacks, services and mechanism, classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, stream and block ciphers. Modern Block Ciphers: Block ciphers principals, Shannon's theory of confusion and diffusion, fiestal structure, data encryption standard(DES), differential and linear cryptanalysis of DES, block cipher modes of operations, triple DES.

Unit II

AES, RC6, random number generation.S-box theory: Boolean Function, S-box design criteria, Bent functions, Propagation and nonlinearity, construction of balanced functions, S-box design.

Unit III

Public Key Cryptosystems: Principles of Public Key Cryptosystems,RSA Algorithm, security analysis of RSA, Exponentiation in Modular Arithmetic.Key Management in Public Key Cryptosystems: Distribution of Public Keys, Distribution of Secret keys using Public Key Cryptosystems. X.509 .Discrete Logarithms, Diffie-Hellman Key Exchange.

Unit IV

Message Authentication and Hash Function: Authentication requirements, authentication functions, message authentication code, hash functions, birthday attacks, security of hash functions and MAC, MD5 message digest algorithm, Secure hash algorithm(SHA).Digital Signatures: Digital Signatures, authentication protocols,digital signature standards (DSS), proof of digital signature algorithm.Remote user Authentication using symmetric and Asymmetric Authentication

Unit V

Pretty Good Privacy.IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulation Security Payload in Transport and Tunnel mode with multiple security associations (Key Management not Included).Strong Password Protocols: Lamport's Hash, Encrypted Key Exchange.