Subject: Information and Network Security (2170709)

B.E. SEM – VII, CE, CSE, IT

Questions Bank

Unit : 01	
Topics ➲	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques

1	Explain the challenges of Computer Security.	
2	Briefly describe types of Security attacks.	
3	Draw and explain Network Security Model.	
4	Define the terms. : Plain text, Cipher text, Cryptography, Cryptanalysis, Brute-Force attack,	
5	Draw and explain Symmetric Cipher Encryption Model.	
6	Describe below substitution techniques. Caesar Cipher, Monoalphabetic Cipher, Polyalphabetic Cipher, Playfair Cipher, Hill Cipher, Vernam Cipher	
7	Describe Transposition techniques. Rail fence Cipher, Columnar Transposition Cipher technique.	

Unit : 02	
Topics ➲	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation

1	Describe Block Ciphers and Stream ciphers in brief.	
2	Explain Feistel Encryption and Decryption.	
3	Describe DES in brief.	
3	What is an Avalanche effect in DES?	
4	What is strength of DES?	
5	Briefly discuss Design Principles of Block Cipher.	
6	Explain AES Encryption process with diagram.	
7	Explain Key expansion in AES.	
8	Briefly describe SubBytes.	
9	Briefly describe ShiftRows.	
10	Briefly describe MixColumns	
11	Briefly describe AddRoundKey.	

Unit : 03	
Topics ➲	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode

1	What is Double DES and Triple DES Encryption?	
2	What is the meet-in-the-middle attack?	
3	Compare different Block Cipher modes of operation.	
3	Explain Electronic Codebook (ECB).	
4	Explain Cipher Block Chaining (CBC).	
5	Explain Cipher Feedback (CFB).	
6	Explain Output Feedback (OFB).	
7	Explain Counter (CTR).	

Unit : 04	
Topics ➲	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack

1	Explain Public key Cryptosystem. OR What are the principal elements of a public-key cryptosystem?	
2	What are the roles of the public and private key?	
3	Describe Public key Cryptosystem: Secrecy and Authentication.	
4	Explain applications of public-key cryptosystems?	
5	What requirements must a public key cryptosystems fulfill to be a secure algorithm?	
6	What is a one-way function?	
7	What is a trap-door one-way function?	
8	Explain RSA in brief.	
9	Briefly explain Diffie-Hellman key exchange.	
10	Describe Key Exchange protocols and Man-in-Middle attack in brief.	