CB3491 CRYPTOGRAPHY AND CYBER SECURITY

IMPORTANT QUESTIONS (Topics)

UNIT 1: INTRODUCTION TO SECURITY

1. Classical Encryption Techniques: Substitution, Steganography

2. Network Security: Types of Attacks, Mechanism

3. Modern Cryptography Terminologies: (Perfect security, Information Theory, Product Cryptosystem, Cryptanalysis)

4. Network Security: OSI architecture, Model

UNIT 2: SYMMETRIC CIPHERS

1. Euclid's Algorithm

2. Symmetric Key Ciphers: RC4, SDES

3. Modular Arithmetic

4. Group, Rings, Fields, Finite Fields

UNIT 3: ASYMMETRIC CRYPTOGRAPHY

1. Chinese Remainder Theorem

2. RSA cryptosystem

3. Euler's totient function, Fermat's and Euler's Theorem

UNIT 4: INTEGRITY AND AUTHENTICATION ALGORITHMS

1. Digital signature and authentication protocols

2. MAC, HMAC, CMAC 3. SHA

4. MUTUAL TRUST: Key management and distribution

5. Authentication Applications / X.509 Certificates

UNIT 5: CYBER CRIMES AND CYBER SECURITY

1. Cyber Crime: Basic Terminologies, Types, Lifecycle

2. SQL Injection, Spywares

3. Cyber Security: Wireless security, Web security, Cloud Security

4. Cybercrime (basic definitions): Pornography, Email spoofing, Phishing, Identity theft, Hacking

Expected Part-C Questions: (15 m)

1. Case Study Based (Units Combined Mean)

2. Authentication Application: Kerberos V4/V5 (Unit 4)

3. Algorithmic problem (Unit 2,3)