Module No.1
Introduction & Number Theory

1. Enlist security goals.Discuss their significance. **OR** Define goals of security and mechanism to achieve them. **OR** Explain the relationship between Security Services and Mechanisms in Detail ?
2. Explain network security model in detail with neat diagram.
3. Explain transposition ciphers with illustrative examples. **OR** Explain with example Keyed and Keyless Transposition Cipher ?
4. Write a short note on : (i)Steganography
5. List and explain various types of attacks on encrypted message.
6. Difference between : (i) Substitution Cipher and Transposition cipher
   (ii) Block ciphers and stream Ciphers
   (iii) Steganography and Cryptography
7. Numerical on:

   Substitution Ciphers:

   - Monoalphabetic Cipher
   - Additive Cipher
   - Multiplicative Cipher
   - Affine Cipher
   - Polyalphabetic Ciphers:
   - Playfair Cipher
   - Autokey Cipher
   - Vignere Cipher
   - Hill Cipher

   Transposition Ciphers

   - Keyed Transposition Ciphers
   - Keyless Transposition Ciphers

Note : Theory questions out of 10 M

Draw Neat Diagram.....4M
Explanation 6M

OR

Neat Diagram.....3M
Explanation 5M
Any mathematical equation ... 2M

Module No.2

Block Ciphers & Public Key Cryptography

1. Compare AES and DES which one is bit oriented and which one is byte oriented ?
2. Discuss in detail Block Cipher Modes of operation with example .

OR

What are block ciphers? Explain with examples the CBC and ECB modes of block ciphers.

OR

Discuss CBC and OFB Block cipher Modes with examples.

3. Write a short note on:**(Theory Questions)**

(a)AES Algorithm
(b) DES
(c) Triple DES
(d) RSA Algorithm
(e)Blowfish
(f) RC5
(g) Knapsack Algorithm
(e) El-Gamal Algorithm
(f) Diffie Hellman Key Exchange

Questions on : DES

6. Describe triple DES with two DES keys. Is man in the middle attack on triple DES? 5M
7. Explain working of DES detailing the Fiestel structure 10M

8. With reference to DES component of the followings:
   (i) Block size and Key size
   (ii) Need for expansion permutation
   (iii) Avalanche and completeness effects
   (iv) Weak keys and semi-weak keys.
   (v) Role of S--box

Question on : RSA

9. Elaborate the steps of key generation using RSA algorithm 5m

10 . Numerical on:

(i) RSA Algorithm.....**IMP**
(ii) Diffie Hellman Key Exchange.....**IMP**
(iii) Knapsack Algorithm
(iv) El-Gamal Algorithm

Note: Refer university question paper for numericals (uploaded in google classroom)

Module No.3
Cryptographic Hashes, Message Digests and Digital Certificates

1. What is the need for message Authentication?. List various techniques use for message authentication. Explain any one of them.
2. Define the proporties and applications of HASH function? Explain role of hash function in security

OR

Explain Hash Based Message Authentication Code. Give Example also.

3. Give the format of X 509 digital certificate and explain the use of a digital signature in it.

OR

Explain Digital Signature and Digital Certificate used for authentication

4. Comparison between : (I) HMAC,CBC-MAC AND CMAC.
   (II)MD-5 versus SHA
5. SHA provides better security than MD. Justify.
6. What is PKI ? Explain different PKI architectures in detail.
7. What characteristics are needed in secure hash function? Explain the operation of secure hash algorithm on 512 bit block.
8. What is the significance of a digital signature on a certificate ? Justify.
9. Write a short note on :
   (i) SHA-1 **OR** SHA-256
   (ii)MD5
   (iii) HMAC
   (iv) CMAC
   (v) X.509

10.