Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1	a.	Explain Playfair Cipher	Algorithm.	Find the Ciphertext	for plaintext =	"instruments"	with
		key = "MONARCHY".	(	4		(10 M	(arks)

Explain with neat diagram Feistel Cipher structure for Encryption and Decryption. (10 Marks)

Explain Hill Cipher Algorithm. Using Hill-Cipher perform encryption and decryption for

17 17 45 plaintext = "paymoremoney" using key K = 21 18

b. Explain with neat diagram DES encryption algorithm.

(10 Marks)

(10 Marks)

Module-2

a. Explain RSA algorithm. Using RSA algorithm perform encryption and decryption using p = 17, q = 11, e = 7 and M = 88.(10 Marks)

b. Explain Diffie-Hellman key exchange algorithm and also show that the calculations produce the identical results.

(10 Marks)

a. Explain Elgamal cryptosystem. Perform encryption and decryption using  $q=19,\ \alpha=10$ , k = 6, M = 17,  $X_A = 5$  and  $Y_A = 3$ . (10 Marks)

b. Explain the requirements and applications for public key cryptography.

(10 Marks)

Module-3

Explain the concept of PRNG based on RSA.

(10 Marks)

Explain the distribution of public keys with public key Authority.

(10 Marks)

Explain with neat diagram control vector encryption and decryption.

(10 Marks)

Explain distribution of public keys using public key certificates.

(10 Marks)

Module-4

Explain X.509 certificate format.

(10 Marks)

Bring out the differences between Kerberos version 4 and version 5 and also mention the technical deficiencies in Kerberos version 4 protocols. (10 Marks)

OR

Explain PKIX architectural model.

(10 Marks)

Explain with neat diagram the key components of Internet Mail Architecture.

(10 Marks)

Module-5

Explain the benefits and applications of IPsec.

(10 Marks)

b. Explain the IP traffic processing for outbound and inbound packets.

(10 Marks)

10 Explain ESP packet format.

(10 Marks)

Explain the concept of transport and tunnel modes.

(10 Marks)

Important Note: 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.

2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.