CBCS SCHEME

USN □□□□□□□□□□

18CS744

Seventh Semester B.E. Degree Examination, Jan./Feb. 2023

Cryptography

Time: 3 hrs. Max. Marks: 100

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

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.

Module-1

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

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

OR

2 a. Explain Hill Cipher Algorithm. Using Hill-Cipher perform encryption and decryption for plaintext = "paymoremoney" using key $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$. **(10 Marks)**

b. Explain with neat diagram DES encryption algorithm. **(10 Marks)**

Module-2

3 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)**

OR

4 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

5 a. Explain the concept of PRNG based on RSA. **(10 Marks)**

b. Explain the distribution of public keys with public key Authority. **(10 Marks)**

OR

6 a. Explain with neat diagram control vector encryption and decryption. **(10 Marks)**

b. Explain distribution of public keys using public key certificates. **(10 Marks)**

Module-4

7 a. Explain X.509 certificate format. **(10 Marks)**

b. 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

8 a. Explain PKIX architectural model. **(10 Marks)**

b. Explain with neat diagram the key components of Internet Mail Architecture. **(10 Marks)**

Module-5

9 a. Explain the benefits and applications of IPsec. **(10 Marks)**

b. Explain the IP traffic processing for outbound and inbound packets. **(10 Marks)**

OR

10 a. Explain ESP packet format. **(10 Marks)**

b. Explain the concept of transport and tunnel modes. **(10 Marks)**

* * * * *