CBCS SCHEME

USN | | | | | | | | | | 18CS744

Seventh Semester B.E. Degree Examination, Feb./Mar. 2022
Cryptography

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Draw the simplified model of symmetric encryption and explain it **(06 Marks)**

b. With a neat schematic, explain the DES encryption algorithm. **(10 Marks)**

c. Encrypt he plaintext "ELECTRONICS" using a playfair cipher with a key "INDIA". **(04 Marks)**

OR

2 a. Encrypt the plaintext "CRYPTOGRAPHY" using HILL CIPHER technique with key matrix $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and decrypt the same. **(10 Marks)**

b. Distinguish between:
i) Confusion and Diffusion ciphers
ii) Block cipher and stream ciphers. **(06 Marks)**

c. Explain Caesar cipher with an example. **(04 Marks)**

Module-2

3 a. With a neat diagram, explain the six ingredients of a public-key cryptography. **(06 Marks)**

b. Explain RSA algorithm operation in detail. Perform an encryption of plain text and decryption of cipher text using RSA algorithm for P = 3, q = 11, e = 7 and M = 5. **(10 Marks)**

c. Explain the Elgamal cryptosystem. **(04 Marks)**

OR

4 a. With relevant diagram, explain Authentication and secrecy in public-key cryptosystem. **(06 Marks)**

b. Explain Diffie-Hellman key exchange algorithm. Apply Diffie-Hellman key exchange algorithm for q = 71, its primitive root α = 7. A's private key is 5, B's private key is 12. Find: i) A's public key ii) B's public key iii) Shared secret key. **(10 Marks)**

c. What requirements must a public-key cryptosystems fulfill to be a secure algorithm? **(04 Marks)**

Module-3

5 a. With a neat diagram, explain public-key authority and public-key certificates techniques for the distribution of public keys. **(08 Marks)**

b. Apply Elliptic curve arithmetic on the elliptic curve E23 (1, 1), P = (3, 10) and Q = (9, 7). Find: i) P+Q ii) 2P **(06 Marks)**

c. Explain ECC Diffie-Hellman key exchange, elliptic curve encryption and decryption process. **(06 Marks)**

OR

6 a. With relevant diagram, explain the key distribution scenario. (07 Marks)
b. With a neat diagram, explain pseudo random number generation based on RSA. (07 Marks)
c. With a neat diagram, explain secret key distribution with confidentiality and authentication. (06 Marks)

Module-4

7 a. With a neat diagram, explain the general format of X.509 certificate. (10 Marks)
b. With relevant diagram, explain the confidentiality and authentication services provided by PGP protocol. (10 Marks)

OR

8 a. Explain Kerberos version and message exchanges. (07 Marks)
b. With relevant diagram, explain the DKIM functional flow. (08 Marks)
c. Describe the various header fields defined in MIME. (05 Marks)

Module-5

9 a. Draw a diagram to illustrate IP security scenario and also explain benefits of IPsec. (08 Marks)
b. Discuss the top level format of an Encapsulating Security Payload (ESP) packet. (08 Marks)
c. List the important features of IKE KEY Determination algorithm. (04 Marks)

OR

10 a. Draw and explain the IP traffic processing model for inbound and outbound packets. (10 Marks)
b. With relevant diagram, describe IKE header and payload format. (10 Marks)

* * * * *