CBCS SCHEME

USN | | | | | | | | | | |

18CS744

Seventh Semester B.E. Degree Examination, June/July 2024
Cryptography

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. What are the three independent dimensions of cryptography? Explain. **(06 Marks)**

b. Explain unconditionally secure and computationally secure encryption schemes. **(04 Marks)**

c. If intruder has an access to part of plaintext and corresponding cipher text generated using Hill Cipher. Part plaintext is TECH and corresponding Cipher text is NQUZ. Estimate key and decrypt the message NQUZ TQTE. **(10 Marks)**

OR

2 a. Compare stream Cipher and block Cipher. **(06 Marks)**

b. Illustrate one round of Feistel Cipher. Assume that the data received from previous round is 1A2B3C4D and key used is 123ABC. **(04 Marks)**

c. Explain DES algorithm and its strength. **(10 Marks)**

Module-2

3 a. Illustrate the application of public-key cryptosystem for

i) Authentication

ii) Secrecy

iii) Authentication and secrecy application. **(10 Marks)**

b. Encrypt plaintext 9 using the RSA public-key encryption algorithm. Use prime numbers p = 7 and q = 11 to generate the public and private keys. Demonstrate Chinese reminder theorem in RSA while decrypting. **(10 Marks)**

OR

4 a. Illustrate Man-in-the-Middle attack in Diffie-Hellman key exchange algorithm. **(05 Marks)**

b. Compute public-key and secrete key of two users using Diffie-Hellman key exchange algorithm. Use q = 353, X_A = 97 and X_B = 233. **(10 Marks)**

c. Explain Elgamal cryptographic algorithm. **(05 Marks)**

Module-3

5 a. Summarize Abelian group and Elliptic curves over real numbers. **(06 Marks)**

b. List the two families of elliptic curves used in cryptography applications and explain them. **(08 Marks)**

c. Consider the group $E_{23}(1, 1)$ compute 3G left base point G = (3, 10). **(06 Marks)**

OR

6 a. Explain the public-key authority technique and public-key certification technique of public-key distribution. How they are more secure than public announcements and publicly available directory, technique? **(10 Marks)**

b. Explain simple key distribution mechanism and illustrate man-in-the-middle attack for the scheme. Explain any one scheme to over come the attack. **(10 Marks)**

Module-4

7 a. What requirements are not satisfied by X509 version 2? Explain each extension of version 3. **(10 Marks)**

b. Illustrate the working of Kerberos and explain the Kerberos exchanges among the parties in a network. **(10 Marks)**

OR

8 a. Write about the following with respect to S/MIME:
i) S/MIME functionalities.
ii) Cryptography algorithm used. **(10 Marks)**

b. What is Domain keys identified mail? Summarize internet mail architecture. **(10 Marks)**

Module-5

9 a. What is IPsec? List its applications. Illustrate how IPsec is used in an organization. **(08 Marks)**

b. Compare transport mode and tunnel mode with respect to functionalities supported by security services of IPsec. Taking an example explain how tunnel mode IPsec operates. **(06 Marks)**

c. Recall the services of ESP. With a neat diagram, explain ESP packet format. **(06 Marks)**

OR

10 a. Illustrate using ESP with IPV4 and IPV6. Summarize the transport mode operation. **(10 Marks)**

b. What is the use of Tunnel Mode ESP? Explain the steps that occur when an external host wishes to communicate with a host on an internal network protected by a firewall, and in which ESP is implemented in the external host and the firewalls. **(10 Marks)**

* * * * *