CBCS SCHEME

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

15EC744

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

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Generate the table for GF(2^3) Addition, Multiplication and also find additive multiplicative inverses. **(08 Marks)**

b. Write the Euclid's algorithm for determining the GCD of two positive integers. Also find the GCD of (24140, 40902) using Euclid's algorithm. **(08 Marks)**

OR

2 a. Explain in detail group, Ring and Field. **(08 Marks)**

b. For the given polynomial perform addition, subtraction, multiplication and division operations over GF(2)

$f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$ and $g(x) = x^3 + x + 1$ **(08 Marks)**

Module-2

3 a. Explain the general model of network security system. **(08 Marks)**

b. Explain the playfair rules for encryption using play fair keyword "MESSAGE". Encrypt the plain text "CRYPTOGRAPHY". **(08 Marks)**

OR

4 a. Wit neat diagram, explain single round DES along with the key generation. **(08 Marks)**

b. Encrypt the plain text "SECURITY" using Hill Cipher technique with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Find the Cipher text. **(08 Marks)**

Module-3

5 a. With a neat diagram, explain the AES Encryption algorithm. **(08 Marks)**

b. Explain the AES key expansion algorithm with neat diagram. **(08 Marks)**

OR

6 a. Explain the LFSR with neat diagram. **(08 Marks)**

b. Explain the following stream ciphers with neat diagrams:

(i) Alternating stop and go generator.

(ii) Bilateral stop and go generator. **(08 Marks)**

Module-4

7 a. Explain Diffie Hellman key exchange algorithm. Also find (i) A's public key (ii) B's public key (iii) Shared secret key using Diffie Hellman key exchange q = 71, its primitive root $\alpha = 7$. A's private key is '5' B's private key is 12. **(08 Marks)**

b. Explain RSA algorithm, also perform encryption and decryption using RSA algorithm for p = 7, q = 11, e = 17 and m = 8 **(08 Marks)**

OR

8 a. State and explain Fermat's theorem, also find prime number a =7, p = 19. **(08 Marks)**

b. Explain Chinese remainder theorem. By using CRT find 'X' for the following:

$X \equiv 1 \pmod{5}$

$X \equiv 2 \pmod{6}$

$X \equiv 3 \pmod{7}$ **(08 Marks)**

Module-5

9 a. Briefly explain the operation of MD_4 and MD_5. **(08 Marks)**

b. With neat diagram, explain general hash function length equals block size. **(08 Marks)**

OR

10 a. Explain discrete logarithm signature schemes. **(08 Marks)**

b. Write a note on digital signature algorithm. **(08 Marks)**

* * * * *