CBCS SCHEME

USN | | | | | | | | | |

15EC744

Seventh Semester B.E. Degree Examination, Dec.2018/Jan.2019
Cryptography

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Explain the Euclid's algorithm for determining the GCD of two positive integers. Find the GCD of (1970, 1066) using Euclid's algorithm. **(08 Marks)**

b. Mention the Modular Arithmetic Operation properties and prove the same. **(08 Marks)**

OR

2 a. Explain the extended Euclid's Algorithm for determining the GCD and multiplicative inverse of two integers. **(08 Marks)**

b. Find gcd [a(x), b(x)] for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$. **(08 Marks)**

Module-2

3 a. Draw the model of symmetric cryptosystem and explain it. **(08 Marks)**

b. Explain playfair Cipher and its rules for the following example:
Ex: Keyword : "Computer"
Plaintext : "parrot" **(08 Marks)**

OR

4 a. Using Hill Cipher technique encrypt and decrypt the plain text "crypto" using the key $K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$. **(08 Marks)**

b. With a neat block diagram, explain general depiction of DES encryption algorithm. **(08 Marks)**

Module-3

5 a. Explain with a neat diagram of AES encryption process. **(08 Marks)**

b. Explain AES key expansion algorithm. **(08 Marks)**

OR

6 a. Explain linear feedback shift registers with necessary diagrams. **(08 Marks)**

b. Explain the following with necessary diagrams:
i) Generalized Geffe Generator
ii) Threshold Generator. **(08 Marks)**

Module-4

7 a. State and prove Fermat's Theorem. Also find 3^{201} mod 11 using it. **(08 Marks)**

b. Explain Chinese Remainder Theorem. By using CRT, find 'x' for the following:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$. **(08 Marks)**

OR

8 a. Explain elaborately Diffie-Hellman key exchange algorithm. **(05 Marks)**

b. Perform encryption and decryption using RSA algorithm for p = 3, q = 11, e = 7 and M = 5. **(06 Marks)**

c. Explain Elliptic curve over real numbers. **(05 Marks)**

Module-5

9 a. Explain the concept of N-Hash algorithm with a neat diagram. **(08 Marks)**

b. With the neat diagram, explain the operation of Secure Hash Algorithm (SHA). **(08 Marks)**

OR

10 a. What are the criticisms against DSA, explain in brief. **(08 Marks)**

b. Explain Discrete Logarithm Signature schemes. **(08 Marks)**

* * * * *