CBCS SCHEME

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

15EC744

Seventh Semester B.E. Degree Examination, Aug./Sept.2020
Cryptography

Time: 3 hrs. Max. Marks: 80

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. Find the greatest common divisor (1970, 1066) using Euclidean Algorithm and Explain the Algorithm. **(07 Marks)**

b. Explain Extended Euclid algorithm for (m, b). **(05 Marks)**

c. Define Rings and its axioms. **(04 Marks)**

OR

2 a. Define groups and fields. Explain its axioms. **(06 Marks)**

b. Explain polynomial Arithmetic, with an examples. **(05 Marks)**

c. List out the properties of modular Arithmetic for integers in Z_n. **(05 Marks)**

Module-2

3 a. With an example explain play fair cipher. **(09 Marks)**

b. Explain transposition techniques. **(04 Marks)**

c. What is Causal cipher? Give an example. **(03 Marks)**

OR

4 a. Encrypt a message "Paymole money" using a Hill cipher with the key

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$ **(08 Marks)**

b. With the help of block diagram explain single round of DES algorithm. **(08 Marks)**

Module-3

5 a. With the help of block diagram explain AFS Encryption and decryption. **(10 Marks)**

b. With a example explain 4-bit linear feedback shift registers. **(06 Marks)**

OR

6 a. Elaborate geffe generator, generalized geffe generator and stop-and-go generator of stream ciphers using LFSRs. **(08 Marks)**

b. With the help block diagram Beth-piper stop-and-go generator, alternating stop-and-go generator and Bilateral stop-and-go generator. **(08 Marks)**

Module-4

7 a. State and prove Felmat's theorem. **(05 Marks)**

b. Briefly explain RSA algorithm and key generation. **(07 Marks)**

c. Differentiate between conventional and public-key Encryption. **(04 Marks)**

OR

8 a. State and prove Euler's theorem. (05 Marks)

b. Discuss Diffie Hellman key exchange algorithm. Explain how the algorithm is used to exchange secret key. (06 Marks)

c. In RSA system it is given P = 17, q = 11, e = 7, M = 88. Find the cipher text C and message M from decryption. (05 Marks)

Module-5

9 a. Explain the requirements for message authentication codes. (08 Marks)

b. With the help of neat diagram, explain the message digital generation using SHA-512. (08 Marks)

OR

10 a. Explain direct digital signature and arbitrated digital signature. (08 Marks)

b. Explain MDS main loop. (08 Marks)

* * * * *

VTU-02-09-2020 09:15:46am SN - SN - SN - SN - SN