7932

BCA VIth Semester Examination, 2024

CRYPTOGRAPHY

Paper : BCA–6044

Time : 3 Hours] [*M.M. : 70*

Note :– Answer any *five* questions. All questions carry equal marks.

1. Explain the concept of block cipher in Cryptography. Discuss the modes of operations of block cipher. [14]

2. Draw the block diagram of DES algorithm. Also explain its functionality in detail. [14]

3. What do you mean by cryptography ? Explain the different types of security attack in cryptography and also define services and mechanisms. [14]

4. Define the concept of Blowfish and how is it used in cryptography ? Explain in detail. [14]

5. Explain the following :

(i) Triples DES

(ii) RC5 [14]

6. Explain Chinese Remainder Theorem (CRT) and find X for the given set of congruent equations using CRT:

X = 1 mod 5

X = 2 mod 7

X = 3 mod 9

X = 4 mod 11 [14]

7. Describe RSA algorithm in detail. Calculate the private key of A where in RSA Cryptosystem a particular A uses two prime numbers p = 13 and q = 17 to generate her public and private key. Lets the public key of A is 35. [14]

8. Explain the idea of Digital Signature for the authentication. Discuss signing and verifying process of Digital Signature Algorithm (DSA) in detail. [14]

9. Why message authentication is required ? Discuss working of MAC with suitable block diagram. [14]

10. What do you understand by hash functions ? Discuss the working of secure hash algorithm (SHA) in message authentication. [14]