2022

COMPUTER SCIENCE

Paper : CSMC-204

(Cryptography and Network Security)

Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer ***question no.* 1, *question no.* 2** and ***any four*** questions from the rest.

1. Answer ***any five*** of the following : 2×5

(a) What is the basic difference between steganography and cryptography?

(b) State Shanon's Theorem.

(c) What is an active attack?

(d) What is a polyalphabetic cipher? Give an example.

(e) Given a set of elements G and a binary operation * and (G,*) is a group what additional property must (G,*) have, so that it becomes a Commutative group.

(f) What is ESP in IPsec documentation?

(g) What is a replay attack?

2. Answer ***any five*** of the following :

(a) Describe the steps of 3DES. 4

(b) State two different ways in which polynomials can be stored. Compare the time complexity of performing addition and multiplication of two polynomials in both the representations. 2+2

(c) What are the components of a feistel structure? 4

(d) Solve the simultaneous congruences $x \sim 6 \pmod{11}$, $x \sim 13 \pmod{16}$, $x \sim 9 \pmod{21}$, $x \sim 19 \pmod{25}$. 4

(e) Describe the general AES structure by means of a block diagram. Why is the AES structure not a feistel structure? 3+1

(f) How can hashcode be used if both confidentiality as well as digital signature are required? 4

(g) What are the two types of firewalls? Discuss the differences between the two types. 2+2

3. State the block cipher modes of operation and give a brief description of each mode. 10

4. (a) What are the steps of Elgamal encryption? Explain with an example.

   (b) How can it be used to verify digital signature? 7+3

5. (a) What is a hash function?

   (b) What are the properties a good cryptographic hash function must have?

   (c) Give two different ways in which hash codes can be used to provide message authentication. 2+3+5

6. (a) What are the services provided by IPsec?

   (b) Describe transport and tunnel mode. 4+6

7. (a) Describe a key distribution protocol using key distribution center (KDC).

   (b) Show mathematically, how KDC reduces the number of keys needed to be shared between n clients than if the clients communicated within themselves without using KDC for symmetric key cryptography. 6+4
