2017

Time : 3 hours

Full Marks : 80

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

The figures in the margin indicate full marks.

*Answer **five** questions in which Q. No. 1 is compulsory.*

1. Choose the correct alternative of the following : 2×8 = 16

(a) In Cryptography, what is Cipher ?

(i) Algorithm for performing encryption and decryption

(ii) Encrypted message

(iii) Both (i) and (ii)

(iv) None of the mentioned

(b) In asymmetric key Cryptography the private key is kept by :

(i) Sender

(ii) Receiver

(iii) Sender and receiver

(iv) All the connected devices to the network

(c) In Crytography the order of the letters in a message is rearranged by :

(i) Transpositional ciphers

(ii) Substitution ciphers

(iii) Both (i) and (ii)

(iv) None of these

(d) Which one of the following is not used in assymmetric key cryptography ?

(i) RSA algorithm

(ii) Diffie-Heltman algorithm

(iii) Electronic code book algorithm

(iv) None oth these

(e) What is a data encryption standard (DES) ?

(i) Block Cipher

(ii) Bit Cipher

(iii) Stream Cipher

(iv) None of these

(f) Cryptanalysis is used :

(i) To find some insecurity in a cryptographic scheme

(ii) To increase the speed

(iii) To encrypt the data

(iv) None of these

(g) Which one of the following is a cryptographic protocol used to secure HTTP connection ?

(i) Stream Control Transmission Protocol (SCTP)

(ii) Transport Layer Security (TSL)

(iii) Explicit Congestion Notification (ECN)

(iv) Resource Reservation Protocol

(h) Voice privacy in GSM cellular telephone protocol is provided by :

(i) 5/2 Cipher

(ii) 5/4 Cipher

(iii) 5/6 Cipher

(iv) 5/8 Cipher

2. Define Euler's totient function or phi-function and their applications. 16

3. Compare stream cipher and block cipher with example. 16

4. What are the advantages and disadvantages of one time pad encryption algorithm or Diffie-Hellman algorithm. 16

5. Distinguish active and passive attack with examples. 16

6. How many keys are required for two people to communicate via a cipher ? Explain SSL and TLS protocol in short. 16

7. What are the types of attacks on encrypted message ? Explain Cryptanalysis and cryptography. 16

8 What are the key principles of security ? How does Firewall helps. 16

9. What are the two approaches of digital signatures ? Describe about hash functions. 16