2019

Time : 3 hours

Full Marks : 80

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

The questions are of equal value.

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

1. Choose the correct alternative of the following :

   (a) A substitution cipher substitutes one symbol with :

   (i) Keys

   (ii) Others

   (iii) Multiple parties

   (iv) Single party

   (b) An asymmetric-key (or public-key) cipher uses :

   (i) 1 key

   (ii) 2 key

(iii) 3 key

(iv) 4 key

(c) We use Cryptography term to transforming messages to make them secure and immune to :

(i) Change

(ii) Idle

(iii) Attacks

(iv) Defend

(d) Heart of Data Encryption Standard (DES) is the :

(i) Cipher

(ii) Rounds

(iii) Encryption

(iv) DES function

(e) Advanced Encryption Standard (AES), has three different configuaration with respect to number of rounds and :

(i) Data size

(ii) Round size

(iii) Key size

(iv) Encryption size

(f) Caesar cipher is an example of :

(i) Substitution cipher

(ii) Transposition cipher

(iii) Substitution as well as transposition cipher

(iv) None of these

(g) A digital signature needs a :

(i) Private key system

(ii) Shared key system

(iii) Public key system

(iv) All of these

(h) When data must arrive at receiver exactly as they were sent, its called :

(i) Message Confidentiality

(ii) Message Integrity

(iii) Message Splashing

(iv) Message Sending

2. What are the tools available for session hijacking ? Explain briefly how they work.

3. What is the relation between security mechanisms and attacks ? Explain.

4. What is Message Authentication ? How is it different from Message integrity ? What is phishing ?

5. Determine the security services required to counter various types of active and passive attacks. What are the common C-functions that give raise to buffer overflow ?

6. What is plain text ? What is cipher-text ? Give an example of transformation of plains text into cipher text.

7. Explain Secure Socket Layer in details ? What is e-mail security ?

8. Explain Data Encryption Standard (DES) in details. How can the same key be reused in triple DES ?

9. Write short notes on any two the following :

   (a) Digital signature algorithm

   (b) Cryptographic hash function

   (c) IDEA algorithm

   (d) RSA algorithm