B.TECH/IT/8TH SEM/INFO 4243/2019
CRYPTOGRAPHY & NETWORK SECURITY
(INFO 4243)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

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

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) ..... is an attack in availability
(a) interception (b) interruption (c) both a and b (d) none of this.

(ii) ..... mode cannot be used for transmitting long messages.
(a) ECB (b) CBC (c) OFB (d) all of these.

(iii) ..... algorithm produces 160-bit hash value.
(a) MD5 (b) SHA (c) all of these (d) none of these.

(iv) OSI position of ..... is between transport and application.
(a) IPSec (b) SSL (c) all of these (d) none of these.

(v) ..... is susceptible to bucket brigade attack.
(a) Diffie-Hellman (b) Double DES (c) both (a) and (b) (d) none of these.

(vi) Key ring is found in.....
(a) PEM (b) PGP (c) SSL (d) none of these.

(vii) ..... is a computationally secure encryption algorithm.
(a)DES (b) BDE (c) RC5 (d) both a and c.

(viii) ..... cipher uses 6 × 6 matrix.
(a) Hill (b) Rail fence (c) Polygram (d) Playfair.

(ix) ..... mode uses stream cipher.
(a) CFB (b) OFB (c) both (a) and (b) (d) none of these.

(x) ..... is a combination of cryptography and cryptanalysis
(a) Linear cryptanalysis (b) Differential cryptanalysis
(c) Cryptology (d) none of these.

Group – B

2. (a) State and discuss different principles of security with proper examples. Differentiate between masquerade and pharming.

(b) State the cipher text for the plain text ***"fundamentals of network security"*** using (i) Caesar cipher technique with key=9 and (ii) Rail fence technique.

(6 + 2) + 4 = 12

3. (a) Differentiate between brute force attack and cryptanalysis.

(b) State the cipher text for the plain text **"23, Elgin road, Kolkata-700026"** using Playfair substitution technique. Keyword to be used is **Network cryptanalysis** *(Step detailing and diagram mandatory for above problem.)*

(c) Discuss different approaches of security.

2+ 6 + 4 = 12

Group – C

4. (a) Explain the following algorithm modes with neat diagram:
(i) Cipher feedback mode
(ii) Counter mode
(iii) Output feedback mode

(b) Explain Diffie-Hellman key exchange algorithm.

9 + 3 = 12

5. (a) Discuss single round encryption of IDEA algorithm in detail including output transformation round.

(b) Explain different modes of RC5.

8 + 4 = 12

Group – D

6. (a) Explain RSA algorithm in detail. Calculate public key and private key for p=7 and q=17 using RSA algorithm.

(b) Explain strong, weak and random password with suitable example.

(3 + 3) + 6= 12

7. (a) Explain the working of HMAC algorithm in detail with neat diagram.

(b) State the requirements of asymmetric key cryptography.

(c) Differentiate between MD5 and SHA-1.

6+ 3 + 3 = 12

Group – E

8. (a) Explain different attacks possible on packet filtering router. State the suitable countermeasure for each attack.

   (b) Explain with neat sketch, the working of PGP mail security protocol.

6 + 6 = 12

9. (a) Why SSL is placed between application layer and transport layer of OSI model?

   (b) State atleast two advantages and drawbacks of application-level gateway.

   (c) Explain with neat sketch, the working of handshake protocol in SSL.

2+ 2 + 8 = 12