**SPECIAL SUPPLE B.TECH/IT/8TH SEM/INFO 4243/2018**

# CRYPTOGRAPHY AND 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 Authentication
(a) Confidentiality (b) Integrity
(c) Fabrication (d) None of these.

(ii) ..... is an unconditionally secure encryption algorithm.
(a) One time pad cipher (b) DES
(c) IDEA (d) all of these.

(iii) ..... cipher uses 5x5 matrix.
(a) Hill (b) Rail fence
(c) Polygram (d) Playfair.

(iv) ..... cipher uses Vignere table
(a) Polyalphabetic (b) Polygram
(c) none of these (d) Monoalphabetic.

(v) ..... algorithm uses 16 rounds of encryption.
(a) DES (b) IDEA
(c) FEAL (d) SAFER.

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

(vii) ..... algorithm produces 128 bit hash value.
(a) MD5 (b) SHA
(c) all of these (d) none of these.

(viii) Blinding is a countermeasure applicable in .....
(a) RSA (b) DES
(c) MD2 (d) all of these.

(ix) FAR and FRR are applicable with.....
(a) Certificate Authentication
(b) Biometric Authentication
(c) Fabrication
(d) none of these.

(x) Record protocol is a sub protocol of.....
(a) DES (b) IDEA
(c) SSL (d) RSA.

## Group - B

2. (a) State and discuss different principles of security with proper examples. Differentiate between Substitution and Transposition technique.

(b) State the cipher text for the plain text "***Network Security***" using (i) Caesar cipher technique with key = 5 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 "**11, Garia road, Kolkata-700142**" using Playfair substitution technique. Keyword to be used is **Cryptography**
(*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) Counter mode
(ii) Output Feedback mode
(iii) Cipher block chaining mode.

(b) State the steps of Diffie-Hellman Key Exchange algorithm.

**9 + 3 = 12**

5. (a) Discuss Single round encryption of DES algorithm in detail.

   (b) Differentiate between Algorithm types and modes. Explain Cipher Feedback mode with neat diagram.

**5 + (2 + 5) = 12**

## Group - D

6. (a) State the requirements of Asymmetric key cryptography.

   (b) Explain RSA algorithm in detail. Calculate public key and private key for p = 7 and q = 11 using RSA algorithm. What is Authentication token?

**5 + (3 + 3 + 1) = 12**

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

   (b) State the requirements of Digital Signature (Any Five).

**7 + 5 = 12**

## Group - E

8. (a) Explain the working of Handshake protocol in detail with neat diagrams.

   (b) Explain the working of Alert protocol in detail with neat diagram.

**9 + 3 = 12**

9. (a) Explain with neat sketch, the working of PEM mail security protocol.

   (b) Explain DMZ architecture of firewall with neat diagram. State the characteristics of firewall.

**6 + (3 + 3) = 12**