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 on confidentiality
(a) Interception (b) Interruption
(c) Integrity (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) PGP (d) None of these.

(v) ..... is susceptible to Bucket Brigade attack.
(a) Diffie-Hellman (b) Double DES
(c) Triple DES (d) None of These.

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

(vii) ..... mode uses stream cipher.
(a) CFB (b) OFB (c) Both (a) and (b) (d) None of these

(viii) ..... accommodates varying number of rounds and variable bit key size.
(a) DES (b) RC5 (c) MD2 (d) All of these.

(ix) Mathematical attack is applicable in .....
(a) RSA (b) DES (c) MD2 (d) All 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) Differentiate between substitution and transposition technique.

(b) State the cipher text for the plain text "***fundamentals of cryptography***" using (i) Caesar cipher technique with key=7

(c) State the conditions for an encryption algorithm to be computationally secure.

(d) Describe the following attacks with an example each: replay attack, reflection attack, DoS attack.

2+ 2+ 2+ 6 = 12

3. (a) State the cipher text for the plain text "**15, Hazra road, Kolkata-700029**" using Playfair substitution technique. Keyword to be used is **Network security.** (*Step detailing and diagram mandatory for above problem.*)

(b) Discuss different types of attack on an encrypted text performed by cryptanalyst.

(c) Differentiate between symmetric key cryptography and asymmetric key cryptography.

6 + 4 + 2 = 12

Group – C

4. (a) Explain the following algorithm modes with neat diagram:
(i) Electronic code book mode
(ii) Cipher block chaining mode

(b) Explain the concept of digital envelope.

(c) Explain RC5 encryption algorithm in detail, with a neat diagram.

6+ 2 + 4 = 12

5.(a) State the principles of diffusion and confusion. What is cryptology?

(b) Discuss Man in the Middle attack with suitable numeric example.

(c) Explain the drawback of DES and Double DES algorithm and state the concept of Triple DES algorithm. Use suitable diagrams as necessary.

(2+1)+ 4+5 = 12

Group – D

6. (a) Calculate public key and private key for p=11 and q=17 using RSA algorithm.

   (b) State the properties of digital signature.

   (c) Explain the working of HMAC algorithm in detail, with neat diagram.

3+ 3 + 6 = 12

7. (a) Explain the attacks on RSA algorithm and discuss its countermeasures.

   (b) Differentiate between certificate based authentication and biometric authentication.

   (c) State the requirements of hash function.

6+ 3 + 3 = 12

Group – E

8. (a) Differentiate between hardware firewall and software firewall. Explain different types of firewall with neat diagram (s).

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

(2 + 5)+ 5 = 12

9.(a) What is a firewall? Explain different types of firewall configurations.

   (b) Explain the working of record protocol in detail, with a neat diagram.

   (c) Enumerate the steps in working of S/MIME protocol.

(1 + 4)+ 3+4= 12