B.TECH/AEIE/ECE/8TH SEM/INFO 4281/2019
FUNDAMENTALS OF CRYPTOGRAPHY
(INFO 4281)

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) .... suffers from meet in the middle attack.
(a) Double DES (b) Triple DES (c) RSA (d) SSL.

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

(iii) .... uses block cipher.
(a) Caesar cipher (b) Rail fence (c) Polygram (d) Playfair.

(iv) .... cipher uses both transposition and substitution.
(a) Combinational (b) Product (c) Double (d) none of these.

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

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

(vii) .... firewall hinders system performance.
(a) Hardware (b) Software (c) Hybrid (d) none of these.

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

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

(x) DNS Secure protocol is a countermeasure used in...................... attack
(a)PEM (b) pharming (c) SSL (d) none of these.

Group – B

2. (a) What is cryptology? Differentiate between monoalphabetic cipher and homophonic cipher.

(b) State the cipher text for the plain text "***cryptography and network security***" using (i) Caesar cipher technique with key=7 and (ii) Rail fence technique.

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

(1 + 2) + 4 +5 = 12

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

(b) State the cipher text for the plain text "**15, Garia station road, Kolkata-700132"** using Playfair substitution technique. Keyword to be used is **NETWORK FUNDAMENTALS**.

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

2+ 6 + 4 = 12

Group – C

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

(b) Draw and explain the block diagram of DES encryption algorithm.

(c) Differentiate between confusion and diffusion.

(2 + 4)+ 3 + 3= 12

5. (a) Explain Diffie-Hellman key exchange algorithm.

(b) Explain in detail, key shifting process of IDEA encryption algorithm from round 1 to round 8.

4 + 8 = 12

Group – D

6. (a) Explain RSA algorithm in detail. Calculate public key and private key for p=5 and q=13 using RSA algorithm.

(b) State the requirements of asymmetric key cryptography.

(c) State the requirements of digital signature.

(3 + 3)+4 +2= 12

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

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

(c) Explain time based authentication token.

6+ 4 + 2 = 12

Group – E

8. (a) What is firewall? Explain different types of firewall configuration with neat diagram.

(b) Differentiate between hardware firewall and software firewall. Explain application-level gateway and circuit-level gateway.

(1 + 5)+(2 + 4) = 12

9.(a) Explain the working of handshake protocol in detail with neat diagrams.

(b) Explain the attacks on packet filtering router.

9 + 3 = 12