B.TECH/AEIE/ECE/8TH SEM/INFO 4281/2018

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

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

(iii) ..... algorithm produces 128 bit hash value.
(a) MD5 (b) SHA (c) All of these (d) None of these.

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

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

(vi) ..... cipher facilitate one to many substitution.
(a) Polyalphabetic (b) Polygram
(c) Homophonic (d) Monoalphabetic.

(vii) ..... mode can be used for transmitting long messages.
(a) ECB (b) CBC
(c) None of these (d) All of these

(viii) ..... algorithm uses 16 rounds of encryption.
(a) IDEA (b) DES
(c) RSA (d) Both a and c

(ix) OSI position of ..... is between transport and application.
(a) IPSec (b) SSL (c) PGP (d) None of these.

(x) FAR and FRR are applicable with.....
(a) certificate authentication (b) biometric authentication
(c) fabrication (d) none of these.

Group – B

2. (a) What is product cipher? Differentiate between substitution and transposition technique.

(b) State the cipher text for the plain text "**17, Harinavi road, Kolkata-700142**" using Playfair substitution technique. Keyword to be used is **NETWORK CRYPTANALYSIS.**

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

(1 + 2) + 6 + 3=12

3. (a) State the cipher text for the plain text "***fundamentals of cryptology***" using Simple Columnar Transposition technique for 4 rounds. Keys for first round: (3,2,1), second round :(3,1,2),third round:(2,1,3) and fourth round:(1,2,3)
(*Step detailing and diagrams are mandatory for above problems.*)

(b) State the cipher text for the plain text "***fundamentals of cryptography***" using Caesar cipher technique with key=11

(c) Differentiate between brute force attack and cryptanalysis.

(d) Explain the concept of digital envelope.

4+ 2+ 2 + 4 =12

Group – C

4.(a) Explain the following algorithm modes with a neat diagram: cipher block chaining mode.

(b) Differentiate between block cipher and stream cipher.

(c) State the concept of Triple DES with a neat sketch.

(d) Diagrammatically show the working of Diffie-Hellman key exchange algorithm.

3+ 2+ 3+ 4 =12

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

(b) Discuss single round encryption of IDEA algorithm in detail, including output transformation round.

4 + 8 =12

Group – D

6. (a) Calculate public key and private key for p=7 and q=11 using RSA algorithm.

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

   (c) State the properties of digital signature.

   (d) State the features of authentication token.

3+ 4+ 3+ 2=12

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

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

6 + 6 = 12

Group – E

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

   (b) Draw and explain SSL protocol stack.

(3+5) + 4 = 12

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

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

(3 +3) + 6= 12