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

(ii) _____uses stream cipher.
(a) Hill (b) Rail fence
(c) Polygram (d) Playfair

(iii) _____rounds do not require key shifting in IDEA
(a) 2 and3 (b) 5 and 1
(c) 4and 8 (d) 1, 4 and 8

(iv) _____ rounds do not require key shifting in IDEA
(a) 2 and3 (b) 5 and 1
(c) 4and 8 (d) 1, 4 and 8

(v) Mathematical attack is applicable in _____
(a) RSA (b) DES
(c) MD2 (d) All of these.

(vi) _____ is susceptible to Bucket Brigade attack.
(a) Diffie-Hellman (b) Double DES
(c) Both(a) and (b) (d) None of These

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

(viii) _____ algorithm uses 8 rounds of encryption.
(a) IDEA (b) DES
(c) RSA (d) Both a and c

(ix) _____ mode cannot be used for transmitting long messages.

(a) ECB (b) CBC
(c) None of these (d) All of these

(x) _____ cipher facilitate one to many substitution

(a) Polyalphabetic (b) Polygram
(c) Homophonic (d) Monoalphabetic

Group – B

2. (a) State the cipher text for the plain text "***cryptography and cryptology***" using the following techniques:
   (i) Playfair cipher technique with keyword= **NETWORK SECURITY**
   (ii) Simple Columnar Transposition technique up to 3 rounds with keys for First round (4,2,1,3) Second round (3,4,2,1) and Third round(2,3,1,4) (*Step detailing and diagram mandatory for above problem.*)

   (b) State the cipher text for the plain text "***cryptography and cryptanalysis***" using (i) Caesar cipher technique with key=5 and (ii) Rail Fence technique.

(4 + 4) + 4 = 12

3. (a) State the cipher text for the plain text "***CRYPTOLOGY SECURITY***" using one time pad technique. key to be used is
" **BARCEKAPERALAZERON**".

   (b) State the cipher text for the plain text "**12, Garia avenue, Kolkata-700132**" using Playfair substitution technique. Keyword to be used is **NETWORK ANALYSIS**

   (c) Differentiate between Private key cryptography and Public key cryptography.

3 + 5 + 4 = 12

Group – C

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

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

   (c) State the concept of Double DES with a neat sketch. Explain Meet in the Middle attack.

(2 + 3) + 3 + (2 + 2) = 12

5. (a) Explain Bucket Brigade attack with attached numerical parameters [n=11, g=7; x for sender=3; y for receiver=9 and x=8, y=6 for attacker].

   (b) Explain in detail, Key shifting process of IDEA encryption algorithm from round 1 to round 6.

6 + 6 = 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 the attacks on RSA algorithm and discuss its countermeasures.

(3 + 3) + 6 = 12

7. (a) What is Biometric authentication? Differentiate between FAR and FRR.

   (b) Explain Certificate based authentication token.

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

(2 + 2) + 2 + 6 = 12

Group – E

8. (a) What is Screened subnet Firewall? Explain different types of firewall with neat diagrams.

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

(2 + 5) + 5 = 12

9. (a) Explain with neat sketch, the working of Alert protocol in SSL. State the limitations of Firewall.

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

   (c) Draw and explain SSL protocol stack. State the characteristics of firewall.

(3 + 3) + 3 + 3 = 12

Department & Section	Submission Link
ECE	https://classroom.google.com/c/Mjk4NjI3NTcwNjQ4/a/MzYwMTYxNDk5NjQ4/details