PRINCIPLES OF CRYPTOGRAPHY
(INF3121)

Time Allotted : 2½ hrs **Full Marks : 60**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A

1. Answer any twelve: **12 × 1 = 12**

Choose the correct alternative for the following

(i) Which principle of security ensures secrecy between sender and receiver?
(a) Confidentiality (b) Modification
(c) Authentication (d) All of the above

(ii) Which of the following is a substitution cipher?
(a) Caesar Cipher (b) Mono-Alphabetic Cipher
(c) Both (a) and (b) (d) None of these

(iii) What is a combination of Cryptography and Cryptanalysis?
(a) Linear Cryptanalysis (b) Differential Cryptanalysis
(c) Cryptology (d) None of the above

(iv) Which algorithm is susceptible to Man in the Middle attack?
(a) Double DES (b) Triple DES
(c) Diffie-Hellman Key Exchange algorithm (d) None of the above

(v) Which rounds require key shifting in IDEA?
(a) 4 and 8 (b) 1, 4 and 8
(c) 2, 3, 5, 6, 7 and Output transformation round (d) All of the above

(vi) Brute-Force attack is applicable in which of the following algorithm?
(a) RSA (b) DES
(c) MD2 (d) Both (a) and (b)

(vii) Which algorithm produces 128-bit hash value?
(a) MD5 (b) SHA1
(c) Both (a) and (b) (d) None of the above

(viii) Which are the optional components of Authentication Token?
(a) Real time clock and Keypad (b) LCD display, Processor and Battery
(c) LCD display and Battery (d) None of these

(ix) If the first byte of Alert message in SSL has value 1, what does it indicate?
(a) Fatal Error (b) Warning
(c) Both of the above (d) None of the above

(x) Which firewall suffers from Source routing attack?
(a) Application level Gateway (b) Packet Filter router
(c) Circuit level gateway (d) None of above

Fill in the blanks with the correct word

(xi) Handshake protocol in SSL has _____ phases.

(xii) Key size of Triple DES is _____bits

(xiii) When two different message digests have the same value, it is called as _____

(xiv) A person who attempts to break cryptography solutions is called _____.

(xv) If RC5 encryption algorithm uses 12 rounds, it generates _____ sub keys.

Group - B

2. (a) Construct a vigenere table for polyalphabetic substitution technique. Using the table develop the cipher text for plain text **"network cryptology"**. Key to be used is **transposition.** *[(CO2) (Create/HOCQ)]*
(b) Develop the cipher text for the plain text "***CYBER SECURITY***" using one time pad technique. Key to be used is "**CELTPERALASKA**". *[(CO2) (Create/HOCQ)]*
(c) Differentiate between Phishing and Replay attack. *[(CO1) (Analyze/IOCQ)]*
(3 + 3) + 4 + 2 = 12

3. (a) State the cipher text for the plain text "**15, Bantala Road, Kolkata-700059**" using Playfair Substitution technique. Keyword to be used is **CYBER ANALYSIS.**
State the cipher text for the plain text "***principles of security***" using (i) Caesar cipher technique with key=5 and (ii) Rail Fence technique. *[(CO2) (Evaluate/HOCQ)]*
(b) Differentiate between IP Spoofing and Packet sniffing. *[(CO1) (Analyze/IOCQ)]*
(6 + 4) + 2 = 12

Group - C

4. (a) Differentiate between Confusion and Diffusion. Explain Meet in the Middle attack. *[(CO3) (Analyze/IOCQ) (CO3) (Understand/LOCQ)]*
(b) Discuss Single round encryption of IDEA algorithm in detail including Output transformation round. *[(CO3) (Understand/LOCQ)]*
(2 + 2) + 8 = 12

5. (a) Alice and Bob want to establish a secret key using the Diffie-Hellman Key exchange algorithm. Assuming the values as n=11, g=5, x=3 and y=4, find out the values of A, B, K1 and K2. *[(CO3)(Apply/IOCQ)]*

(b)

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

From the above S-Box, calculate the output for the following inputs:
(i) 001101(ii) 110110 (iii) 010101. *[(CO3)(Analyze/IOCQ)]*

6 + 6 = 12

Group - D

6. (a) Explain RSA algorithm in detail. Solve and calculate public key and private key for p=5 and q=17 using RSA algorithm. *[(CO4)(Understand/LOCQ/Analyse/IOCQ)]*

   (b) Explain the working mechanism of Kerberos authentication protocol with neat diagram. *[(CO5)(Understand/LOCQ)]*

(2 + 4) + 6 = 12

7. (a) Differentiate between Message Authentication Code and Message Digest. Explain the working of HMAC algorithm in detail with neat diagram. *[(CO4)(Analyze/IOCQ/Understand/LOCQ)]*

   (b) Differentiate between Challenge-Response authentication token and Time based authentication token. *[(CO5)(Analyze/IOCQ)]*

(2 + 5) + 5 = 12

Group - E

8. (a) Explain three types of firewall configuration with neat diagrams. *[(CO6)(Understand/LOCQ)]*

   (b) Explain with neat sketch, the working mechanism of PEM mail security protocol. *[(CO6)(Understand/LOCQ)]*

6 + 6 = 12

9. (a) Explain the working of Handshake protocol in detail with neat diagrams. *[(CO6)(Understand/LOCQ)]*

   (b) Discuss the attacks possible on Packet Filtering router. *[(CO6)(Understand/LOCQ)]*

8 + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	44.79	28.12	27.08