CRYPTOGRAPHY & NETWORK SECURITY
(INFO 3201)

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 cipher facilitates one to one substitution?
(a) Caesar Cipher (b) Mono-Alphabetic Cipher
(c) Homophonic Cipher (d) All of above

(ii) An attack in availability is known as
(a) Fabrication (b) Modification
(c) Interruption (d) All of the above

(iii) If RC5 algorithm uses 14 rounds of encryption, how many sub keys will be generated?
(a) 14 (b) 28 (c) 30 (d) 42

(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 algorithm can use variable rounds of encryption?
(a) RC5 (b) IDEA (c) Triple DES (d) DES.

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

(vii) 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.

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

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

(x) What is the position of SSL in TCP/IP model?
(a) Between Transport and Application (b) Between Transport and Network
(c) Between Transport and Physical (d) None of the above.

Fill in the blanks with the correct word

(xi) An attack in authentication is called_____.

(xii) Key size of Triple DES is _____ bits.

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

(xiv) Handshake protocol in SSL has _____ phases.

(xv) _____ firewall architecture has at least three network interfaces.

Group - B

2. (a) Differentiate between Brute force attack and Cryptanalysis. *[(CO1)(Analyze/IOCQ)]*
(b) Develop the cipher text for the plain text "**22, Kalikapur Road, Kolkata-700137**" using Playfair substitution technique. Keyword to be used is **NETWORK CRYPTANALYSIS.** *[(CO2)(Evaluate/HOCQ)]*
(c) Develop the cipher text for the plain text "***theory of substitution***" using Simple Columnar Transposition technique for 4 rounds. Keys for First round (3, 2, 1, 4), Second round (4, 1, 3, 2), Third round (2, 1, 3, 4) and Fourth round (1, 2, 3, 4). reference architecture. *[(CO2)(Evaluate/HOCQ)]*

2 + 6 + 4 = 12

3. (a) Explain the principles of Network Security. Differentiate between IP Sniffing and DNS spoofing. *[(CO1)(Understand/LOCQ)(Analyze/IOCQ)]*
(b) Develop the cipher text for the plain text "***theory of transposition***" using (i) Caesar cipher technique with key= 5 and (ii) Rail Fence technique. *[(CO2)(Evaluate/HOCQ)]*

(6 + 2) + (2 + 2) = 12

Group - C

4. (a) Explain the following algorithm modes with neat diagram:
(i) Electronic Code book mode (ii) Cipher Block chaining mode
(iii) Cipher Feedback mode *[(CO3)(Understand/LOCQ)]*
(b) Differentiate between Block cipher and Stream cipher. *[(CO2)(Analyze/IOCQ)]*

(3 + 3 + 4) + 2 = 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=2 and y=3, find out the values of A, B, K1 and K2. *[(CO3)(Apply/IOCQ)]*

(b) From the S-Box, calculate the output for the following inputs:
(i) 111001(ii) 110111 (iii) 010111

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

[(CO3)(Analyze/IOCQ)]

6 + 6 = 12

Group - D

6. (a) Differentiate between Certificate based authentication and Biometric authentication. *[(CO5)(Analyze/IOCQ)]*

(b) Discuss three properties of Digital Signature. *[(CO4)(Understand/LOCQ)]*

(c) Discuss five requirements of Hash function. *[(CO4)(Understand/LOCQ)]*

4 + 3 + 5 = 12

7. (a) Discuss the requirements of Asymmetric key cryptography. Solve and calculate public key and private key for p=17 and q=11 using RSA algorithm.
[(CO2)(Understand/LOCQ/(CO3)Analyze/IOCQ)]

(b) Discuss the working of Challenge-Response authentication token.
[(CO5)(Understand/LOCQ)]

(3 + 4) + 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	48.96	36.46	14.58