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 algorithm suffer from Meet in the Middle attack?
(a) Double DES (b) Triple DES
(c) Diffie-Hellman Key Exchange Algorithm (d) SSL.

(ii) Which principle of security ensures non modification of data?
(a) Integrity (b) Authentication (c) Confidentiality (d) None of these.

(iii) Canonical conversion is related to which of the following?
(a) PEM (b) RSA (c) SSL (d) None of these.

(iv) Transformed key is used in which of the following?
(a) SSL (b) DES (c) HMAC (d) None of these.

(v) Which firewall architecture makes servers publicly available?
(a) DMZ (b) DES (c) DMQ (d) All of these.

(vi) Which encryption algorithm uses 16 rounds of encryption?
(a) One time pad cipher (b) DES
(c) IDEA (d) All of these.

(vii) Which encryption algorithm is suitable for smart card?
(a) DES (b) RSA (c) RC5 (d) All of these.

(viii) OSI position of what is in between transport and application?
(a) IPSec (b) SSL (c) All of these (d) None of these.

(ix) Which one is used to generate unique password in Authentication Token?
(a) Seed (b) Clock (c) Battery (d) None of these

(x) Which firewall configuration has 2 level of defence?
(a) Screened Host Firewall Single Homed Bastion
(b) Screened Subnet Firewall
(c) Screened Host Firewall Dual Homed Bastion
(d) None of these.

Fill in the blanks with the correct word

(xi) _____ uses Ticket Granting Server.

(xii) _____mode suffers from message stream modification attack.

(xiii) Alert protocol is a sub protocol of _____.

(xiv) _____ authentication makes use of FAR and FRR

(xv) Attack in Availability is called _____.

Group - B

2. (a) (i) State the cipher text for the plain text "**53, Christopher Road, Kolkata-700023**" using Playfair Substitution technique. Keyword to be used is **CRYPTOLOGY.**

(ii) State the cipher text for the plain text "***fundamentals of entropy***" using (i) Caesar cipher technique with key=9 and (ii) Rail Fence technique

(*Step detailing and diagram mandatory for above problems.*) *[(CO2)(Evaluate/HOCQ)]*

(b) Differentiate between Virus and Worm. *[(CO1)(Analyze/IOCQ)]*

(c) Differentiate between Logic Bomb and Pharming. *[(CO1)(Understand/LOCQ)(Analyze/IOCQ)]*

(5 + 3) + 2 + 2 = 12

3. (a) Construct a vigenere table for polyalphabetic substitution technique. Using the table develop the cipher text for plain text **"network analysis"**. Key to be used is **cryptolysis.** *[(CO2)(Create/HOCQ)]*

(b) Develop the cipher text for the plain text "***SEVERE CYCLONE"*** using one time pad technique. Key to be used is "**ACEKBPERALAFR**". *[(CO2)(Create/HOCQ)]*

(c) Differentiate between unconditionally secure and computationally secure encryption algorithms. *[(CO1)(Analyze/IOCQ)]*

(d) Develop the cipher text for the plain text "***fundamentals of cryptology***" using Simple ColumnarTransposition technique for 3 rounds. Keys for First round (3, 1, 5, 4, 2), Second round (1, 3, 2, 4, 5),Third round (2, 3, 1, 4, 5). *[(CO2)(Evaluate/HOCQ)]*

(*Step detailing and diagrams are mandatory for above problems.*)

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

Group - C

4. (a) Explain Single round encryption of DES algorithm in detail with neat diagram. *[(CO3)(Understand/LOCQ)]*

(b) Discuss Single round encryption of IDEA algorithm in detail. *[(CO3)(Understand/LOCQ)]*

(c) Differentiate between Algorithm types and Algorithm modes. *[(CO2)(Analyze/IOCQ)]*

5 + 5 + 2 = 12

5. (a) Explain RC5 sub key algorithm in detail with a neat diagram. *[(CO3)(Understand/LOCQ)]*

(b) Demonstrate Man in the Middle attack with the following numerical parameters: [n=11, g=7; x for sender=5; y for receiver=7 and x=4, y=6 for attacker]. *[(CO3)(Apply/IOCQ)]*

(c) Illustrate Key Shifting mechanism in IDEA encryption algorithm from First round to Fourth round. *[(CO3)(Evaluate/HOCQ)]*

4 + 4 + 4 = 12

Group - D

6. (a) Explain RSA algorithm in detail. Solve and calculate public key and private key for p=17 and q=7 using RSA algorithm. *[(CO3)(Understand/LOCQ)][(CO3)(Apply/IOCQ)]*

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

(3 + 3) + 6 = 12

7. (a) Differentiate between MAC and Message Digest. Explain the working of Biometric authentication in detail. *[(CO4)(Analyze/IOCQ)(CO5) (Understand/LOCQ)]*

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

(c) Discuss the properties of Digital Signature. *[(CO4)(Understand/LOCQ)]*

(3 + 3) + 3 + 3 = 12

Group - E

8. (a) Consider the 24 bit binary stream, [100111001010110001110101]. Deduce the hexadecimal printable characters from the above binary stream using Base 64 encoding technique. *[(CO6)(Evaluate/HOCQ)]*

(b) Differentiate the workings of PGP & PEM mail security protocols. *[(CO6)(Understand/LOCQ)]*

6 + 6 = 12

9. (a) Explain with neat sketch, the working mechanism of Handshake protocol in SSL. *[(CO6)(Understand/LOCQ)]*

(b) Differentiate between Screened host firewall single homed bastion and Screened subnet firewall with neat diagrams. *[(CO6)(Analyze/IOCQ)]*

(c) Discuss the working mechanism of Alert protocol. *[(CO6)(Understand/LOCQ)]*

6 + 3 + 3 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	45.83	25	29.17

Course Outcome (CO):

After the completion of the course students will be able to

1. Define the concepts of Network security. Classify different types of attack on Network security. Recall the principles of security.
2. Classify different kinds of Substitution techniques and Transposition techniques and illustrate the concepts of Symmetric key cryptography and Asymmetric key cryptography.

3. Discuss in detail DES, RSA, IDEA and RC5 algorithm. Solve numerical based on DES and RSA algorithms. Explain Diffie-Hellman Key exchange algorithm and Digital Envelope.
4. Compare MAC, Message Digest and Hash function. Analyze MD5 Message Digest algorithm and HMAC algorithm. Illustrate Digital Signature.
5. Explain Authentication token and Classify between different types of Authentication tokens. Compare Certificate based authentication and Biometric Authentication. Explain Kerberos Authentication protocol.
6. Analyze the concept of SSL, PGP and PEM. Explain VPN. Explain the concepts of Firewall and DMZ Network. Compare between Packet filtering router, Application-level gateway and Circuit-level gateway. Classify between different Firewall Configurations.

**LOCQ: Lower Order Cognitive Question; IOCQ: Intermediate Order Cognitive Question; HOCQ: Higher Order Cognitive Question.*