CRYPTOGRAPHY & NETWORK SECURITY
(CSEN 4132)

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) Use Caesar's Cipher to decipher the following
HQFUBSWHG WHAW
(a) ABANDONED LOCK (b) ENCRYPTED TEXT
(c) ABANDONED TEXT (d) ENCRYPTED LOCK.

(ii) When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called
(a) DNS lookup (b) DNS hijacking
(c) DNS spoofing (d) none of the mentioned.

(iii) Public key encryption is advantageous over Symmetric key Cryptography due to
(a) speed (b) space (c) key exchange (d) key length.

(iv) In the DES algorithm the round key is _________ bit and the Round Input is __________ bits.
(a) 48, 32 (b) 64,32 (c) 56, 24 (d) 32, 32.

(v) The minimum positive integer p such that 3^p modulo 17 = 1 is
(a) 5 (b) 8 (c) 12 (d) 16.

(vi) For a network with N nodes, how many master keys are present?
(a) N(N-1)/2 (b) N (c) N(N+1)/2 (d) N/2.

(vii) In RSA, Φ(n) = ______ in terms of p and q.
(a) (p)/(q) (b) (p)(q) (c) (p-1)(q-1) (d) (p+1)(q+1)

(viii) Which of the following is false for ECB mode of operation?
(i) The Plain text is broken into blocks of size 128 bytes
(ii) Blocks can be swapped, repeated, replaced without recipient noticing
(iii) Good for short data

(iv) Encryption of each block is done separately using a randomly generated key for each block

(a) (i) only
(b) (ii) and (iii)
(c) (i) and (iv)
(d) (i) (ii) and (iv).

(ix) What is the key size allowed in PGP?

(a) 1024-1056
(b) 1024-4056
(c) 1024-4096
(d) 1024-2048.

(x) For an n-bit tag and a k-bit key, the level of effort required for brute force attack on a MAC algorithm is

(a) 2^k (b) 2^n (c) min(2^k,2^n) (d)2^n/2^k.

Group – B

2. (a) Find X for the given set of congruent equations X≡2 mod 3, X≡3 mod 5 and X≡2 mod 7. What is the "chosen cipher text" attack? [(CO1,CO2)(Evaluate/HOCQ)]

(b) Encrypt the message "GOODMORNING" with Playfair cipher with keyword "ROUNDTABLE". [(CO1)(Evaluate/HOCQ)]

(4 + 2) + 6 = 12

3. (a) What would be the transformation of a message 'We the people of India' using Rail Fence technique ? [(CO3) (Remember/IOCQ)]

(b) Explain Eavesdropping and SYN Flood attack with respect to Denial of Service attack. Find the plain text corresponding to cipher text "BPKYFS" where playfair cipher is used with keyword as "SECRET" (assuming j is combined with i)? List the rules. [(CO1) (Understand/HOCQ)]

3 + (3 + 6) = 12

Group – C

4. (a) Given p=19, q=23, and e=3 Use RSA algorithm to find n, ϕ(n) and d. [(CO2, CO4)(Evaluate/HOCQ)]

(b) Discuss how different cryptographic algorithms use Fiestel Cipher Structure. How many S boxes are there in AES? How S-box is calculated.
[(CO4) (Explain/LOCQ)]

5 + (3 + 2 + 2) = 12

5. (a) Users A and B use the Diffie Hellman key exchange technique, a common prime q = 11 and a primitive root alpha=7. What is the shared secret key? How man in middle attack can be performed in Diffie Hellman algorithm.
[(CO3, CO4)(Evaluate/HOCQ)]

(b) Describe about IDEA encryption. How is key expansion done in Blowfish?
[(CO4) (Analyze/ IOCQ)]

(3 + 3) + (4 + 2) = 12

Group – D

6. (a) Define MAC. Compare MD5 with SHA-1. [(CO5) (Remember/LOCQ)]
   (b) Briefly discuss the operation of Kerberos authentication protocol with suitable Diagram. [(CO5) (Remember/HOCQ)]

(2 + 4) + 6 = 12

7. (a) Discuss about X.509 authentication service in detail.[(CO5)(Understand /IOCQ)]
   (b) Explain HMAC algorithm with suitable diagram. [(CO5) (Understand/LOCQ)]

6 + 6 = 12

Group – E

8. (a) How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components PGP. [(CO6) (Learn/IOCQ)]
   (b) Differentiate transport and tunnel modes of operation of IPsec.
   [(CO6) (Remember /IOCQ)]

(2 + 6) + 4 = 12

9. (a) What protocols comprise SSL? What is the difference between an SSL connection and an SSL session? [(CO6) (Compare/LOCQ)]
   (b) Explain Encapsulating IP Security Payload. What are the steps involved in PGP message generation? [(CO6) (Understand/LOCQ)]

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

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	31.25%	31.25%	37.5%

Course Outcome (CO):

After the completion of the course students will be able to

CO1: Learn the various types of attacks and their characteristics.

CO2: Learn the basics of number theory to understand the mathematical background of cryptography.

CO3: Understand the basic concept of encryption and decryption for secure data transmission.

CO4: Analyze and compare various cryptography techniques.

CO5: Understand the concept of digital signature and its applications.

CO6: Learn the basic principle of network security designs using available secure solutions (such as PGP, SSL, IPSec, etc)

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

Department & Section	**Submission link:**
CSE A+B(gr 1)	https://classroom.google.com/c/NDAxNDgyMDQ2MjU5/a/NDY0MTkzOTExOTE1/detail
CSE B(group 2)+C	https://classroom.google.com/c/Mzk3Nzc4NzAzMzU4/a/NDU4NzM3NzUyNzk1/details