CRYPTOGRAPHY & NETWORK SECURITY
(CSEN 4132)

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

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and <u>any 4 (four)</u> from Group B to E, taking <u>one</u> 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) On Encrypting "thepepsiisintherefrigerator" using Vignere Cipher System using the keyword "HUMOR" we get cipher text
(a) abqdnwewuwjphfvrrtrfzn sdokvl
(b) abqdvmwuwjphfvvyyrf znydokvl
(c) tbqyrvmwuwjphfvvyy rfznydokvl
(d) baiuvmwuwjphfoeiyrf znydokvldependency

(ii) What is Advanced Encryption Standard (AES)?
(a) Block Cipher (b) Stream Cipher
(c) Bit Cipher (d) None of (a), (b) & (c).

(iii) The 4×4 byte matrices in the AES algorithm are called
(a) States (b) Words (c) Transitions (d) Permutations.

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

(v) On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text
(a) nlazeiibljji (b) nlazeiibljii
(c)olaaeiibljki (d) mlaaeiibljk.

(vi) What is the key size allowed in PGP?
(a) 1024-1056 (b) 1024-4056
(c) 1024-4096 (d) 1024-2048.

(vii) The process to discover plain text or key is known as
(a) Cryptanalysis (b) Cryptodesign
(c) Cryptoprocess (d) Cryptographic.

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

(ix) What will be the value of Ø(27)=

(a) 6 (b) 12 (c) 26 (d) 18.

(x) In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is P + Q if P = (0,-4) and Q = (1, 0)?

(a) (15,-56) (b) (-23,-43)

(c) (69,26) (d) (12, -86).

Fill in the blanks with the correct word

(xi) SHA-1 produces a hash value of ___________ bits.

(xii) In the DES algorithm the round key is _________ bit and the Round Input is ___________bits.

(xiii) AES uses a ___________ bit block size and a key size of _________ bits.

(xiv) The value of 3^{201} mod 11 is _________.

(xv) In AES the 4×4 bytes matrix key is transformed into a keys of size _________.

Group - B

2. (a) Evaluate 3^{21} mod 11 using Fermat's little theorem. *[(CO2)(Understand/LOCQ)]*

(b) State the encryption process of Playfair Cipher. Encrypt the word "COMSEC means communications security." with the keyword "GALOIS". *[(CO2,CO5)(Apply/IOCQ)]*

3 + (3 + 6) = 12

3. (a) Define Spoofing and Pharming. *[(CO1,CO3)(Understand/LOCQ)]*

(b) Some intruder intercepted the cipher Text as "UVACLYFZLJBYL". Assuming it is to be modified Caeser Cipher; break it. What is the Plain text and what is the value of K? *[(CO4)(Analyze/HOCQ)]*

(c) Find out the quadratic residue of mod 11. *[(CO2)(Apply/IOCQ)]*

(2 + 2) + 4 + 4 = 12

Group - C

4. (a) In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? Explain man in the middle attack with suitable example. *[(CO3)(Analyse/HOCQ)]*

(b) Explain the steps of the AES Algorithm with suitable diagram. *[(CO4)(Remember/LOCQ)]*

(3 + 4) + 5 = 12

5. (a) In an RSA cryptosystem, a particular A uses two prime numbers, 13 and 17, to generate the public and private keys. If the public of A is 35, then find the private key of A. *[(CO3)(Analyse/HOCQ)]*

(b) List out the attacks to RSA. *[(CO2)(Remember/LOCQ)]*

(c) What are the design parameters of Feistel cipher network? *[(CO3)(Analyze/IOCQ)]*

6 + 3 + 3 = 12

Group - D

6. (a) Define MAC. Compare MD5 with SHA-1 with operational example. *[(CO3,CO4)(Analyse/IOCQ)]*

(b) Explain HMAC algorithm with suitable diagram. *[(CO4)(Remember/LOCQ)]*

(2 + 4) + 6 = 12

7. (a) Describe the role of Ticket Granting Ticket and service granting Ticket in Kerberos. *[(CO5)(Analyse/HOCQ)]*

(b) Describe SHA-1 algorithm in detail. *[(CO4)(Remember/LOCQ)]*

(c) Differentiate MAC and Hash function? *[(CO3)(Analyze/IOCQ)]*

4 + 6 + 2 = 12

Group - E

8. (a) Explain the working of IPSec. *[(CO5)(Understand/LOCQ)]*

(b) State the limitations of a firewall. *[(CO6)(Remember/LOCQ)]*

(c) Explain Encapsulating IP Security Payload. *[(CO5,CO6)(Understand/IOCQ)]*

6 + 3 + 3 = 12

9. (a) List the different protocols of SSL. Explain in detail Handshake protocol. Tell how does the server get authenticated to client in SSL? *[(CO3,CO6)(Analyse/HOCQ)]*

(b) Differentiate transport and tunnel modes of operation of IPsec. *[(CO5)(Remember/LOCQ)]*

(2 + 3 + 3) + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	41.66	28.12	30.20

Course Outcome (CO):

After the completion of the course students will be able to

CSEN4132:1: Understand the concepts of Cryptography and Network Security including Private and Public key cryptography and various protocols to protect computing system against potential threats.

CSEN4132:2: Explore Mathematical techniques for supporting the cryptographic mechanisms.

CSEN4132:3: Analyze and compare various cryptographic techniques.

CSEN4132:4: Evaluate security mechanisms using rigorous approaches by key ciphers, message authentication and Hash functions.

CSEN4132:5: Investigate various network security applications, IPSec, Firewall, IDS, Web Security, Email Security and Malicious software etc.

CSEN4132:6: Design a secure network after analysing the vulnerabilities in any computing system.

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