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) _____mode cannot be used for transmitting long messages.
(a) ECB (b) OFB (c) CBC (d) All of these

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

(iii) The multiplicative Inverse of 1234 mod 4321 is
(a) 3239 (b) 3213 (c) 3242 (d) Does not exist

(iv) Is $x^3 + x^2 + 1$ reducible over GF(2)?
(a) Yes (b) No (c) Can't Say (d) Insufficient Data.

(v) Find the 8-bit word related to the polynomial $x^6 + x + 1$
(a) 01000011 (b) 01000110 (c) 10100110 (d) 11001010

(vi) IP Sec services are available in _____ layer
(a) Application (b) Data Link (c) Network (d) Transport

(vii) In RSA, $\Phi(n)$ = _____ in terms of p and q, where n = pq
(a) (p)/(q) (b) (p)(q) (c) (p-1)(q-1) (d) (p+1)(q+1)

(viii) What is the number of round computation steps in the SHA-256 algorithm?
(a) 80 (b) 76 (c) 64 (d) 70.

(ix) The man-in-the-middle attack can endanger the security of the Diffie-Hellman if two parties are not
(a) authenticated (b) joined
(c) submit (d) separate

(x) _____ prevents either sender or receiver from denying a transmitted message.
(a) Access control (b) Non-repudiation
(c) Masquerade (d) Integrity

Group- B

2. (a) Find X for the given set of congruent equations $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$. Explain Eavesdropping and SYN Flood attack with respect to Denial of Service attack? [(CO1,CO2)(Evaluate/HOCQ)]
   (b) Define Pharming. [(CO3) (Understand/LOCQ)]
   (c) Encrypt the message "OBSTACLE" with Playfair cipher with keyword "ROUNDTABLE". [(CO1, CO4)(Evaluate/HOCQ)]
   (4 + 2) + 2 + 4 = 12

3. (a) Compare symmetric and asymmetric key cryptography algorithms? [(CO3)(Analyze/IOCQ)]
   (b) Evaluate gcd(1547,560) using Euclid's algorithm. Define Euler's totient function and its application. [(CO2,CO5)(Apply/IOCQ)]
   (c) Using Fermat's theorem find the value of $5^{158} \bmod 11$? [(CO2)(Learn/LOCQ)]
   4 + 6 + 2 = 12

Group - C

4. (a) Given p=17, q=11, and e=7 Use RSA algorithm to find n, $\phi(n)$, d, Public and Private Key. [(CO2, CO4)(Evaluate/HOCQ)]
   (b) What are the limitations of Electronic Code Book? How many S boxes are there in AES? How is S-box calculated? [(CO3, CO4)(Explain/LOCQ)]
   6 + (2 + 2 + 2) = 12

5. (a) Draw and illustrate the steps involved in the encryption and decryption of the Cipher block chaining (CBC) mode of DES. [(CO1)(Remember/LOCQ)]
   (b) Explain the Key Generation Process of DES with suitable diagram. [(CO3)(Analyze/IOCQ)]
   6 + 6 = 12

Group - D

6. (a) Explain HMAC algorithm with suitable diagram. [(CO4)(Remember/LOCQ)]
   (b) How does "Birthday Attack" work? Explain MD5 single round operation. [(CO1, CO5)(Analyze/IOCQ)]
   6 + (2 + 4) = 12

7. (a) Explain the MD5 algorithm with suitable diagram. How is it different from SHA-1? [(CO4)(Analyze/HOCQ)]
   (b) Explain the role of the Authentication Server (AS), and the Ticket Granting Server (TGS) in Kerberos. [(CO3, CO6)(Apply/HOCQ)]
   (3 + 3) + (3 + 3) = 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 of PGP. [(CO5, CO6)(Understand/IOCQ)]
   (b) Explain about IPSec architecture. [(CO5, CO6)(Understand/LOCQ)]
   (2 + 6) + 4 = 12

9. (a) What are different types of firewalls? Briefly explain the working principle of each. [(CO1)(Remember/LOCQ)]
   (b) Briefly explain the Handshake Protocol of SSL. [(CO5)(Analyze/IOCQ)]
   (2 + 4) + 6 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	33.33	37.5	29.17

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