

(c) Write short notes on :

- (i) Method to obtain consistent set of checkpoints
- (ii) Domino effect.

5. Attempt any **two** questions :

- (a) Discuss the optimistic methods for distributed concurrency control. What are the different validations conditions for optimistic concurrency control ? Explain it.
- (b) How will you execute the transaction when data is replicated among several sites and data consistency is highest criteria ? Also discuss the case when data availability is highest criteria.
- (c) Write short notes on :
 - (i) Flat and nested transaction
 - (ii) 2PL and strict 2 PL.

(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 2757

Roll No.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

B. Tech.

(SEM.VII) THEORY EXAMINATION 2011-12.

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours

Total Marks : 100

Note :- (1) Attempt **all** questions.

(2) All questions carry equal marks.

(3) Notations/Symbols/Abbreviations used have usual meaning.

(4) Make suitable assumptions, wherever required.

1. Attempt any **four** parts of the following :

(a) Explain the following terms :

(i) Message Integrity

(ii) Denial of Service

(iii) Passive Attack

(iv) Fiestal Cipher

(v) Steganography.

(b) Define the Hill Cipher. Show the encryption of plaintext **ME** using the Hill Cipher with the key matrix **K** defined by the following elements :

$$K_{11} = 9, K_{12} = 4, K_{21} = 5, K_{22} = 7$$

Further show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

- (c) Draw a block level diagram to depict the structure of one round of DES. Prove that if plaintext block and encryption key are complemented then resulting ciphertext block of DES encryption is also complemented.
- (d) Describe the encryption and decryption process of a block cipher in Cipher Feedback (CFB) mode.
- (e) Describe the Man-in-the-Middle attack on Double DES.
- (f) What is permutation cipher? Whether permutation ciphers are susceptible to the statistical analysis or not? Discuss. Encryption key in a permutation cipher is (3, 7, 2, 6, 1, 8, 5, 4). Find the decryption key.

2. Attempt any **four** parts of the following :

- (a) Describe RSA algorithm. Whether RSA encryption and decryption works or not if message m has common factor with the modulus n of the scheme. Justify your answer.
- (b) Define Group. Give an example of group which is not a Field. Let G be finite group of order n with generator a . Prove that a^m is also generator of G if m is relatively prime to n .
- (c) Give a comparison of AES Cipher to the DES cipher. Show that (x^3+x+1) is the inverse of (x^2+1) in $GF(2^4)$ modulo (x^4+x+1) .
- (d) State Chinese Remainder theorem. Use it to solve the following simultaneous congruences :

$$x \equiv 4 \pmod{7}, x \equiv 4 \pmod{13}, x \equiv 0 \pmod{12}$$

- (e) State and prove Fermat's theorem. Determine the value of $3^{2005} \pmod{500}$.
- (f) Apply Miller-Rabin Algorithm using base 2 to test whether the number 341 is composite or not.

3. Attempt any **two** parts of the following :

- (a) What is message authentication code? How it differs from hash function? What are the requirements of a message authentication code? Suggest at least one scheme to show that symmetric encryption algorithm can also be used to generate message authentication code.
- (b) Compare and contrast a conventional ink based signature and a digital signature. Describe the Elgamal scheme of digital signature generation and verification. Why do signatures of the same message, signed on different occasions, differ?
- (c) Consider a hash function H that creates n -bit message digest. H is applied to k random inputs to create digests. Derive the value of k for which the probability of at least one duplicate (i.e. $H(x) = H(y)$ for some distinct x, y) is more than 0.5.

4. Attempt any **two** parts of the following :

- (a) Diffie-Hellman Key exchange algorithm is vulnerable to Man-in-the-Middle Attack. How? Users A and B use a Diffie-Hellman key exchange protocol with a chosen common prime $p = 23$ and a primitive root $g = 7$. Given that private keys of A and B are 3 and 5 respectively. Determine the public keys of A and B. Further determine the shared secret key K .