Printed Pages : 1 **Roll No.** | | | | | | | | | | | **CS -271**

M.TECH. (SEM–II)

CARRY OVER EXAMINATION 2016-17

CRYPTOGRAPHY

Time : 3 Hours ***Max. Marks : 100***

Note : *Be precise in your answer. In case of numerical problem assume data wherever not provided.*

1. Attempt any Four parts of the following: **4 × 5 = 20**

(a) What is a prime number? And what is the meaning of the expression divides?

(b) What is Euler's totient function with suitable example?

(c) The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality?

(d) What is the difference between an index and a discrete logarithm?

(e) What is a primitive root of a number with suitable example?

(f) Consider the function: $f(n)$ = number of elements in the set $\{a : 0 \le a < n and \gcd(a, n) = 1\}$. What is this function?

2. Attempt any Two parts of the following: **2 × 10 = 20**

(a) What are three broad categories of applications of public-key cryptosystems? And give Elliptic Curve based Diffie-Hellman key exchange algorithm.

(b) Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for $p = 17, q = 11, e = 7, m = 88$. And Compute $3^{201} \bmod 11$: what is the minimum number of the multiplication-required for this computation?

(c) Explain the problems with key management and how it affects symmetric cryptography. What are the requirements for the use of a public-key certificate scheme?

3. Attempt any Two parts of the following: **2 × 10 = 20**

(a) Why the middle portion of triple DES in a decryption rather than encryption? Discuss the strength of DES algorithm and also explain the substitution method in including the P-Box?

(b) Describe at least two modes of operation of block cipher. What is the most security-critical component of DES round function? Give a brief description of this function.

(c) Explain the concept of differential cryptanalysis of DES with example. Also describe the RC4.

4. Attempt any Two parts of the following: **2 × 10 = 20**

(a) Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same K (secret per message) is used to sign two different message using DSA?

(b) What are the requirements of a Message Authentication Code (MAC)? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.

(c) What is hash function? List the requirements of a hash function? In what ways, can a hash value be secured to provide message authentication?

5. Attempt any Two parts of the following: **2 × 10 = 20**

(a) What is Finite Automata with example? Explain the structure of ciphers.

(b) Explain the selection of function Ma, h and d function with suitable example.

(c) Discuss the advantage of cipher design using automata with example.