Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
A Constituent Institution of Manipal University

1st SEMESTER M.TECH. (COMPUTER SCIENCE & INFORMATION SECURITY)

END SEMESTER EXAMINATIONS, Nov 2017

SUBJECT: Number Theory and Cryptography (CSE 5121)

REVISED CREDIT SYSTEM

(23/11/2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1A. State and prove Euler's theorem. **4M**

1B. State the Chinese remainder theorem and find the value of x for the following set of congruences: **4M**

$x \equiv 5 \pmod 7$
$x \equiv 3 \pmod{11}$
$x \equiv 10 \pmod{13}$

Ensure the validation of the value of x.

1C. Using Vigenère cipher, decrypt the word "OWYNCBPF" using "log" as the key. **2M**

2A. Explain the two types of transposition techniques. Give a suitable example for each to illustrate both encryption as well as decryption. **4M**

2B. Draw neat diagrams and explain the output feedback mode of block cipher for encryption and decryption. **3M**

2C. Explain one round of DES algorithm with a neat diagram. **3M**

3A. Define the terms a group and a cyclic sub group of algebraic structures. In GF (2^8), find the inverse of (x^5) modulo ($x^8+ x^4 + x^3+x+1$). **3M**

3B. Distinguish between symmetric and asymmetric cryptosystem. Consider n=17*11, using RSA algorithm find public and private keys, cipher text and decrypt the message. Given plain text M=88 and let e=7. **3M**

3C. What do you mean by an elliptic curve? Write the procedure to find the points on the elliptic curve. What do you mean by hash function mention any two applications of hash functions. **4M**

4A. Draw a neat diagram and explain pseudorandom number generation using triple DES. **3M**

4B. What is Public Key Cryptography? What are its advantages and disadvantages? What are the important properties of DH key exchange? **4M**

4C. Write Blum-Blum-Shub Pseudorandom Bit Generators algorithm. Write the encryption and decryption procedure of RC4 public-key bit stream cryptosystem. **3M**

5A. Write the requirements of cryptographic hash function and illustrate the birth day problem in cryptographic hash function. Write the block diagram of SHA-512. How is the hash buffer initialized in SHA-512? **4M**

5B. 5B.Write the structure/model of the following. **4M**
(i)HMAC
(ii) General Digital Signature model

5C. With the help of the diagrams distinguish between DSS and RSA Signature approaches. **2M**