Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

VI SEMESTER B.TECH. (COMPUTER SCIENCE & ENGINEERING) DEGREE MAKEUP EXAMINATION-JUNE 2018
SUBJECT: PRINCIPLES OF CRYPTOGRAPHY (CSE 4015)
REVISED CREDIT SYSTEM
(22/06/2018)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Explain the security goals. Which types of security attacks cause a threat to integrity? Explain. 4M

1B. Explain the working of Hill Cipher. Use an autokey system to decrypt the message "ZICVTWQNGKZEIIG", given the key as "deceptive". 4M

1C. Use a double transposition cipher with the key 1357246 and encrypt the message "MISSION FAILED COVER YOURSELF". 2M

2A. Draw a neat diagram and explain the single round of DES algorithm. What security attacks are possible on DES algorithm? 5M

2B. Draw neat diagrams and describe counter mode of encryption and decryption of a block cipher. Explain its advantages. 5M

3A. Find the following: 3M

i) 5^{-1} mod 23(Using extended Euclid algorithm)

ii) φ(256) (Using Euler's Totient function)

iii) 5^{301}mod 11 (Using Fermat theorem)

3B. State Euler's theorem. Use Chinese remainder theorem to find Z, given 3M
Z=X-2 and X ≡ 1mod 2,
X ≡ 0 mod 3, X ≡ 4 mod 5.

3C. What is avalanche effect? Explain the construction of S-box and inverse S-box of AES. Comment on the number of rounds and key sizes in AES. 4M

4A. Explain the three tests of randomness. Generate a sequence of random numbers using Linear Congruential Generator in which a=5, c=0, x_0=1, and m=32. Is this design generating a full period? 4M

4B. Briefly explain the different types of attacks on RSA algorithm. 4M

4C. Consider a Diffie-Hellman scheme with a common prime q=13, and a primitive root α=7. 2M

i) If Bob has a public key Y_B=12, what is his private key X_B?

ii) What is the shared secret key, given Alice public key of 5?

5A. Explain two simple hash functions. What are preimage resistant and second preimage resistant properties? 3M

5B. Draw a neat diagram and explain SHA-512 processing of a single 1024-bit block of message. 4M

5C. Draw a neat diagram and explain the use of MAC for achieving message authentication. What is a direct digital signature? 3M

****