Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
A Constituent Institution of Manipal University

VI SEMESTER B.TECH. (COMPUTER SCIENCE & ENGINEERING) DEGREE MAKEUP EXAMINATION-APRIL/MAY 2017
SUBJECT: PRINCIPLES OF CRYPTOGRAPHY (CSE 4015)
REVISED CREDIT SYSTEM
(/ /2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Explain the security goals. What are the different attacks that can affect these security goals? 3M

1B. Explain the working of a Hill Cipher. How can it be broken? Explain. 5M

1C. Explain key generation in DES algorithm. 2M

2A. What are the different types of attacks that can be applied on DES algorithm? 3M

2B. Draw neat diagrams and explain Cipher Block Chaining mode of operation. What are its merits and demerits? 4M

2C. State and prove Fermat's theorem. Find 3^{202} mod11, and 5^{-1} mod 23. 3M

3A. Draw a neat diagram and explain all the stages of AES decryption. 5M

3B. Draw a neat diagram and explain pseudo random number generation using triple DES. 2M

3C. Write the pseudo code and explain RC4 algorithm. 3M

4A. What is a one way function? Draw different diagrams and explain how public key cryptosystems can be used to provide secrecy only and authentication only. 5M

4B. Write the Diffie-Hellman key exchange algorithm. Explain its strengths and weaknesses. 5M

5A. What are the requirements of a cryptographic Hash function? 3M

5B. Draw a neat diagram and explain internal error control. Why is it required? 3M

5C. Write the generic model of a digital signature process and explain. Mention any four types of attacks on digital signature. 4M

****