Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

I SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) MAKE UP EXAMINATIONS, DEC 2016/JAN 2017

SUBJECT: NUMBER THEORY AND CRYPTOGRAPHY [CSE 5121]

REVISED CREDIT SYSTEM
(03/01/2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. You are trying to cryptanalyze an affine enciphering transformation of a single–letter message units in a 37 letter alphabet. This alphabet includes the numerals 0-9, which are labeled by themselves. (i.e. by the integers 0-9). The letters A-Z have numerical equivalents 10-35, respectively, and blank=36. You intercept the ciphertext "OHF7F86BB9". You know that the plaintext ends with the signature "007"(Zero, Zero, Seven). What is the message? **4M**

1B. Find an integer that has a remainder of 3 when divided by 7 and 13 but is divisible by 12. **3M**

1C. Write the algorithm for Miller –Rabin primality test.and check whether 561 passes the Miller Rabin Test. Indicate all the steps. **3M**

2A. With a neat diagram explain the IDEA encryption algorithm **4M**

2B. With an example explain the class of Complementary problems in NP. **3M**

2C. What do you mean by *algebraic structures*? List the properties of the Ring R=< S, +, .> **3M**

3A. Derive the expressions for addition of two points P=(x1,y1) and Q=(x2,y2) on elliptic curves. **4M**

3B. With a neat diagram explain the concept of public key cryptosystem. What are the security and efficiency requirements of public key cryptosystem? **3M**

3C. Explain RSA pseudorandom bit generator. Construct an instance of a RSA pseudorandom bit generator for p=7 and q=11, n=8, seed=3, e=5. Create a sequence of bits by extracting the three less significant bits from each integer. What is the period of the sequence? **3M**

4A. With a neat diagram explain the DES key scheduling algorithm **4M**

4B. What is hashing. Explain the properties and the major classes of hash functions **3M**

4C. What are fail stop signatures? What are the conditions that a fail-stop signature must satisfy? **3M**

5A. Explain how the interactive proof for the QNR problem proceeds and show how the proof system satisfies the completeness and soundness property. **4M**

5B. Given an A-code in the form of its authentication matrix shown in Table Q.5.B., determine the set of encoding rules E, the set of tags T, the set of source states S and the set of cryptograms M. Assume that the communicants have agreed to use the encoding rule $e_{3.}$ What are the cryptograms for all possible messages? Is the cryptogram $(s_1, 2)$ valid?

Table Q.5.B.

E\S	s1	s2	s3
e1	1	2	3
e2	2	3	1
e3	3	1	2
e4	1	3	2
e5	3	2	1
e6	2	1	3

4M

5C. Explain the following variants of RSA **2M**
(i)Rabin scheme
(ii)Williams scheme.