Reg. No.										

Manipal Institute of Technology, Manipal

(A Constituent Institute of Manipal University)

I SEMESTER M.TECH (COMPUTER SCIENCE AND INFORMATION SECURITY) END SEMESTER EXAMINATION, NOV/DEC 2015

SUBJECT: NUMBER THEORY AND CRYPTOGRAPHY [CSE 523]

REVISED CREDIT SYSTEM

Time: 3 Hours 3-12-2015 MAX. MARKS: 50

Instructions to Candidates:

- Answer **ANY FIVE FULL** questions.
- Missing data, if any, may be suitably assumed.

1A. Jessica breeds rabbits. She's not sure exactly how many she has today, but as she was moving them about this morning, she noticed some things. When she fed them, in groups of 5, she had 4 left over. When she bathed them, in groups of 8, she had a group of 6 left over. She took them outside to romp in groups of 9, but then the last group consisted of only 8. She's positive that there are fewer than 250 rabbits - but how many does she have? Use Chinese Remainder Theorem. 4M

1B. Classify the functions based on their rates of growth and explain the same. 2M

1C. Define Fiestel Transformation. Explain the Lucipher cryptosystem developed using Fiestel Transformation 4M

2A. Suppose that an affine cipher E(x) = (ax + b) MOD 26 enciphers H as X and Q as Y. Find the cipher (that is, determine a and b). 3M

2B. For the group G=<Z_6 , +> ,

(i) find the order of the group.

(ii)find the elements of subgroup generated by each of the element of the group and specify its order.

(iii)Identify the generators of the group. 4M

2C. State Fermat's Theorem and Euler's Theorem. Also prove Euler's Theorem 3M

3A. Assume an elliptic curve E_7 (2,4) with points whose coordinates P=(x,y) satisfy the following congruence $y^2 \equiv x^3+2x+4 \pmod 7$. Find all the points on the curve. For the given two points P = (2, 3) and Q = (3, 3), find the point R = P+Q. 4M

3B. With a neat diagram, explain public key cryptosystem. Explain the security and efficiency requirements of a public key cryptosystem. 3M

3C. Write the Miller Rabin Primality test algorithm and check whether the number 561 passes the Miller Rabin test. Indicate all the steps. 3M

4A. Explain Rabin scheme variant of RSA and show that it is insecure against chosen ciphertext attack and is immune against chosen plaintext attack. 5M

4B. For the input plain text $\{F0E1D2C3B4A5968778695A4B3C2D1E0F\}_x$ and the key $\{10101010101010101010101010101010\}_x$ using Rijndael algorithm,

(i) Show the original contents of the **State**

(ii) Show the contents of State after Add Round Key

(iii)Show the contents of State after Shift Rows Transformation
(iv)Show the first element of the State after Mix Column transformation using the constant matrix given in Table Q.4.B. Consider the multiplication of bytes in GF(2^8) with modulus ($x^8 + x^4 + x^3 + x + 1$)
(Use the output of each step as the input to the next step) 5M

Table Q.4.B

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

5A.What is probabilistic encryption. Explain Blum and Goldwaser probabilistic encryption scheme. 3M
5B. Define the following
(i)Function generator
(ii)Witness Circuit
(iii)Next Bit test 3M
5C. How do blind signatures work? Explain RSA blind signature scheme. 4M

6A. With neat diagrams, explain the birthday attack and the meet in the middle attack launched against the hashing schemes. 3M
6.B. With a neat diagram, explain the model of authentication system. Given an A-code in the form of its authentication matrix shown in Table Q.6.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? 4M

Table Q.6.B.

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

6C.What is a transcript simulator? Write the transcript simulator for Graph Isomorphism Interactive proof system. 3M