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

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

END SEMISTER EXAMINATIONS, NOV 2018

SUBJECT: NUMBER THEORY AND CRYPTOGRAPHY [CSE 5121]

REVISED CREDIT SYSTEM

(27/11/2018)

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 Chinese remainder theorem and find the value of x for the following example: **3M**

x ≡ 5 (mod 6)
x ≡ 4 (mod 11)
x ≡ 3 (mod 17)

Ensure the validation of the value of x.

1C. Given the message "additionalsheet" use a Rail Fence of key 3 to encrypt and decrypt this message. Show all the steps in detail. Make suitable assumptions if required. **3M**

2A. The vigenere key stream does not depend on the plaintext characters; it depends only on the position of the character in the plaintext. Write the procedure of encryption and decryption. Also, encrypt the message "She is listening" using the 6-character keyword "PASCAL". **3M**

2B. What is the Data Encryption Standard (DES)? Write the block diagram of the Data Encryption Standard system. Write encryption and decryption algorithms of DES system. **4M**

2C. Write the general design of AES encryption cipher. Distinguish between AES and DES crypto systems. **3M**

3A. Using Diffie Helman, prove KA=KB where KA and KB are shared secret keys. Consider a Diffie-Hellman scheme with a common prime number q=11 and primitive root α =7. Alice chooses a secret integer XA = 3. Bob chooses a secret integer XB = 6. Find the public keys and a shared key of Alice and Bob. **3M**

3B. Describe the RC4 algorithm for key- stream generation. Write encryption and decryption process of RC4 cryptosystem. **3M**

3C. Write Blum-Blum-Shub Pseudorandom Bit Generator and find linear congruential generator output, when m=16, a=3, and b=1, a, b are relatively prime numbers, m is modulus and x0 is initial seed value. Write the procedure to find points on the elliptic curve. **4M**

4A. Explain the key generation, encryption, and decryption of Rabin cryptosystem. Why it is called a variant of RSA? Clearly discuss the decryption process of Rabin cryptosystem by using Chinese remainder theorem. **3M**

4B. What is hashing function? Explain the general operation of a cryptographic hash function. Briefly explain the four message authentication techniques with the relevant diagrams. **4M**

4C. With the help of a diagram explain overview and step by step procedure of SHA-512. **3M**

5A. Why we need message authentication? write three types of functions that are used to produce an authenticator. With the help of a diagram briefly explain HMAC structure. **4M**

5B. Mention the key generation steps of Elliptic curve digital signature scheme. Write the block diagram representations of the following digital signature schemes. **3M**

(i) RSA digital signature scheme.

(ii) The RSA signature on the message digest.

5C. Briefly explain the model authentication system. What is zero-knowledge proof statements? write any two properties of zero-knowledge proof statements. **3M**