| Reg. No. | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|

# MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

*A Constituent Institution of Manipal University*

## I SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) END SEMESTER EXAMINATIONS, NOV/DEC 2016

SUBJECT: NUMBER THEORY AND CRYPTOGRAPHY [CSE 5121]

**REVISED CREDIT SYSTEM**
**(01/12/2016)**

Time: 3 Hours MAX. MARKS: 50

**Instructions to Candidates:**

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

**1A.** Assume that Eve intercepts the ciphertext PWUFFOGW encrypted by using an affine enciphering transformation of single letter message units in the 26 letter alphabet. She knows that the ciphertext WF corresponds to the plaintext ET. Find the plaintext. **4M**

**1B.** Write the Vigenere cipher encryption algorithm and using it encrypt the plain text *wearediscoveredsave* using the key *deceptive*. **3M**

**1C.** Write the Euclid algorithm for finding the greatest common divisor of two integers and using it find the gcd of 1547 and 560. Clearly indicate all the steps **3M**

**2A.** With a neat diagram, explain the Rijndael encryption algorithm and the key expansion algorithm for a block size of 128 bits **4M**

**2B.** What are class P and class NP problems? Give examples. **3M**

**2C.** What do you mean by *algebraic structures*? List the properties of the Field F=< S, +,.> **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.** In a public-key system using RSA, you intercept the ciphertext $C$ = 10 sent to an user whose public key is $e$ = 5, $n$ = 35. What is the plaintext $M$? **3M**

**3C.** Define pseudorandom number generators. The congruence $x_{i+1} \equiv ax_i + c \bmod N$ is used to generate a sequence of pseudorandom numbers. Compute first 10 numbers assuming the following parameters: N=7, a=3 and c=2. Assume initial seed=2. What is the period of the sequence? **3M**

**4A.** Explain how the blind signature scheme works and explain the RSA blind signature scheme **4M**

**4B.** Explain how serial and parallel hashing schemes could be used to compress arbitrarily long messages using a fixed input size hash function. **3M**

**4C.** Explain the various modes of operation of DES encryption algorithm. **3M**

**5A.** What is a transcript simulator? Write the transcript simulator for Quadratic Residue Interactive proof system **4M**

**5B.** Consider the authentication matrix given in Table Q.5B. Suppose an attacker, Oscar, knows that the communicants use the strategy $\pi = (\pi_{e1}, \ldots\ldots\ldots \pi_{e6}) = (\frac{1}{12}, \frac{3}{12}, \frac{1}{12}, \frac{4}{12}, \frac{2}{12}, \frac{1}{12})$.What are the conditional probabilities payoff$\pi(m_i)$ for all possible cryptograms $m_i$? What are the conditional probabilities payoff$_{\pi^*}(m_i)$ when the communicants Alice and Bob select the encoding rules with uniform probabilities (so $\pi^* = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$)? Discuss the results in the context of the impersonation attack. **4M**

Table **Q.5B**.

| E\M | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|
| $e_1$ | 1 | 2 | 3 |
| $e_2$ | 2 | 3 | 1 |
| $e_3$ | 3 | 1 | 2 |
| $e_4$ | 1 | 3 | 2 |
| $e_5$ | 3 | 2 | 1 |
| $e_6$ | 2 | 1 | 3 |

**5C.** Explain the properties that Substitution Permutation Networks are expected to have **2M**