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

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) MAKEUP EXAMINATIONS, AUGUST 2022

SUBJECT: CRYPTANAYSIS [CSE 5271]

REVISED CREDIT SYSTEM
(17/08/2022)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1.A Explain the method for addition of two points on the elliptic curves. Given the elliptic curve $y^2 = x^3+x-1$ (mod 11), with a point P(1,1) on the curve, compute the value of 2P, 4P, and 5P. **5M**

1.B For the S Box Representation given below **3M**

Input	0	1	2	3
Output	1	3	0	2

Construct the Linear Approximation Table. Show all the steps needed to arrive at the result.

1.C Compare the following LFSR based generators and mention one drawback of each. **2M**

(i) Geffe Generator
(ii) Shrinking Generator

2.A Compute the value of x in the expression $a^x = b$ (mod p) given a=2, b=5 and p=19 using Index Calculus method of computing the discrete logarithm. Clearly indicate all the steps in the computation. **5M**

2.B Do you think Brent's algorithm could be used to attack the Delayed CBC encryption implemented as a block wise mode of operation beyond the birthday paradox bound? If so, explain. **3M**

2.C Using Baby step Giant step algorithm, compute x in $3^x = 2$ (mod 17). **2M**

3.A Identify the modifications brought into CBC encryption to convert it into a secure CBC MAC, along with a note to justify the modifications. **5M**

3.B Outline the steps in the computation of the factors of an integer N using the Quadratic Sieve Factorization method. Also, identify the theorem used. **3M**

3.C Identify the application of cycle detection algorithms in finding collisions between meaningful messages in hash functions, and explain the same. **2M**

4.A Derive the expression for x in the equation $g^x = X \pmod p$ in the Pollard Kangaroo method of finding the discrete logarithm. Use $G = Z_{13}^*$ with g = 6 and X = 3 to determine x, such that $g^x = 6^x = X = 3 \pmod{13}$ using Pollard Kangaroo method. Define h : G → J = {1, 2, 3} by a table, where h repeats modulo 4 = 2s – 2 for s=3 **5M**

4.B Cryptanalyse the Affine Cipher to find the keys used for encryption, if, through frequency analysis, it is known that the ciphertext character R maps to character E in plaintext and ciphertext character K maps to plaintext character T. Hence decode the ciphertext **HFQR**. Show clearly all the steps. **3M**

4.C Is it possible to subject ElGamal algorithm to birthday attacks? If yes, state the requirements and elaborate the process. If no, mention the reasons. **2M**

5.A Factorize the numbers given below using the following Factorization Algorithms **5M**

(i) N=3675 using Fermat's differences of squares

(ii) N= 8051, given $g(x)= (x^2 + 1)$, using Pollard-Rho Algorithm

5.B Write the basic Eratosthenes's sieve algorithm. What improvements could be made on this algorithm to make it efficient? Explain. **3M**

5.C Describe the concept of value dependent cycle finding used in Nivasch's cycle detection algorithm. **2M**