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

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) MAKE UP EXAMINATIONS, JUNE/JULY 2023

SUBJECT: CRYPTANALYSIS [CSE 5271]

REVISED CREDIT SYSTEM
(28/06/2023)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1.A Demonstrate the usage of elliptic curves to factorize an integer. Consider an Elliptic curve given by the expression $y^2 = x^3 + x - 1 \pmod N$ with a point P(1,1) on the elliptic curve. Compute the factors of N, where N=21 using Lenstra's elliptic curve factorization method. Clearly show all the steps. **5M**

$$x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad where\ m = \frac{3x_1^2 + A}{2y_1}$$

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad where\ m = \frac{y_2 - y_1}{x_2 - x_1}$$

1.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**

1.C Identify the cryptographic system composition that can be subjected to ciphertext stealing attack and illustrate the attack. **2M**

2.A Compute the value of x in $a^x = b \pmod p$, using Index calculus method of finding discrete logarithm given a=2, b=10 and p=19. Clearly indicate all the steps in the computation. **5M**

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

2.C Show that CBC MAC is not secure for varying length messages. **2M**

3.A Determine the expressions for the corrections to be done on the input message words of a linearized SHA-0 algorithm to prevent the effect of difference in a single bit of input word from propagating further, in the two parallel computations of hash value. **5M**
The expressions used in computation of the inner state in SHA-0 algorithm is given below for reference.

$$A^{(i+1)} = \texttt{ROL}_5\left(A^{(i)}\right) + f^{(i)}(B^{(i)}, C^{(i)}, D^{(i)}) + E^{(i)} + W^{(i)} + K^{(i)}$$
$$B^{(i+1)} = A^{(i)},$$
$$C^{(i+1)} = \texttt{ROL}_{30}\left(B^{(i)}\right),$$
$$D^{(i+1)} = C^{(i)} \text{ and}$$
$$E^{(i+1)} = D^{(i)}.$$

3.B Prove that CBC MAC algorithm is not secure if IV is selected arbitrarily. Illustrate with an example. **3M**

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

(i) Geffe Generator

(ii) Shrinking Generator

4.A Describe Floyd's and Brent's cycle detection algorithms and bring out a comparison of both. Identify which one is better and justify your answer. **5M**

4.B Suppose Bob uses RSA algorithm to encrypt a message using the public modulus 899 and public key 7. Show how Pollard's p-1 algorithm can be used to attack the RSA cryptosystem. Clearly indicate all the steps. **3M**

4.C Develop a method to attack the El Gamal algorithm using the birthday paradox. **2M**

5.A Using Atkin and Bernstein's sieve, compute the prime numbers less than 60. Clearly indicate all the steps **5M**

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**