II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) END SEMESTER EXAMINATIONS, MAY 2023

SUBJECT: CRYPTANALYSIS [CSE 5271]

REVISED CREDIT SYSTEM

(22/05/2023)

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. Given the elliptic curve $y^2 = x^3+x-1 \bmod 11$, with a point P(1,1) on the curve, compute the value of 2!P, 3!P. **5M**

The formulae for addition of two points on the elliptic curve is given below.

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

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

1.B Show that the ECB mode of symmetric key encryption is insecure against various kinds of distinguishing attacks. **3M**

1.C Identify the cryptographic system composition that can be subjected to forwarding 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=5 and p=19. Clearly indicate all the steps in the computation. **5M**

2.B Apply cycle detection algorithms to attack the hash functions. **3M**

2.C In a certain public key cryptographic system, the attacker encounters the expression $2^x=10 \pmod{19}$ in order to attack the system. Help the attacker to solve the expression using Baby Step Giant step algorithm. **2M**

3.A Consider SHA-0 hashing algorithm. Introduce a change on single bit of W and let the change occur in the 5^{th} bit position. Summarize all possible interactions between interleaved local collisions and list them in a table. How many interferences of overlapping local collisions are identified? Explain. **5M**

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

3.C Determine the index of coincidence for the following ciphertext produced by Vigenere cipher. **2M**

SMWP PYAJS TLVA SMWJP

4.A Bob sends the broadcast message M to four recipients R1, R2, R3 and R4, who are using the public modulus 5, 7, 11 and 13 respectively. Bob obtains the public keys of all the recipients and computes the ciphertexts of the four recipients R1, R2, R3 and R4 as 1, 6, 7 and 8 respectively, using RSA algorithm with public key e=3 and sends the corresponding ciphertexts to the four recipients. Suppose Eve intercepts the ciphertexts, show how Eve computes the message M using Hastad's Attack on Broadcasted Messages. Clearly indicate all the steps. **5M**

4.B Using Atkin and Bernstein's sieve, compute the prime numbers less than 20. Clearly indicate all the steps. **3M**

4.C Develop a method to attack the RSA algorithm using the birthday paradox. List out the requirements. **2M**

5.A Suppose Bob and Alice decide to communicate using RSA cryptosystem. Alice computes the private key with public modulus as given below, and transmits the public modulus, along with a chosen public key to Bob. Demonstrate the usage of the following algorithms to attack the cryptosystem. **5M**

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

(ii)N=8051 and $g(x)= (x^2 + 1)$ using Pollard Rho factorization Algorithm

5.B Outline the basic Eratosthenes's sieve algorithm. Compare the performance of Wheel factorization with basic Eratosthenes's sieve algorithm. List the drawback of wheel factorization. **3M**

5.C Compute the sequence by applying Brent's cycle detection algorithm, for the given function $F(x) = (x^2 + 1) \pmod{255}$, with initial value for x as 3. Also find the length of the cycle and the tail. Plot the function. **2M**