REV-01
MSM/07/12

2024/05

SET A

M.SC. MATHEMATICS
FOURTH SEMESTER
CRYPTOGRAPHY
MSM - 403E

[USE OMR FOR OBJECTIVE PART]

Duration: 1:30 hrs. **Full Marks: 35**

Objective

Time: 15 mins. **Marks: 10**

Choose the correct answer from the following: ***1×10=10***

1. The number of possible keys in the affine cipher over $\mathbb{Z}_{26}$ is:
   a. 26 b. 26!
   c. 312 d. None of these
2. Which of the following cryptosystem has randomized encryption algorithm?
   a. RSA cryptosystem b. ElGamal cryptosystem
   c. Rabin cryptosystem d. All the above
3. Signature generation algorithm needs
   a. Secret key of signer b. Public key of signer
   c. Secret key of verifier d. Public key of verifier
4. Which of the following is/are not a cryptosystem
   a. RSA cryptosystem b. ElGamal cryptosystem
   c. Diffie-Hellman key exchange protocol d. None of these
5. What is the maximum period of an n-bit LFSR?
   a. $2^n - 1$ b. 2^n
   c. n^2 d. n
6. What is the primary function of a Linear Feedback Shift Register (LFSR)?
   a. To generate random numbers b. To perform arithmetic operations
   c. To generate sequences of bits d. None of these
7. In Elliptic curve, the inverse point for $P = (r, s)$ is
   a. $(-r, s)$ b. $(r, -s)$
   c. $(-r, -s)$ d. None of these
8. In non-singular elliptic curve, the elliptic curve $^3 + + = 0$ has
   a. Three distinct roots. b. three equal roots
   c. no distinct roots d. None of these

9. Which of the following is/are decisional problem?
   a. Discrete logarithm problem
   b. Integer Factorization Problem
   c. Diffie-Hellman Problem
   d. None of these

10. Which of the following algorithm has no probabilistic polynomial time algorithm?
   a. Algorithm to compute product of first n natural number.
   b. Algorithm to compute sum of first n natural number.
   c. Algorithm to convert a decimal number to binary.
   d. Algorithm to compute gcd of two non-zero integers.

-- --- --

Descriptive

Time : 1 hr. 15 mins. **Marks: 25**

[Answer question no.1 & any two (2) from the rest]

1. Suppose $m = 4$ and the keystream is generated using the linear recurrence $z_{i+4} = (z_i + z_{i+1}) \bmod 2, i \geq 1$. If the keystream is initialized with $(1, 0, 0, 0)$ then generate the keystream and also find the period of the keystream. **5**

2. Let E be the elliptic curve $y^2 = x^3 + x + 6$ define over $\mathbb{Z}_{11}$. **5+1+4 =10**
   (a) Determine the number of points on E.
   (b) Prove or disprove that E is cyclic.
   (c) If $P = (3, 5)$. Find $3P$.

3. Explain RSA Cryptosystem in details. Prove that the RSA Cryptosystem is insecure against a chosen ciphertext attack. In particular, given a ciphertext c, describe how to choose a ciphertext $c' \neq c$, such that knowledge of the plaintext $m' = d_K(c')$ allows $m = d_K(c)$ to be computed, where d_K is the decryption function. **5+5=10**

4. Explain ElGamal Signature Scheme in details. Prove that Existential forgery is possible in ElGamal Signature Scheme under key-only attack. **5+5=10**

5. Suppose the plaintext *friday* is encrypted using a Hill cipher with $m = 2$, to give the ciphertext *PQCFKU*. Find the secret key of the Hill cipher. **10**

= = *** = =