Total number of printed pages: **Programme(UG)/3rd Semester/UCSE302**

2023

Elementary Number Theory and Algebra

Full Marks: 100

Time: Three hours

Answer any Five questions.

1. i. Using Playfair cipher encrypt and decrypt the message "**Attack tonight**" using the key "**Monarchy**". 5

   ii. Use Mathematical Induction, for any positive integer number n, to prove that $(n3 + 2n)$ is always divisible by 3. 5

   iii. What is the Diffie-Hellman Key Exchange Algorithm? Suppose Alice and Bob agreed on **p** as **7** and **g** as **5**. Find the value of secret keys? 2+3=5

   iv. Explain the security threat of the Diffie-Hellman Key Exchange Algorithm with the help of diagram. 5

2. i. Using Hill cipher encrypt and decrypt the message "BALL" with key 10

$$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

   ii. Using Chinese remainder theorem solve the value of x: 10

   $X \equiv 2(\text{mod } 4)$, $X \equiv 1(\text{mod } 5)$, $X \equiv 3(\text{mod } 9)$, $X \equiv 7(\text{mod } 13)$

3 i. Discuss properties of a group in details. 8

   ii. Prove that $Z = \{0,1,2,3,4,5\}$ is a Ring with respect to modulo 6 under operation $(Z, +, *)$. 12

4. i. What is the full form of RSA. Write RSA algorithm. 2+3=5

   ii. In an RSA cryptosystem, a particular A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. If the public key of A is 35. Then the private key of A is? 4+3=7

   Show the encryption and decryption for message M=10.

iii. What are the major vulnerability points of the RSA algorithm? 4

iv. Find the **gcd (167, 28)** also find the value of s and t using Extended Euclidean Algorithm. 4

5. i. Convert the following: 2*5=10

i. $(100111.1110)_2 = (?)_{10}$

ii. $(1001111110)_2 = (?)_{16}$

iii. $(100)_{10} = (?)_8$

iv. $(ABCD)_{16} = (?)_{10}$

v. $(AB3D)_{16} = (?)_2$

ii. Find the multiplicative inverse of 57 mod 26. 5

iii. Compute the following: 1*5=5

i. -114 mod 3

ii. 212 mod 4

iii. -8 mod 11

iv. 2152 mod 6

v. 212 mod 11

6. **Write short note on** 4*5=20

i. Rail fence cipher

ii. Cyclic Group

iii. Rings

iv. Euclidean's algorithm

7. **Difference between** 4*5=20

i. Symmetric key and Asymmetric key cryptography.

ii. Encryption and Decryption algorithm

iii. Abelian group and cyclic group

iv. Semi group and monoid

****