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

2022

Elementary Number Theory and Algebra

Full Marks: 100

Time: Three hours

Answer any Five questions.

1.	i.	Using Palyfair cipher encrypt and decrypt the message "CRYPTOGRAPHY IS TOO COOL " using the key "MONARCHY".	10
	ii.	Use Mathematical Induction to prove that sum of the first n odd positive integer is n^2.	10
2.	i.	Discuss Eular's Phi function. What is value of Φ(240)?	5
	ii.	Using Chinese remainder theorem solve the value of x: $3x \equiv 1 (\text{mod } 5)$ $4x \equiv 6 (\text{mod } 14)$ $5x \equiv 11 (\text{mod } 3)$	15
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 to prime numbers. 13 and 11, to generate the public key and private key.	7
	iii.	With the help of a diagram explain the encryption and decryption process	8
5.	i.	Using Hill cipher encrypt and decrypt the message "ATTACK" with key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$	20
6.		Write short note on	4*5=20
	i.	Symmetric key and Asymmetric key cryptography.	
	ii.	Cyclic Group	
	iii.	Rings	
	iv.	Euclidean's algorithm	

****