MODEL QUESTION PAPER : 2023-24

Course Code:21MA563

VIDYAVARDHAKA COLLEGE OF ENGINEERING
Autonomous Institute, Affiliated to Visvesvaraya Technological University, Belagavi
Gokulam, 3rd Stage, Mysuru 570 002
Fifth Semester B.E. Examinations
COURSE NAME: NUMBER THEORY AND CRYPTOGRAPHY

Duration: 3-hour **Max. Mark: 100**

INSTRUCTION TO STUDENTS

1) Answer <u>One Full</u> question from each module

Q. No.	Module-I	Marks	BL	CO
1. (a)	Use Euclidean algorithm to obtain integers x and y satisfying: $gcd(12378, 3054) = 12378x + 3054y$	6	L3	2
1. (b)	Determine all integer solutions of the following Diophantine equations: i. $56x + 72y = 40$ ii. $221x + 35y = 11$ / or Linear Congruence	7	L3	2
1. (c)	Use Chinese remainder theorem to solve the simultaneous congruence: $x \equiv 1(mod\ 3)$ $x \equiv 2(mod\ 5)$ $x \equiv 3(mod\ 7)$	7	L3	2
	Module-II			
2.(a)	State and prove Euler's theorem. / Fermat thm	6	L2	1
2.(b)	Find the last two digits of 3^{2050}	7	L3	2
2.(c)	Prove that $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$ is a finite field with respect to the binary operations addition and multiplication modulo 7.	7	L4	3
	Module-III			
3.(a)	Let the integer a have order k modulo n. Then prove that $a^h \equiv 1(mod\ n)$ if and only if $k \mid h$.	6	L2	1
3.(b)	Show that if n has a primitive root then it has precisely $\phi(\phi(n))$ number of primitive roots. / & problems	7	L3	2
3.(c)	Determine the remainder when $N = 3^{24}5^{13}$ is divided by 17.	7	L3	2
	(OR)			
4.(a)	Write the definition of Legendre symbol and evaluate $\left(\frac{219}{383}\right)$.	6	L2	1
4.(b)	If p is an odd prime and $\gcd(a, p) = 1$, prove that a is a quadratic residue modulo p if and if $a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$.	7	L3	2

MODEL QUESTION PAPER : 2023-24

Course Code:21MA563

4.(c)	Solve the following quadratic congruence $x^2 + 7x + 10 \equiv 0(mod\ 11)$	**7**	**L3**	**2**
	Module-IV			
5.(a)	Decipher **HPCCXAQ** if the encipherment function is $E(x) \equiv (5x + 8)(mod\ 26)$.	**6**	**L3**	**2**
5.(b)	Use the Vigenère cipher formula to encrypt a plaintext **ATTACKATDAWN** using a keyword **LEMON.**	**7**	**L4**	**3**
5.(c)	Use a Hill cipher with key $\begin{bmatrix} 3 & 7 \\ 5 & 17 \end{bmatrix}$ to encrypt the following message. **"Agnes Driscoll worked for NSA".**	**7**	**L4**	**3**
	(OR)			
6.(a)	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value $q = 17$ and primitive root is 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged?	**6**	**L3**	**2**
6.(b)	Use RSA algorithm, find the public key and private key with respect to $p = 3, q = 11$ and $M = 31$. Also encrypt and decrypt the number $M = 31$.	**7**	**L4**	**3**
6.(c)	Evaluate the discrete logarithm of 60 to the base 4 with prime $p = 163$.	**7**	**L4**	**3**
	Module- V			
7.(a)	The cubic curve $y^2 = x^3 + 17$ has the following points say $Q_1 = (-2, 3)$ $Q_2 = (2, 5)$, compute the points $Q_3 = -Q_1 + 2Q_2$ and $Q_4 = 3Q_1 - Q_2$.	**6**	**L2**	**1**
7.(b)	Use Miller-Robin's primality test to show that 561 is a composite number.	**7**	**L3**	**2**
7.(c)	Explain Elliptic curve Diffie Hellman key exchange.	**7**	**L3**	**2**