MODEL QUESTION PAPER : 2024-25

Course Code: BMANT553

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/PO
1. (a)	Use Euclidean algorithm to obtain integers x and y satisfying: $gcd1278, 1054=1278x+1054y$	6	L3	2/1
1. (b)	Determine all integer solutions of the following linear congruences: i. $5x \equiv 2 (mod 26)$ ii. $6x \equiv 15 (mod 21)$	7	L3	2/1
1. (c)	Use Chinese remainder theorem to solve the simultaneous congruence: $x \equiv 5 mod 10$ $x \equiv 7 mod 23$ $x \equiv 9 mod 29$	7	L3	2/1
	Module-II			
2.(a)	State and prove Euler's theorem/Fermat theorem.	6	L2	1/1
2.(b)	Find the last two digits of 92557	7	L3	2/1
2.(c)	Prove that $F7=\{0,1,2,3,4,5,6\}$ is a finite field with respect to the binary operations addition and multiplication modulo 7.	7	L4	3/2
	Module-III			
3.(a)	Let the integer a have order k modulo n. Then prove that $ah \equiv 1 (mod n)$ if and only if $k \mid h$.	6	L2	1/1
3.(b)	Show that if n has a primitive root then it has precisely $\phi(\phi(n))$ number of primitive roots.	7	L3	2/1
3.(c)	Use the theory of indices to solve the congruence $7x5 \equiv 3 (mod 17)$ by taking 3 is a primitive root of 17.	7	L3	2/1
	(OR)			
4.(a)	Write the definition of Legendre symbol and evaluate 367588.	6	L2	1/1
4.(b)	State and prove Euler's criterion for quadratic residues.	7	L3	2/1

4.(c)	Solve the following quadratic congruence $x2+7x+10\equiv 0(\mod 11)$	**7**	**L3**	**2/1**
	Module-IV			
5.(a)	Decipher **HPCCXAQ** if the encipherment function is $Ex\equiv(5x+8)(\mod 26)$.	**6**	**L3**	**2/1**
5.(b)	Use Miller-Robin's primality test to show that 561 is a composite number.	**7**	**L4**	**3/2**
5.(c)	Use a Hill cipher with key 37517 to encrypt the following message. **"Agnes Driscoll worked for NSA"**.	**7**	**L4**	**3/2**
	(OR)			
6.(a)	Question on Elgamal/Diffie Hellman crypto system	**6**	**L3**	**2/1**
6.(b)	Encode "BEAT" using RSA algorithm with the key {N=3021,e=17} and p=53, q=57.	**7**	**L4**	**3/2**
6.(c)	Evaluate log312 in Z29* using Shank's baby step-Giant step method.	**7**	**L4**	**3/2**
	Module- V			
7.(a)	The cubic curve $y2=x3+17$ has the following points say Q1=-2,3 Q2=2,5, compute the points Q3=-Q1+2Q2 and Q4=3Q1-Q2.	**10**	**L3**	**2/1**
7.(b)	Explain Elliptic curve Diffie Hellman key exchange with an example. **Or Problem of this kind** Alice and Bob wish to securely establish a shared secret using the **Elliptic Curve Diffie-Hellman (ECDH)** protocol. The elliptic curve is defined as: $y2\equiv x3+2x+3(\mod 17)$ The generator point G=(5,1) is given, and the order of G is n=7. If Alice secret key dA =2, and Bob secret is key dB=3, , what are the public keys they exchanged between them?	**10**	**L3**	**2/1**