Model Question Paper-1 with effect from 2022-23 (CBCS Scheme)

USN

Sixth Semester B.E. Degree Examination
CRYPTOGRAPHY

TIME: 03 Hours   **Max. Marks: 100**

Note: 01. Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE**.

		Module -1	*Bloom's Taxonomy Level	Marks
Q.01	a	Explain the division algorithm with example	L2	10M
	b	Show 8 and 15 are relatively prime because the positive divisor of 8 are 1, 2, 4 and 8, and the positive divisor of 15 are1, 3, 5 and 15.	L3	10M
		OR		
Q.02	a	Explain the polynomial Arithmetic Operations with example.	L2	10M
	b	Explain the Euclidian Algorithm to find the GCD of two numbers.	L2	10M
		Module-2		
Q. 03	a	Draw and explain the model of symmetric cryptosystem.	L2	10M
	b	Explain the application of security in networks.	L3	10M
		OR		
Q.04	a	Explain the different transposition techniques in security.	L3	10M
	b	Explain the Substitution techniques.	L3	10M
		Module-3		
Q. 05	a	Explain traditional block cipher structure with neat diagram	L2	10M
	b	Explain the Euler's theorem with example.	L2	10M
		OR		
Q. 06	a	Present an overview of the general structure of advanced Encryption standard	L2	10M
	b	Describe the overall scheme for DES algorithm and its silent feature.	L3	10M
		Module-4		
Q. 07	a	Explain the requirements of public-key cryptography.	L2	10M
	b	Assuming p=17 and q=11, find the public key and private keys. Perform encryption and decryption for plain text message block M=88	L3	10M
		OR		
Q. 08	a	Explain the Diffie-Hellman key exchange algorithm. Show that the keys generated at sender side and receiver side are same.	L2	10M
	b	Describe the Elliptic curve cryptography.	L3	10M
		Module-5		
Q. 09	a	Explain LFSR and how the shift register sequences are used in cryptography.	L2	10M
	b	Write a note on Design and analysis of stream cipher.	L2	10M
		OR		
Q. 10	a	With a neat diagram explain the generalized Geffe generator.	L2	10M
	b	Write a short note on : i) A5 to encrypt GSM ii) NANOTEQ and RAMBUTAN	L2	10M