

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

USN

--	--	--	--	--	--	--	--	--	--

### 6<sup>th</sup> Semester B.E. Degree Examination Subject Title-Data Security

TIME: 03 Hours

Max. Marks: 100

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

Module -1			*Bloom's Taxonomy Level	CO's	Marks
Q.01	a	Explain Model of symmetric cryptosystem along with its three independent dimensions.	L1	1	5
	b	Construct a Playfair matrix using the key "BALLOON" and encrypt the plaintext "ELECTRONICS AND COMMUNICATION".	L3	1	5
	c	Describe the process of Feistel encryption and decryption with neat figure.	L2	1	10
OR					
Q.02	a	Describe the detailed structure of AES encryption and decryption with neat figure.	L1	1	10
	b	Explain Ceasar cipher encryption. Apply the same for k=6 and Plain Text: CLASSICAL ENCRYPTION TECHNIQUES.	L3	1	5
	c	Discuss the given Block Cipher Modes of operation 1. Cipher Block Chaining                      2. Cipher Feedback 3. Output Feedback                                4. Counter	L2	1	5
Module-2					
Q. 03	a	Explain the Euclidian Algorithm to find the GCD of two numbers.	L2	1	10
	b	Show 8 and 15 are relatively prime.	L3	1	3
	c	Explain the properties of modular Arithmetic for Integers.	L2	1	7
OR					
Q.04	a	Explain divisibility and division algorithm.	L2	1	7
	b	Explain Groups and Rings with its properties.	L2	1	10
	c	Find $11^7 \pmod{13}$ .	L3	1	3
Module-3					
Q. 05	a	Explain Fermat's and Euler's theorems.	L2	1	6
	b	Discuss Diffie-Hellman key exchange.	L2	1	6
	c	Explain Elliptic curve arithmetic.	L2	1	8
OR					
Q. 06	a	Explain RSA algorithm. Find the public key and private key by using RSA algorithm for p=17, q=11.	L2	1	10
	b	List the difference between conventional encryption and public key encryption	L2	1	5

	c	Explain public key cryptosystem with authenticity and secrecy.	L3	1	5
<b>Module-4</b>					
Q. 07	a	Explain the security requirements for a cryptographic Hash function H.	L1	2	6
	b	Describe the structure and design objectives of the Hash-based Message Authentication Code (HMAC).	L2	2	10
	c	Discuss two simple Hash Function.	L2	2	4
OR					
Q. 08	a	Explain the step-by-step process of SHA-512 message digest generation with figure.	L1	2	10
	b	Discuss Message Authentication Code to provide confidentiality and authentication.	L2	2	10
<b>Module-5</b>					
Q. 09	a	With neat figure discuss secret key distribution with confidentiality and authentication.	L2	2	6
	b	Explain a transparent key control scheme and decentralized key distribution.	L2	2	6
	c	Discuss elliptic curve digital signature algorithm.	L2	2	8
OR					
Q. 10	a	Explain simplified depiction of essential elements of digital signature process.	L2	2	6
	b	Explain the digital signature algorithm along with neat figure of DSA signing and verifying.	L2	2	8
	c	Discuss four methods used for distributing public keys.	L2	2	6

\*Bloom's Taxonomy Level: Indicate as L1, L2, L3, L4, etc. It is also desirable to indicate the COs and POs to be attained by every bit of question