CBCS SCHEME

USN | | | | | | | | | | |

BCS703

Seventh Semester B.E./B.Tech. Degree Examination, Dec.2025/Jan.2026
Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M : Marks , L: Bloom's level , C: Course outcomes.

		Module – 1	M	L	C
Q.1	a.	Obtain Ciphertext for the given plaintext "HILLCIPHER" by applying the Hill Cipher technique using key $K = \begin{bmatrix} 03 & 02 \\ 08 & 05 \end{bmatrix}$	7	L3	CO1
	b.	Write a short note on Steganography and its advantages and disadvantages.	6	L2	CO1
	c.	With a neat diagram, explain the model for network security.	7	L2	CO1
		OR			
Q.2	a.	State the rules used for encryption in PLAYFAIR cipher and encrypt the message "COMPUTER" using the keyword "ENGINEERING" using PLAYFAIR cipher.	7	L3	CO1
	b.	Describe simple XOR and one – time pad encryption techniques with an example and their difficulties.	7	L2	CO1
	c.	With a block diagram, explain the various steps involved in encryption and key generation of the DES algorithm.	6	L2	CO1
		Module – 2			
Q.3	a.	Demonstrate the Diffie – Hellman key exchange algorithm.	8	L2	CO2
	b.	Perform encryption and decryption using the RSA algorithm given public key is 6 for two prime numbers 17 and 31 with message 3.	7	L3	CO2
	c.	Describe the fundamental requirements that a public key cryptosystem must meet to ensure security.	5	L2	CO2
		OR			
Q.4	a.	Explain briefly the elliptic curve cryptography and mention two applications.	8	L2	CO2
	b.	Let q = 719 and g = 5 , Xa = 157 , Xb = 293. Use the Diffie Hellman Key exchange algorithm to find Ya , Yb and Secret key K.	7	L3	CO2
	c.	Briefly explain the security aspects of the RSA algorithm.	5	L2	CO2

		Module – 3			
Q.5	**a.**	Explain the symmetric key distribution using Asymmetric Encryption.	**7**	**L2**	**CO3**
	b.	Explain the role of cryptographic hash functions in message authentication with a neat diagram.	**8**	**L2**	**CO3**
	c.	Discuss the general elements of an X.509 certificate.	**5**	**L2**	**CO3**
		OR			
Q.6	**a.**	What is Key Management? Explain with a neat diagram, how key usage can be controlled in encryption and decryption using control vectors.	**7**	**L2**	**CO3**
	b.	Describe the architecture of the Public Key Infrastructure X.509 (PKIX) model with a neat diagram.	**8**	**L2**	**CO3**
	c.	Write a short note on the various schemes of public key distribution.	**5**	**L2**	**CO3**
		Module – 4			
Q.7	**a.**	Explain functions and cryptographic algorithms used in S/MIME functionality.	**8**	**L2**	**CO4**
	b.	Define TLS and explain its architecture with a neat diagram.	**7**	**L2**	**CO4**
	c.	Bring out the differences between Kerberos version 4 and version 5.	**5**	**L2**	**CO4**
		OR			
Q.8	**a.**	Describe remote user authentication using asymmetric encryption.	**8**	**L2**	**CO4**
	b.	Explain Pretty Good Privacy (PGP) message transmission and reception with a neat diagram.	**7**	**L2**	**CO4**
	c.	Elaborate on the various security approaches that address web security threats.	**5**	**L2**	**CO4**
		Module – 5			
Q.9	**a.**	How does Domain Keys Identified Mail (DKIM) address the threats posed by email attackers and what is its strategy for email authentication?	**8**	**L2**	**CO5**
	b.	Explain Internet Key Exchange (IKE) key determination features.	**7**	**L2**	**CO5**
	c.	Explain Basic combinations of Security Associations.	**5**	**L2**	**CO5**
		OR			
Q.10	**a.**	Illustrate the key components of the Internet mail architecture with a clear diagram.	**8**	**L2**	**CO5**
	b.	Explain the Encapsulating IP Security Payload.	**7**	**L2**	**CO5**
	c.	Describe the functional flow of Domain Keys Identified Mail (DKIM).	**5**	**L2**	**CO5**

* * * * *