EPCET LIBRARY BANGALORE-49

CBCS SCHEME

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

BCS703

Seventh Semester B.E./B.Tech. Degree Examination, June/July 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.**	What is Cryptography? Explain a model for Network Security.	**6**	**L1**	**CO1**
	b.	Explain Monoalphabetic Cipher with Caesar Cipher.	**6**	**L2**	**CO2**
	c.	Explain Playfair Cipher and encrypt 'QUESTION' with the key = 'ANSWER' based on playfair cipher.	**8**	**L3**	**CO2**
		OR			
Q.2	**a.**	Explain stream ciphers and block ciphers with neat diagram.	**6**	**L1**	**CO1**
	b.	Discuss the strength of DES.	**6**	**L2**	**CO2**
	c.	Encrypt the message "X HOW ARE YOU" based on hill Cipher with the key $K = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$.	**8**	**L3**	**CO2**
		Module – 2			
Q.3	**a.**	Write a model of public key cryptosystem used for secrecy.	**6**	**L1**	**CO2**
	b.	Perform encryption and decryption using the RSA algorithm for the p = 5, q = 13, e = 5, M = 8.	**8**	**L3**	**CO2**
	c.	Write an algorithm for Diffie-Hellman key exchange.	**6**	**L2**	**CO2**
		OR			
Q.4	**a.**	Alice and Bob use the diffie-Hellman key exchange technique with a common prime q = 157 and a primitive root $\alpha = 5$. i) If Alice has a private key $X_A = 15$, find her public key Y_A. ii) If Bob has a private key $X_B = 27$, find his public key Y_B. iii) What is the shared secret key between Alice and Bob.	**10**	**L3**	**CO2**
	b.	For $E_{11}(1,7)$, consider the point G = (3, 2). Compute 2G and 3G.	**10**	**L3**	**CO2**
		Module – 3			
Q.5	**a.**	Explain symmetric key distribution using public keys.	**10**	**L2**	**CO4**
	b.	Discuss different types of distribution of public keys.	**10**	**L2**	**CO4**

		OR			
Q.6	**a.**	Explain X.509 certificate along with the format.	**10**	**L2**	**CO4**
	b.	Explain essential components of public key infrastructure.	**10**	**L2**	**CO4**
		Module – 4			
Q.7	**a.**	Give the scenario of mutual authentication with respect to remote user authentication using symmetric encryption.	**10**	**L2**	**CO3**
	b.	What is Kerberos? Give the summary of Kerberos version 4 message exchanger.	**10**	**L2**	**CO3**
		OR			
Q.8	**a.**	Compare different threats on the web with respect to threats, consequences and countermeasures.	**10**	**L2**	**CO3**
	b.	Explain different S/MIME services.	**10**	**L2**	**CO3**
		Module – 5			
Q.9	**a.**	Explain DKIM deployment with example.	**10**	**L2**	**CO5**
	b.	Explain applications and benefits of IP security.	**10**	**L2**	**CO5**
		OR			
Q.10	**a.**	Differentiate transport mode and tunnel modes.	**5**	**L2**	**CO5**
	b.	Explain processing model for outbound packets.	**10**	**L2**	**CO5**
	c.	Write top level format of an ESP packet.	**5**	**L2**	**CO5**

* * * * *

VTU-13-06-2026 08:56:39am - EP - EP - EP