CBCS SCHEME

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

BCY602

Sixth Semester B.E./B.Tech. Degree Examination, June/July 2025
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.	Explain playfair cipher algorithm. Find the cipher text for the plain text 'cryptography' with key 'MONARCHY'	10	L2	CO1
	b.	What are strengths of DES algorithm	05	L2	CO1
	c.	With a neat diagram explain the model of Network Security.	05	L2	CO1
		OR			
Q.2	a.	Encrypt the plaintext 'cryptography' using Hill cipher algorithm with key $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$	10	L3	CO1
	b.	With a neat schematic diagram explain DES encryption algorithm.	10	L2	CO1
		Module – 2			
Q.3	a.	Explain the RSA algorithm, perform encryption and decryption using RSA if, p = 3, q = 11, e = 7 and m = 5	10	L3	CO2
	b.	Distinguish between conventional and public key cryptosystem.	05	L2	CO2
	c.	Write the requirements for public key cryptography	05	L2	CO2
		OR			
Q.4	a.	Explain Diffie –Hellman key exchange algorithm and q =71, its primitive root $\alpha = 7$, A's private key is 5 B's private key is 12 Find : i) A's Public Key ii) B's Public Key iii) Shared Secret Key	10	L3	CO2
	b.	With neat diagrams explain the principles of public key cryptosystems.	10	L2	CO2
		Module – 3			
Q.5	a.	With neat diagrams describe the ways of hash code can be used to provide message authentication.	10	L2	CO3
	b.	Explain X = 509 CERTIFICATE with format	10	L2	CO3
		OR			
Q.6	a.	With block diagram explain the PKIX Architectural model	10	L2	CO3
	b.	Discuss four general categories of schemes for the distribution of public keys.	10	L2	CO3
		Module – 4			
Q.7	a.	Explain kerbos authentication service with version 4 dialogue	10	L2	CO4
	b.	Explain remote user authentication using a symmetric encryption.	10	L2	CO4
		OR			
Q.8	a.	Explain Transport layer security architecture.	10	L2	CO4
	b.	Explain four S/MIME message related services	10	L2	CO4
		Module – 5			
Q.9	a.	Explain domain keys identified mail strategy.	10	L2	CO5
	b.	Explain Transport mode and Tunnel mode of Ipsec.	10	L2	CO5
		OR			
Q.10	a.	With neat diagrams explain internet key exchange formats.	10	L2	CO5
	b.	Explain ESP (Encapsubting Security Pay load) packet format.	10	L2	CO5

* * * * *