Model Question Paper-I with effect from 2023-24 (CBCS Scheme)

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

Third Semester B.E. Degree Examination
Cryptography and Network Security

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	Draw the model of a symmetric cryptosystem and explain it.	L2	7
	B	Using Hill Cipher to encipher and decipher the message "Hi". Use the key (03 02 05 07)	L3	7
	C	List and explain the block cipher design principles	L2	6
		OR		
Q.02	A	Explain DES construction in detail with a neat diagram	L2	7
	B	Explain Playfair Cipher and its rules for the following example: Ex: Keyword: "Computer" Plaintext: "parrot"	L3	7
	C	What is the one-time pad technique? List the advantages and disadvantages.	L2	6
		Module-2		
Q.03	A	Explain the public key cryptosystem with a neat diagram.	L2	7
	B	What is the cipher text if the plain text is 63 and the public key is 13? Use the RSA algorithm.	L3	6
	C	Write about key generation, encryption and decryption in the ElGamal Cryptosystem.	L2	7
		OR		
Q.04	A	List the difference between Conventional and public key encryption	L2	7
	B	Let q=353 and g=3. Xa=97, Xb=233. Use Diffie Hellman Key exchange algorithm to find Ya, Yb and Secret key K.	L3	6
	C	What are the practical issues related to RSA?	L2	7
		Module-3		
Q.05	A	What is meant by key management? Explain Key Distribution scenarios with KDC	L2	10
	B	Explain the use of Control Vector Encryption and Decryption for controlling key usage. Mention its advantages.	L2	10
		OR		
Q.06	A	List and explain the four general categories of schemes for the distribution of public keys.	L2	10
	B	Explain Symmetric Key Distribution Using Asymmetric Encryption with a solution for man in the middle attack	L2	10
		Module-4		
Q.07	A	Write X.509 Formats. How is an X.509 certificate revoked?	L2	10
	B	Explain the Kerberos Version 4 diagram with message Exchanges.	L2	10
		OR		
Q.08	A	Explain the Needham-Schroeder Protocol. How Denning overcomes the weakness in the Needham-Schroeder Protocol.	L2	10

	B	With a neat diagram, explain the PKIX Architectural Model	L2	10
		Module-5		
Q.09	A	Explain PGP cryptographic functions or PGP functions with a neat diagram	L2	6
	B	Explain the ESP format in a neat diagram. Also, explain the transport and tunnel modes of ESP	L2	7
	C	With a neat diagram, explain IKE v2 exchanges.	L2	7
		OR		
Q.10	A	With a neat diagram explain the transmission and reception of PGP messages	L2	6
	B	Short note on 1) MIME transfer encodings 2) native and canonical form 3) S/MIME functionality 4) S/MIME messages.	L2	7
	C	Explain the Ipsec Architecture	L2	7