Q. Code:734410

Reg. No. | | | | | | | | | | | | | |

B.E./ B.TECH. DEGREE EXAMINATIONS, MAY 2024

Fifth &Seventh Semester

EC18006 – CRYPTOGRAPHY AND COMMUNICATION NETWORK SECURITY

(Electronics and Communication Engineering)

(Regulation 2018/2018A)

TIME:3 HOURS **MAX. MARKS: 100**

COURSE OUTCOMES	STATEMENT	RBT LEVEL
CO 1	Comparison of classical encryption techniques.	**2**
CO 2	Compare and implement symmetric and asymmetric key algorithms for real time applications.	**3**
CO 3	Realize the authentication and hash function concepts.	**3**
CO 4	Figure out network security issues and identify suitable solution.	**3**
CO 5	Figure out system level security issues and identify suitable solution.	**3**

PART- A(10x2=20Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	Differentiate between an unconditionally secure cipher and a computationally secure cipher.	**1**	**3**
2.	Encrypt the plaintext "CRYPTOGRAPHY" using shift cipher technique using the key "5".	**1**	**3**
3.	Define a trapdoor one way function.	**2**	**2**
4.	State the difference between conventional encryption and public-key encryption.	**2**	**4**
5.	What is the significance of hash functions in cryptography?	**3**	**2**
6.	What do you infer from the word Message Authentication?	**3**	**2**
7.	Identify the requirements for Kerberos.	**4**	**4**
8.	How PGP handles email security?	**4**	**2**
9.	Highlight the design goals of firewalls.	**5**	**4**
10.	Examine the need for an intrusion detection system.	**5**	**4**

PART- B (5x 14=70Marks)

			Marks	CO	RBT LEVEL
11. (a)	**(i)**	Find multiplicative inverse of 27 in Z_{100} using Extended Euclidean Algorithm.	**(6)**	**1**	**4**
	(ii)	Analyze the structure of DES and mention its weaknesses in design.	**(8)**	**1**	**4**

(OR)

(b)	**(i)**	What is the cipher text of "BRILLIANT THINKING" using Playfair cipher with key "EDUCATION"?	**(6)**	**1**	**3**
	(ii)	Categorize various modes of operations of block ciphers.	**(8)**	**1**	**4**
12. (a)	**(i)**	State the Euler's theorem and applications of it.	**(4)**	**2**	**3**
	(ii)	Find the results of 6^{24} mod 35, 20^{62} mod 77, 8^{-1} mod 77, 7^{-1} mod 15 and 71^{-1}mod 100 using Euler's theorem.	**(10)**	**2**	**4**
		(OR)			
(b)	**(i)**	Using RSA algorithm encrypt John's plaintext message 63 to Bob using Bob's public key. Bob chooses two prime numbers p and q as 7 and 11 respectively and his private key as 37. Find public key of Bob before encrypting the given plaintext message. Decrypt the cipher text to get back the same plain text.	**(10)**	**2**	**3**
	(ii)	Illustrate Diffie-Hellman Key exchange algorithm.	**(4)**	**2**	**3**
13. (a)		List the main features of the SHA-512 Cryptographic hash function. What kind of compression function is used in SHA-5l2? Explain it.	**(14)**	**3**	**2**
		(OR)			
(b)		Discuss about ElGamal and Schnorr Digital Signature schemes in detail.	**(14)**	**3**	**2**
14. (a)		Discuss about Kerberos authentication service in detail.	**(14)**	**4**	**2**
		(OR)			
(b)		Explain about S/MIME in detail.	**(14)**	**4**	**2**
15. (a)		Elaborate on the various types of malicious softwares and its related threats. Mention its counter measures.	**(14)**	**5**	**3**
		(OR)			
(b)		What is the necessity for firewalls in any organization? Discuss about various types of firewalls that are helpful to build trusted systems.	**(14)**	**5**	**3**

PART- C (1x 10=10Marks)

(Q.No.16 is compulsory)

			Marks	CO	RBT LEVEL
16.		Find an integer that has a remainder of 3 when divided by 7 and 13 but it is divisible by 12.	**(10)**	**2**	**4**

****