PRIYADARSHINI COLLEGE OF ENGINEERING, NAGPUR

Department: Computer Technology | Semester: VII | Section: A and B

CAT-I (2023-24)

Subject : Cryptography and Network Security | Subject Code : BTCT701T

Duration : 1.5Hrs | Max. Marks : 35

Note:
1) All questions are compulsory.
2) All questions carry marks as indicated.

			Questions	Marks	CO	BL
Q.1	A	I	Which of the following is not substitution cipher? a) Caesar Cipher b) Playfair Cipher c) Hill Cipher d) Railfence Cipher	1M	CO1	II
		II	What is the purpose of Euclidean algorithm? a) To perform primality testing b) To compute GCD of two numbers c) To generate pseudo random numbers d) None of the above	1M	CO1	II
	B		Explain in detail about various transposition ciphers used in cryptography.	5M	CO1	II
	C		Demonstrate the working of encryption and decryption procedure in Hill Cipher with respect to following parameters: Plain Text : HILLCIPHER Key : $\begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$	7M	CO1	III

OR

Q.2	A	I	Caesar Cipher is an example of _____ a) Substitution Cipher b) Transposition Cipher c) a and b both d) None of the mentioned	1M	CO1	II
		II	The Vigenere cipher is an example of _____ a) Poly alphabetic substitution cipher b) Transposition cipher c) Mono alphabetic cipher d) None of the above	1M	CO1	II
	B		Explain in detail about Playfair Cipher and then apply it to encrypt with respect to: Plain Text : CHANDRAYAAN Keyword Matrix : T M P O S Z V W X Y E Q C U R F N A B D L G H I/J K	5M	CO1	III
	C		Apply Extended Euclid algorithm to compute GCD (99,78). Show all the computations.	7M	CO1	III

			Questions	Marks	CO	BL
Q.3	A	I	Symmetric key cryptography involves the usage of the _____ key / Keys. a) one b) Two c) Three d) None of the above	1M	CO2	II
		II	The total number of keys required for a set of n individuals to be able to communicate with each other using secret key and public key cryptosystems, respectively are: a) n(n-1) and 2n b) 2n and n(n-1)/2 c) n(n-1)/2 and 2n d) n(n-1)/2 and n	1M	CO2	II
	B		Differentiate between stream ciphers and block ciphers.	5M	CO2	II
	C		What are the block cipher modes of operation of DES? Explain in detail.	7M	CO2	II
			OR			
Q.4	A	I	DES Algorithm is _____ a) Block cipher algorithm b) Stream cipher algorithm c) Asymmetric algorithm d) None of the above	1M	CO2	II
		II	The DES algorithm has a key length of _____ a) 8 bit b) 32 bit c) 128 bit d) 56 bit	1M	CO2	II
	B		Explain Key Calculation Procedure in Simplified DES algorithm.	5M	CO2	II
	C		Explain in detail about IDEA algorithm.	7M	CO2	II
Q.5	A	I	Identify the value of $\varphi(10)$? a) 6 b) 4 c) 8 d) 3	1M	CO3	III
		II	Extended Euclid's algorithm is used for finding_____ a) GCD of two numbers b) GCD of more than three numbers c) LCM of two numbers d) Both a and c	1M	CO3	II
	B		Apply the Chinese Remainder Theorem to solve following congruent equations. $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$	5M	CO3	III
			OR			
Q.6	A	I	A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statement is TRUE? a) Sender encrypts using receiver's public key b) Sender encrypts using his own public key c) Receiver decrypts using sender's public key d) Receiver decrypts using own public key	1M	CO3	II
		II	Which of the following is not public key Distribution means_____? a) Public key certificates b) Hashing Certificates c) Publicly available directories d) Public Key authority	1M	CO3	II
	B		In public key system using RSA you intercept the cipher text C = 10 sent to the user whose public key is e = 5, n = 35, what is the plaintext M?	5M	CO3	III

********* **Best of Luck** **********