D:- 19.12.22
2nd half

GURU NANAK INSTITUTE OF TECHNOLOGY
An Autonomous Institute under MAKAUT
2022
CRYPTOGRAPHY AND NETWORK SECURITY
CS703C

TIME ALLOTTED: 3Hours **FULL MARKS:70**

The figures in the margin indicate full marks.
Candidates are required to give their answers in their own words as far as practicable

GROUP – A
(Multiple Choice Type Questions)

Answer any *ten* from the following, choosing the correct alternative of each question: **10×1=10**

	Question	Marks	CO No
1. i.	Which one of the following is a cryptographic protocol used to secure HTTP connection? a) stream control transmission protocol (SCTP) b) transport layer security (TSL) c) explicit congestion notification (ECN) d) resource reservation protocol	1	CO2
ii.	Voice privacy in GSM cellular telephone protocol is provided by a) A5/2 cipher b) b5/4 cipher c) b5/6 cipher d) b5/8 cipher	1	CO2
iii.	Caesar Cipher is an example of a. Poly-alphabetic Cipher b. Mono-alphabetic Cipher c. Multi-alphabetic Cipher d. Bi-alphabetic Cipher	1	CO3
iv.	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW a. ABANDONED LOCK b. ENCRYPTED TEXT c. ABANDONED TEXT d. ENCRYPTED LOCK	1	CO3
v.	The ciphers of today are called round ciphers because they involve a) Single Round b) Double Rounds c) Multiple Round d) Round about	1	CO4

vi.	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation a) 1 and 3 b) 2 and 3 c) 3 and 4 d) 2 and 4	1	CO3
vii.	DES follows a) Hash Algorithm b) Caesars Cipher c) Feistel Cipher Structure d) SP Networks	1	CO2
viii.	The DES algorithm has a key length of a) 128 Bits b) 32 Bits c) 64 Bits d) 16 Bits	1	CO2
ix.	How many keys does the Triple DES algorithm use? a) 2 b) 3 c) 2 or 3 d) 3 or 4	1	CO2
x.	AES uses a ____________ bit block size and a key size of __________ bits. a) 128; 128 or 256 b) 64; 128 or 192 c) 256; 128, 192, or 256 d) 128; 128, 192, or 256	1	CO4
xi.	Which one of the following is not a cryptographic algorithm- JUPITER, Blowfish, RC6, Rijndael and Serpent? a) JUPITER b) Blowfish c) Serpent d) Rijndael	1	CO4
xii.	In symmetric-key cryptography, the key locks and unlocks the box is a) same b) shared c) private d) public	1	CO2

GROUP – B

(Short Answer Type Questions)

(Answer any *three* of the following) **3 x 5 = 15**

		Marks	CO No
2.	Use the additive Cipher with key=15 to encrypt the message "hello" and then decrypt it.	5	CO1
3. a.	Define a symmetric-key cipher.	2	CO2
b.	What is a Denial of service attack? Give example.	3	CO2
4.	Use the Euclidean algorithm, find the greatest common divisor of the following pairs of integers: (i) 88 and 220 (ii) 300 and 42 (iii) 24 and 320	5	CO2
5.	Describe cipher block chaining (CBC) mode.	5	CO1
6.	Encrypt "The key is hidden under the door" using Playfair Cipher with keyword "domestic".	5	CO5

GROUP – C

(Long Answer Type Questions)

(Answer any *three* of the following) **3 x 15 = 45**

		Marks	CO No
7. a.	Give the format of X 509 digital certificate and explain the use of digital signature in it.	7	CO2
b.	Perform the following operations using reductions first. i. (273 + 147) mod 10 ii. (4223 + 17323) mod 10 iii. (148 + 14432) mod 12 iv. (2467 + 461) mod 12	8	CO3
8. a.	How authentication and confidentiality are achieved using IPSec?	6	CO4
b.	Calculate Cipher Text using RSA Algorithm for following data: Prime Numbers P=7, Q= 17. Plain Text Message M=10. Find pair of keys and Cipher text (D, C and P).	9	CO4
9. a.	What is the pattern in the cipher text of a one-time pad cipher in each of the following cases? (i) The plaintext is made of n 0's (ii) The plaintext is made of n 1's (iii) The plaintext is made of alternating 0's and 1's (iv) The plaintext is a random string of bits	8	CO3

	b. Describe Synchronous Stream Ciphers	4	CO2
	c. What is Linear Cryptanalysis?	3	CO1
10.	a. State Elgamal Cryptography method.	5	CO2
	b. Apply Encryption and Decryption Technique (Consider PT =7)	5	CO4
	c. Explain SHA algorithm	5	CO3
11.	Write short notes on any three of the following:	3x5=15	
	a. Pretty Good Privacy (PGP)	5	CO4
	b. Advanced Encryption Standard/AES	5	CO4
	c. DSS (Digital Signature Standard)	5	CO3
	d. Elliptic Curve Cryptography	5	CO2
	e. ECB (Electronic Codebook) Mode	5	CO2