

GURU NANAK INSTITUTE OF TECHNOLOGY

An Autonomous Institute under MAKAUT

2020-2021

CRYPTOGRAPHY AND NETWORK SECURITY**CS704C****TIME ALLOTTED: 3 HRS****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 (10)** from the following, choosing the correct alternative of each question: **10×1=10**

	Marks	CO No
1. (i) SHA-1 has a message digest of _____.	01	CO1
a) 160 bits		
b) 512 bits		
c) 628 bits		
d) 820 bits		
(ii) Message authentication is a service beyond _____.	01	CO4
a) Message Confidentiality		
b) Message Integrity		
c) Message Splashing		
d) Message Sending		
(iii) Caesar Cipher is an example of	01	CO2
a) Poly-alphabetic Cipher		
b) Mono-alphabetic Cipher		
c) Multi-alphabetic Cipher		
d) Bi-alphabetic Cipher		
(iv) Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW	01	CO5
a) ABANDONED LOCK		
b) ENCRYPTED TEXT		
c) ABANDONED TEXT		
d) ENCRYPTED LOCK		
(v) A _____ can be used to preserve the integrity of a message.	01	CO2
a) Message digest		
b) Message Summary		
c) Ciphertext		
d) Plaintext		
(vi) Which of the following slows the cryptographic algorithm –	01	CO5
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 | | |
| (vii) | The DES algorithm has a key length of | 01 | CO2 |
| | a) 128 Bits | | |
| | b) 32 Bits | | |
| | c) 64 Bits | | |
| | d) 16 Bits | | |
| (viii) | How many keys does the Triple DES algorithm use? | 01 | CO2 |
| | a) 2 | | |
| | b) 3 | | |
| | c) 2 or 3 | | |
| | d) 3 or 4 | | |
| (ix) | AES uses a _____ bit block size and a key size of _____ bits. | 01 | CO3 |
| | a) 128; 128 or 256 | | |
| | b) 64; 128 or 192 | | |
| | c) 256; 128, 192, or 256 | | |
| | d) 128; 128, 192, or 256 | | |
| (x) | Which one of the following is not a cryptographic algorithm- JUPITER, Blowfish, RC6, Rijndael and Serpent? | 01 | CO2 |
| | a) JUPITER | | |
| | b) Blowfish | | |
| | c) Serpent | | |
| | d) Rijndael | | |
| (xi) | How many entries are present in each of the S-boxes present in the blowfish algorithm? | 01 | CO3 |
| | a) 256 | | |
| | b) 512 | | |
| | c) 1024 | | |
| | d) 64 | | |
| (xii) | For $p = 11$ and $q = 17$ and choose $e=7$. Apply RSA algorithm where Cipher message=11 and thus find the plain text. | 01 | CO5 |
| | a) 88 | | |
| | b) 122 | | |
| | c) 143 | | |
| | d) 111 | | |

GROUP – B

(Short Answer Type Questions)

(Answer any *three (3)* 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 | CO4 |
| 3. | (a) (Define a symmetric-key cipher. | 2 | CO2 |
| | (b) Are all stream ciphers monoalphabetic? Explain. | 3 | CO3 |

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	CO4
5.	Explain working principle of MD5 with diagrams.	5	CO1
6.	State RSA algorithm with example.	5	CO3

GROUP – C

(Long Answer Type Questions)

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

		Marks	CO No
7.	(a) Assume that ‘n’ is a non-negative integer. (a) Find gcd(2n+1,n) (b) Using the result of (a), find gcd(201,100), gcd(81,40)and gcd(501,250)	5	CO4
	(b) Perform the following operations using reductions first. a. (273 + 147) mod 10 b. (4223 + 17323) mod 10 c. (148 + 14432) mod 12 d. (2467 + 461) mod 12	8	CO4
	(c) What is the modulo operator? What is its application?	2	CO2
8.	(a) Find the result of $(x^5 + x^2 + x) \oplus (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$	6	CO4
	(b) Show how a polynomial can represent ‘n’ bit word.	3	CO2
	(c) For the group $G = \langle Z_4, + \rangle$: Prove that, it is an abelian group	3	CO2
	(d) Show the model and the set of permutation tables for a 3-bit block substitution cipher.	3	CO3
9.	(a) (i) What is the pattern in the cipher text of a one-time pad cipher in each of the following cases? (a) The plaintext is made of n 0’s (b) The plaintext is made of n 1’s (c) The plaintext is made of alternating 0’s and 1’s (d) The plaintext is a random string of bits	8	CO4
	(b) Describe Synchronous Stream Ciphers	4	CO2
	(c) What is Linear Cryptanalysis?	3	CO2
10.	(a) State ElGamal Cryptography method.	5	CO3
	(b) Apply Encryption and Decryption Technique (Consider PT =7)	5	CO4
	(c) Explain SHA algorithm	5	CO3

- | | | | |
|-----|--|-----|-----|
| 11. | Write short notes on any three (3) of the following: | 3x5 | |
| (a) | Pretty Good Privacy (PGP) | 5 | CO4 |
| (b) | S/MIME Cryptographic Algorithms | 5 | CO4 |
| (c) | Different approaches to attack the RSA algorithm | 5 | CO3 |
| (d) | Elliptic Curve Cryptography | 5 | CO2 |
| (e) | Digital signature | 5 | CO3 |