GURU NANAK INSTITUTE OF TECHNOLOGY

An Autonomous Institute under MAKAUT

2020-2021

NETWORK SECURITY & CRYPTOGRAPHY

MCAE505A

TIME ALLOTTED: 3 HOURS **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**

			Marks	CO No
1.	(i)	Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not a) Authenticated b) Joined c)Submit d) Separate	1	CO1
	(ii)	An asymmetric-key (or public-key) cipher uses a) 1 Key b) 2 Key c) 3 Key d) 4 Key	1	CO4
	(iii)	Advanced Encryption Standard (AES), has three different configurations with respect to number of rounds and a)Data Size b) Round Size c) Key Size d) Encryption Size	1	CO2
	(iv)	A transposition cipher reorders (permutes) symbols in a a) block of packets b) block of slots c) block of signals d) block of symbols	1	CO4
	(v)	What are MD4 and MD5? a) Symmetric Encryption Algorithms b) Asymmetric encryption Algorithms c) Hashing algorithms d) Digital certificates	1	CO4
	(vi)	TDES means: a) Triple digital encryption standard b) Triangular data encryption standard c) Triple data encryption standard d) Triangular digital encryption standard	1	CO3

	(vii)	If an attacker stole a password file that contained one- way encrypted passwords, what type of an attack would he/she perform to find the encrypted password? a) Man-in-the middle attack b)Birthday attack c) Denial of service attack d)Dictionary attack	1	CO4
	(viii)	Masquerade attack is another name of: a) Virus attack b) Spoofing c) DOS attack d) Trojan Horse	1	CO3
	(ix)	Block cipher processes a) 1000 bits at a time b) One-bit block of data at a time c) both a and b d) None of the above	1	CO4
	(x)	What is an advantage of RSA over DSS? a) It can provide digital signature and encryption functionality b) It uses fewer resources and encrypts quicker because it uses symmetric keys c)It is a block cipher versus a stream cipher d) It employs a one-time encryption pad	1	CO3
	(xi)	SHA – 1 is similar to: a) RSA b)DES c) MD5 d) Rijndael	1	CO3
	(xii)	Kerberos is an authentication scheme that can be used to implement a) Public key cryptography b) Digital Signature c) Hash function d) Single sign on	1	CO5

GROUP – B
(Short Answer Type Questions)

Answer any ***three***from the following:**3×5=15**

			Marks	**CO**
2.	(a)	What are the principles of security?	3	CO3
	(b)	What is off-line and on-line password guessing?	2	CO4
3.	(a)	What are the possible attacks on Computers and network systems?	4	CO5
	(b)	What is tunnel mode?	1	CO3
4.	(a)	Define Authentication Tokens.	3	CO3

	(b)	What is dictionary attack?	2	CO2
5.	(a)	Give a short description on Simple Columnar Transposition Technique.	4	CO2
	(b)	What is Firewall?	1	CO4
6.	(a)	Discuss the Diffie-Hellman Key Exchange Algorithm.	5	CO2

GROUP – C
(Long Answer Type Questions)

Answer any ***three***from the following:**3×15=45**

			Marks	CO No
7.	(a)	Define Monoalphabetic cipher.	2	CO4
	(b)	What is Steganography?	2	CO1
	(c)	What is the purpose of S-boxes in DES?	3	CO5
	(d)	Discuss the advantages of AES over DES.	3	CO2
	(e)	Write a small description on Triple DES approach.	5	CO5
8.	(a)	What is Digital Signature?	2	CO2
	(b)	What is Message Digest?	2	CO5
	(c)	What are the requirements of message digest?	3	CO5
	(d)	What is birthday attack?	1	CO3
	(e)	Describe the working principles of MD5.	7	CO2
9.	(a)	What are the components of a Virus?	3	CO3
	(b)	Discuss the four phases in the life time of a virus?	4	CO5
	(c)	What is firewall and what are its limitations?	2	CO4
	(d)	Discuss any three types of Firewall?	6	CO2
10.	(a)	Explain the operation of DES algorithm using diagram.	7	CO4
	(b)	What is the strength of DES algorithm?	2	CO2
	(c)	Discuss different transposition techniques to convert a plain text message into cipher text.	6	CO2
11.	(a)	What are the functions provided by S/MIME? Explain in detail.	4	CO5
	(b)	Write the RSA algorithm for Encryption and Decryption. Given p=3, q=11, e=7 & m=5,perform RSA encryption and decryption.	8	CO5
	(c)	Explain the Electronic Code Block (ECB) encryption mode which allows block ciphers to provide confidentiality for message of arbitrary length.	3	CO4