GURU NANAK INSTITUTE OF TECHNOLOGY
An Autonomous Institute under MAKAUT
2022
CRYPTOGRAPHY AND NETWORK SECURITY
IT702A

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)	The principle of ..... ensures that only the sender and the intended recipient(s) have access to the contents of a message. a) authentication b) confidentiality c) integrity d) None of these	1	CO1
(ii)	The Cryptography can provide a) Entity authentication. b) Non repudiation of messages. c) Confidentiality. d) All of these	1	CO1
(iii)	The process of transforming plain text to unreadable text is known as a) Decryption b) Encryption c) Network Security d) Information Hiding	1	CO1
(iv)	While creating an envelope, we encrypt the ..... with the..... a) sender's private key, one time session key. b) receiver's public key, one time session key. c) one time session key, sender's private key. d) one time session key, receiver's public key.	1	CO3
(v)	RSA stands for a) Rivest, Shamir, Adleman. b) Roger, Shamir, Adrian. c) Robert, Shamir, Anthoney d) Rivest, Shaw, Adleman	1	CO2

(vi)	Which one of the following algorithms does not use in asymmetric-key cryptography? a) RSA algorithm. b) Diffie-Hellman algorithm. c) Electronic Code Book algorithm. d) None of these mentioned above.	1	CO2
(vii)	DoS attacks is caused by a) Alternation. b) Authentication. c) Fabrication. d) Replay attacks.	1	CO4
(viii)	Caesar Cipher is an example of a) Substitution Cipher. b) Transposition Cipher. c) Substitution as well as Transposition Cipher. d) None of these	1	CO4
(ix)	For RSA to work, the value of P must be less than the value of a) p b) q c) n d) r	1	CO2, CO4
(x)	Triple-DES has _____ keys. a) 1 b) 2 c) 5 d) 4	1	CO2
(xi)	In asymmetric key cryptography, the private key is kept by a) Sender. b) Receiver. c) Sender and receiver. d) All the connected devices to the network.	1	CO3
(xii)	Cryptanalysis is used a) to find some insecurity in a cryptographic scheme. b) to increase the speed. c) to encrypt the data. d) None of these	1	CO2

GROUP – B
(Short Answer Type Questions)
(Answer any *three* of the following) **3 X 5 = 15**

		Marks	CO No
2. a)	What is Brute force attack?	2	CO3
b)	How is key wrapping useful?	3	CO2
3. a)	What is the difference between MAC and Message Digest?	2	CO2
b)	What is IP sniffing and IP spoofing?	3	CO2
4. a)	What is Triple DEA?	2	CO3, CO4
b)	Why DEA is more secure than DES?	3	CO3, CO4
5.	Explain the Diffie-Hellman key exchange algorithm?	5	CO3
6.	Briefly describe the Alert protocol and Record protocol in SSL.	5	CO3

GROUP – C
(Long Answer Type Questions)
(Answer any *three* of the following) **3 x 15 = 45**

		Marks	CO No
7. a)	List the approaches for the intrusion detection?	5	CO3
b)	Explain firewall design principles, characteristics and types of firewalls.	10	CO3
8. a)	What are the services provided by IPsec?	5	CO3
b)	Briefly describe IPsec Architecture?	5	CO2
c)	The key 'MONARCHY' apply play fair to plain text "FACTIONALISM" to convert to cipher text at the destination, decrypt the cipher text.	5	CO2
9. a)	What types of attacks may occur on block ciphers?	2	CO3
b)	State and explain how IDEA works.	7	CO2
c)	In a RSA system, the public key of a user is 17 and N = 187. Calculate the private key and public key.	6	CO2
10. a)	What is factorization problem?	2	CO2
b)	How digital signatures can be generated? What does digital signatures provide to a message?	5	CO2 CO3
c)	How does certificate-based authentication work?	8	CO3 CO4
11. a)	What are the issues with smart cards? How are these issues solved?	7	CO3, CO4
b)	Write short note on DMZ Network.	5	CO4
c)	What are the different security services provided by PGP?	3	CO3