GURU NANAK INSTITUTE OF TECHNOLOGY
An Autonomous Institute under MAKAUT
2021
CRYPTOGRAPHY AND NETWORK SECURITY
IT801B

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*** 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)	RSA..... be used for Digital Signatures a) Must not b) cannot c) Can d) should not.	1	CO1
(iii)	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
(iv)	DOS attacks are caused by a) Alternation b) authentication c) Fabrication d) replay attacks.	1	CO4
(v)	DES encrypts blocks of..... bits a) 32 b) 56 c) 64 d) 128	1	CO2

(vi)	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
(vi)	Which one of the following algorithm is not used in asymmetric-key cryptography? a) RSA algorithm b) Diffie-hellman algorithm c) electronic code book algorithm d) none of the mentioned	1	CO2
(vii)	Cryptographic hash function takes an arbitrary block of data and returns a) fixed size bit string b) variable size bit string c) both (a) and (b) d) none of the mentioned	1	CO2
(viii)	In MD-5 the length of the message digest is a) 160 b) 128 c) 64 d) 54	1	CO1
(ix)	We require..... to verify digital signature. a) sender's private key b) receiver's private key c) sender and receiver's public key d) all the connected devices to the network	1	CO1
(x)	RC4 is an example of a) hash algorithm b) stream cipher c) block cipher d) none of these.	1	CO1
(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)	In Asymmetric-Key Cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is a) Short b) Long c) Flat d) Thin	1	CO2, CO 4

GROUP – B
(Short Answer Type Questions)

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

		Marks	CO No
2. a)	What is Brute force attack?	3	CO3
2. b)	What is Man-in-the Middle attack?	2	CO3
3.a)	Explain PGP ?	3	CO2
3. b)	What is the difference between MAC and Message Digest	2	CO2
4.a)	Explain DOS attack.	2	CO3
4.b)	What is IP sniffing and IP spoofing?	3	CO2
5	Explain Diffie-Hellman key exchange algorithm?	5	CO3
6.a)	What are the typical contents of Digital Certificate?	2	CO4
6.b)	Discuss deffi-hellman Key exchange protocol.	3	CO4

GROUP – C
(Long Answer Type Questions)

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

		Marks	CO No
7. a)	What is the difference between stream cipher and block cipher?	3	CO3
7. b)	What types of attacks may occur on block ciphers?	2	CO3
7. c)	Write the key generation method for DES?	5	CO3
7.d)	What is the difference between MAC and Message Digest?	5	CO3
8.a)	Write down RSA algorithm?	5	CO3
8.b)	In a RSA system, the public key of a user is 17 and N = 187. Calculate the private key and public key?	5	CO2
8.c)	Convert plain text to cipher test using play fair method. The key is ‘MONARCHY' and the plain text "FACTIONALISM”	5	CO2
9.a)	List the approaches for the intrusion detection?	5	CO3
9.b)	Explain firewall design principles, characteristics and types of firewalls.	10	CO3
10.a)	What are the services provided by IPSec?	5	CO3
10.b)	Briefly describe IPsec Architecture?	5	CO2
10.c)	What are the different protocols associated with SSL?	5	CO3
11. a)	How does clear text password authentication work?	8	CO2
11.b)	What are the problems associated with clear text password?	4	CO2
11.c)	What are the differences between authentication andauthorization?	3	CO2