PRIYADARSHINI COLLEGE OF ENGINEERING, NAGPUR

Department: Computer Technology | Semester: VII | Section: A and B

CAT-II (2023-24)

Subject : Cryptography and Network Security | Subject Code : BTCT701T

Duration : 1.5Hrs | Max. Marks : 35

Note:
1) All questions are compulsory.
2) All questions carry marks as indicated.

			Questions	Marks	CO	BL
Q.1	A	I	Identify the value of φ(221)? a) 194 b) 192 c) 208 d) 113	1M	CO3	I
		II	Extended Euclid's algorithm is used for finding_____ a) GCD of two numbers b) GCD of more than three numbers c) LCM of two numbers d) Both a and c	1M	CO3	I
	B		Explain in detail about Euler's Totient function?	5M	CO3	II
	C		Illustrate the working RSA algorithm with suitable example.	7M	CO3	III
			OR			
Q.2	A	I	A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statement is TRUE? a) Sender encrypts using receiver's public key b) Sender encrypts using his own public key c) Receiver decrypts using sender's public key d) Receiver decrypts using own public key	1M	CO3	I
		II	Which of the following is not public key Distribution means_____? a) Public key certificates b) Hashing Certificates c) Publicly available directories d) Public Key authority	1M	CO3	I
	B		In public key system using RSA you intercept the cipher text C = 10 sent to the user whose public key is e = 5, n = 35, what is the plaintext M?	5M	CO3	III
	C		Explain in detail about the working of Diffie-Hellman key exchange algorithm.	7M	CO3	II
Q.3	A	I	Which of the following is not an element/field of the X.509 certificates? a) Issuer Name b) Serial Modifier c) Issuer unique Identifier d) Signature	1M	CO5	I
		II	Digital certificates are described using the _____ format. a) X.508 b) X.509 c) X.510 d) X.409	1M	CO5	I
	B		Explain MD5 Message Digest Algorithm.	5M	CO5	II
	C		Explain the Hash Functions and their Security.	7M	CO5	II
			OR			

Q.4	A	I	When a hash function is used to provide message authentication, the hash function value is referred to as _____	1M	CO5	I
			a) key code c) keyed hash function	b) message digest d) message key hash function			
		II	Message authentication code is also known as _____	1M	CO5	I
			a) key code c) keyed hash function	b) tag d) message key hash function			
	B		Explain the concept of Kerberos.	5M	CO5	II
	C		Explain in detail about X.509 directory authentication service.	7M	CO5	II
Q.5	A	I	A packet filter firewall filters at _____	1M	CO6	I
			a) Physical Layer c) Network Layer	b) Data Link Layer d) Application Layer			
		II	What is the major drawback of anomaly detection IDS?	1M	CO6	I
			a) These are very slow at detection c) It doesn't detect novel attacks	b) It generates many false alarms d) None of the mentioned			
	B		Explain Application Gateway firewall.	5M	CO6	II

OR

Q.6	A	I	What are strengths of Network based IDS?	1M	CO6	I
			a) Cost of ownership reduced b) Malicious intent detection c) Real time detection and response d) All of the mentioned				
		II	Network layer firewall works as a _____	1M	CO6	I
			a) Frame Filter c) Content Filter	b) Packet Filter d) Virus Filter			
	B		Explain in detail about SQL injection?	5M	CO6	II

********* **Best of Luck** **********