University of Mumbai			
Examination 2020 under cluster 4 (PCE)			
Program: BE Computer Engineering			
Curriculum Scheme: Rev2012			
Examination: BE Semester VII			
Course Code: CPC702 and Course Name: Cryptography & System Security			
Time: 1 hour		Max. Marks: 50	
Q. No	Q=QUESTIO	question_description	question_type
	A=ANSWER		answer_isright
1	Q	What is the name of the action that a small change in eithe	M
	A	Avalanche Effect	1
	A	Repudiation	0
	A	Confusion	0
	A	Diffusion	0
2	Q	ECB and CBC are belong to _____ ciphers technique	M
	A	Block cipher	1
	A	Stream cipher	0
	A	field	0
	A	Key	0
3	Q	_____ is the first step in DES.	M
	A	Expansion permutation	0
	A	Key transformation.	1
	A	S-box substitution.	0
	A	S-box substitution.	0
4	Q	In Message Integrity, SHA-l hash algorithms create an N-l	M
	A	512 Bit Blocks	1
	A	1024 bit Block	0
	A	2048 bits Block	0
	A	256 bits block	0
5	Q	ACL stands for _____	M
	A	Access Condition List	0
	A	Anti-Control List	0
	A	Access Control Logs	0
	A	Access Control List	1
6	Q	What is Session Hijacking?	M
	A	assuming the role of a user through the compromise of phy	0
	A	an attack that aims at stealing a legitimate session and pos	1

	A	only web applications and is specific to stealing session ID	0
	A	assuming the role of a user through the compromise of phy	0
7	Q	Database of web application might get distroy through __	M
	A	Session Hijacking	0
	A	DOS	0
	A	SQL Injection	1
	A	Network Sniffing	0
8	Q	The three concepts that form what is often referred to as th	M
	A	Confidentiality, Integrity, Authentication	0
	A	Confidentiality, Integrity, Access control	0
	A	Communication, Information and Authenticity	0
	A	Confidentiality, Integrity and Availability	1
9	Q	Vigenere cipher is an example of	M
	A	Polyalphabetic cipher	1
	A	Caesar cipher	0
	A	Mono alphabetic cipher	0
	A	Product cipher	0
10	Q	In Which Cipher, the same key is used by both the sender	M
	A	Symmetric-key	1
	A	Asymmetric-key	0
	A	Public Key Cryptosystem	0
	A	Key exchange System	0
11	Q	What is the minimum number of cryptographic keys requi	M
	A	One	1
	A	Two	0
	A	Three	0
	A	Four	0
12	Q	A MAC Provides the Security Services such as	M
	A	Message Integrity and Authentication	1
	A	Message Confidentiality and Authentication	0
	A	Message Authentication and Non repudiation	0
	A	Message Confidentiality and Non Repudiation	0
13	Q	MD5 is a widely used hash function for producing hash va	M
	A	256 bits	0
	A	160 bits	0
	A	128 bits	1
	A	191 bits	0

14	Q	Entity Authentication is used to protect against which Atta	M
	A	Session Hijacking	0
	A	Replay Attack	0
	A	Impersonation	1
	A	Identity Theft	0
15	Q	Alice and Bob wish to communicate using symmetric cryp	M
	A	AES	0
	A	DES	0
	A	Diffie Hellman	1
	A	RSA	0
16	Q	A program that monitors and analyzes network traffic	M
	A	Firewalls	0
	A	Honeypots	0
	A	Intrusion Detection Systems	0
	A	Sniffers	1
17	Q	A type of attack where the attackers attempt to prevent leg	M
	A	Packet Sniffing	0
	A	IP Spoofing	0
	A	Denial of Service	1
	A	ICMP Flood	0
18	Q	In which mode, IPSec does not protect the IP header.	M
	A	Transport Mode	1
	A	Tunnel Mode	0
	A	Neither Transport nor Tunnel Mode	0
	A	End to End Mode	0
19	Q	In RSA Cryptosystem, Whose keys are used for Encryptio	M
	A	Receiver's Public key and Private Key respectively	1
	A	Sender's Public key and Private Key respectively	0
	A	Sender's Private Key and Public key respectively	0
	A	Receiver's Private Key and Public key respectively	0
20	Q	The process of writing the text as rows and read it as colu	M
	A	Vernam cipher	0
	A	Caesar cipher	0
	A	Transposition columnar cipher	1
	A	Homophonic substitution cipher	0
21	Q	_____ are people who are caught and convicted of cor	M
	A	Attackers	0

	A	Computer Criminals	1
	A	Terrorists	0
	A	Robbers	0
22	Q	Which of the following can be chosen as a key range in th	M
	A	Key Range is in Z26 Group	1
	A	Key Range is not in Z26	0
	A	Key range is Z26 *	0
	A	Key range is outside Z26 group	0
23	Q	Certificate can be Revoked by the Certification Authority	M
	A	The CA's Private Key may have been Compromised	1
	A	The CA's Public Key may have been Compromised	0
	A	The User's Public Key may have been Compromised	0
	A	CA willingly revoking the certificate for any user who are	0
24	Q	Which of the following differentiates a virus from a worm	M
	A	a woem requires user interation to infect a machine	0
	A	a worm can infect multiple machines	0
	A	a virus requires user interaction to infect a machine	1
	A	a virus can only infect a single machine	0
25	Q	Password, PIN numbers, passphrases, a secret handshake,	M
	A	Something the user knows	1
	A	Something the user has	0
	A	Something the user is	0
	A	Pre-User protection	0
