Program: BE Information Technology
Curriculum Scheme: Revised 2016
Examination: Third Year Semester V
Course Code: ITC504 and Course Name: Cryptography & Network Security
Time: 1 hour Max. Marks: 50

Note :- All the Questions are compulsory and carry equal marks

Q.	Question Statement	OPTION A:	OPTION B:	OPTION C:	OPTION D:
1	Which is a passive attack ?	Traffic Analysis	Replaying	Denial of Service	Reputation
2	Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.	Non-repudiation	Confidentiality	Integrity	Availability
3	An…….algorithm transforms plaintext to ciphertext	Decryption	Encryption	Key	Cipher text
4	Cryptanalysis is used _____	to find some insecurity in a cryptographic scheme	to increase the speed	to encrypt the data	to make new ciphers
5	Hill cipher requires prerequisite knowledge of?	Integration	Differentiation	matrix algebra	Differential equation
6	In RSA, if p=17, q=11, then, what is phi(n)?	189	187	160	161
7	In El-Gamal cryptosystem, if q=19, alpha = 10, what is the public key?	[19, 10, 3]	[19, 10, 2]	[19,10,5]	[19,3,5]
8	In the RSA algorithm, we select 2 random large values ‘p’ and ‘q’. Which of the following is the property of ‘p’ and ‘q’?	p and q should be divisible by phi(n)	p and q should be co-prime	p and q should be prime	p/q should give no remainder
9	How many keys does the Triple DES algorithm use?	2	3	2 or 3	3 or 4
10	……is the process of verifying who a user is, while …….is the process of verifying what they have access to.	Authentication, Authorization	Authorization , Access Control	Access Control, Authorization	Authorization, Authentication

11	To make revocation very effective, the ……certificate revocation list has been introduced.	Alpha	Beta	Delta	Gamma
12	…… is Hash Function Properties which measures how difficult to devise a message which hashes to the known digest and its message	duplication	Second preimage resistant	Collision resistant	Preimage resistant
13	For SHA-1: if the user needs to seek out the 2 messages having identical message digest then user would need to perform…….	2^80 operations	2^60 operations	2^70 operations	2^50 operations
14	In the MD5 the message is divided into blocks of size …….bits for the hash computing	256	512	1024	160
15	Define Non-Repudiation	It means that sender and receiver expect privacy	It means that the data received at the receiver is exactly same as sent.	It means that a sender must not be able to deny sending a message that he sent	It means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
16	In El Gamal cryptosystem, given the prime p=31. Choose e1= first primitive root of p and d=10, calculate e2	24	36	25	62
17	Digital signature certification is needed by an independent authority because	private key claimed by a sender may not be actually his	it is safe	it gives confidence to a business	the authority checks and assures customers that the public key indeed belongs to the business which claims its ownership
18	In which attack the user gets redirects queries to a DNS because of override of system's TCP/IP settings?	DNS mal-functioning	DNS cracking	DNS redirecting	DNS hijacking

19	How can an attacker get the information of all the services running on the target system?	Packet Sniffing	ARP spoofing	port scanning	IP spoofing
20	Which is not a type of port scanning technique	TCP scan	SYN scan	Idle Scan	Rapid Scan
21	What is the main advantage of honeypot	Improves security	not good in terms of security	easy implementation	A honeypot once attacked can be used to attack other systems.
22	Which of them is not a step in reconnaissance?	Check for live systems	Check for open ports	Identifying the malware in the system	Identifying of services
23	Three headed dog of identity is known as	X.509	IPSec	Public-key infrastructure	Kerberos
24	Kerboros consists of__	Authorization Server	Client Server	Authentication server	Mail server
25	Which is not a Header Fields defined in MIME	Content-Log	Content-Type	Content-Transfer-Encoding	Content-Description