University Exam DECEMBER 2020

MCQ Section

Subject: Cryptography & Network Security Course Code: ITC504
Semester: V Branch: Information Technology
Year : Third Year M arks :40

1] All questions are Compulsory
2] Assume suitable data wherever required.

Q1. Attempt all questions. [20*2=40M]

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	An...................algorithm transforms plaintext to ciphertext	Decryption	Encryption	Key	Cipher text
3	Cryptanalysis is used ___________	to find some insecurity in a cryptographic scheme	to increase the speed	to encrypt the data	to make new ciphers
4	Hill cipher requires prerequisite knowledge of?	Integration	Differentiation	matrix algebra	Differential equation
5	In RSA, if p=17, q=11, then, what is phi(n)?	189	187	160	161
6	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]
7	How many keys does the Triple DES algorithm use?	2	3	2 or 3	3 or 4
8	……………….. 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
9	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
10	In the MD5 the message is divided into blocks of size ……….bits for the hash computing	256	512	1024	160

11	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.
12	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
13	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
14	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
15	How can an attacker get the information of all the services running on the target system?	Packet Sniffing	ARP spoofing	port scanning	IP spoofing
16	Which is not a type of port scanning technique	TCP scan	SYN scan	Idle Scan	Rapid Scan
17	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.
18	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
19	Kerboros consists of__	Authorization Server	Client Server	Authentication server	Mail server
20	Which is not a Header Fields defined in MIME	Content-Log	Content-Type	Content-Transfer-Encoding	Content-Description

Descriptive Section

Attempt all questions. [40M]

Q2. Write Short note on (Any 4 each for 5 Marks)

A) Security Services
B) RC5 Algorithm
C) HMAC
D) Needham Schroeder Authentication Protocol
E) Network Based IDS
F) PGP

Q3. Attempt the following (Any 2 each for 10 Marks)

A) Using Affine cipher, encrypt the Plaintext ‘SECURITY’ with key pair (5, 2)
B) Explain in details DES Algorithm and Compare with AES.
C) Explain TCP/IP Layer wise vulnerabilities and types of DOS attacks