University of Mumbai

Examination June 2021

Examinations Commencing from 1st June 2021

Program: **Computer Engineering**

Curriculum Scheme: Rev2016

Examination: TE Semester VI

Course Code: **CSC604** and Course Name: **Cryptography and System Security**

Time: 2 hour Max. Marks: 80

==========

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	_____ defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.
Option A:	X.800
Option B:	X.809
Option C:	X.832
Option D:	X.802
2.	_____are fundamental to a number of public-key algorithms, including and the digital signature algorithm (DSA).
Option A:	Discrete logarithms
Option B:	Chinese remainder theorem
Option C:	Fermat's theorem
Option D:	Miller and Rabin algorithm
3.	Plain text message is: "meet me after the toga party" with a rail fence of depth 2. Compute cipher text.
Option A:	MEMATRHTGPRYETEFETEOAAT
Option B:	MEMATRHTGPRYETEFETFOAAT
Option C:	MEMATRHTHPRYETEFETEOAAT
Option D:	MEMATRHTGPRYETEFFTEOAOT
4.	In_____ mode, the same plaintext value will always result in the same cipher text value.
Option A:	Cipher Block Chaining
Option B:	Cipher Feedback
Option C:	Electronic code book
Option D:	Output Feedback
5.	DES encrypting the plaintext as block of _____ bits.
Option A:	64
Option B:	56
Option C:	128
Option D:	32
6.	_____ is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications.
Option A:	AES

Option B:	RSA
Option C:	MD5
Option D:	RC5
7.	The number of rounds in RC5 can range from 0 to _____
Option A:	127
Option B:	63
Option C:	31
Option D:	255
8.	How many rounds does the AES-192 perform?
Option A:	10
Option B:	14
Option C:	16
Option D:	12
9.	For the Knapsack: {1 6 8 15 24}, Find the cipher text value for the plain text 10011.
Option A:	40
Option B:	15
Option C:	14
Option D:	39
10.	Which of the following is not possible through hash value?
Option A:	Password check
Option B:	Data integrity check
Option C:	Data retrieval
Option D:	Digital signature
11.	Which of the following is not an element/field of the X.509 certificates?
Option A:	Issuer Name
Option B:	Serial Modifier
Option C:	Issue unique identifier
Option D:	Signature
12.	_____ is responsible for distributing keys to pairs of users (hosts, processes, applications) as needed
Option A:	Key distribution center
Option B:	Key analysis center
Option C:	UKey storing center
Option D:	HKey storing center
13.	A digital certificate system is _____.
Option A:	uses third-party CAs to validate a user's identity
Option B:	uses digital signatures to validate a user's identity
Option C:	uses tokens to validate a user's identity
Option D:	are used primarily by individuals for personal correspondence
14.	Hashed message is signed by a sender using
Option A:	His public key
Option B:	His private key

Option C:	Receivers public key
Option D:	Receivers private key
15.	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
Option A:	Authenticated
Option B:	Joined
Option C:	Submit
Option D:	Separate
16.	Which of the following does authorization aim to accomplish?.
Option A:	Restrict what operations/data the user can access
Option B:	Determine if the user is an attacker
Option C:	Flag the user if he/she misbehaves
Option D:	Determine who the user is
17.	_____ operates in the transport mode or the tunnel mode.
Option A:	IPSec
Option B:	SSL
Option C:	PGP
Option D:	BGP
18.	When a hash function is used to provide message authentication, the hash function value is referred to as
Option A:	Message Field
Option B:	Message Digest
Option C:	Message Score
Option D:	Message Leap
19.	Which of the following tool would NOT be useful in figuring out what spyware or viruses could be installed on a client's computer?
Option A:	Wireshark
Option B:	Malware Bytes
Option C:	HighjackThis
Option D:	HitmanPro
20.	What is honey pot attack?
Option A:	dummy device put into the network to attract attackers
Option B:	single line threat
Option C:	Ip spoofing bypass
Option D:	recognition attack

Q2	**Solve any Two** **10 marks each**
A	Explain Security Services and Mechanisms in detail. Explain the relationship between them.
B	What is meant by the Diffie-Hellman key exchange algorithm? Explain with example.
C	Describe HMAC algorithm. Comment on the security of HMAC.

Q3	**Solve any Two** **10 marks each**
A	Describe signing and verification in Digital Signature Algorithm.

B	Explain any 2 ways to classify Intrusion Detection Systems.
C	Explain Man-in-the-Middle and Flooding attacks concept in detail.