University of Mumbai
Examination 2020

Examinations Commencing from 7th January 2021 to 20th January 2021

Program: Information Technology Engineering

Curriculum Scheme: Rev 2016

Examination: T.E. Semester V

Course Code: ITC 504 and Course Name: CNS

Time: 2 hour Max. Marks: 80

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
Q1.	A Digital Signature is
Option A:	a bit string giving identity of the correspondent
Option B:	a unique identification of the sender
Option C:	an authentication of an electronic record by tying it uniquely to a key only a sender knows
Option D:	an encrypted signature of the sender
Q2.	Encryption and decryption provide secrecy, or confidentiality, but not
Option A:	Authentication
Option B:	Integrity
Option C:	Privacy
Option D:	All of the above
Q3.	A (n) _______ function creates a message digest out of a message
Option A:	hash
Option B:	encryption
Option C:	decryption
Option D:	none of the above
Q4.	____________are very crucial for success of RSA digital signature scheme.
Option A:	Integers
Option B:	Negative number
Option C:	Fraction
Option D:	Prime numbers
Q5.	The Elgamal signature scheme involves the use of the
Option A:	public key for encryption and the private key for decryption
Option B:	private key for encryption and the public key for decryption
Option C:	private key for encryption and decryption
Option D:	public key for encryption and decryption
Q6.	A firewall is a _______security system:
Option A:	File
Option B:	Program
Option C:	Network
Option D:	None of These
Q7.	Firewalls are often categorized as:

Option A:	Network Firewalls
Option B:	Either Network firewalls or Host based firewalls
Option C:	Host Based Firewalls
Option D:	None of These
Q8.	Which among the following is correct characteristics about proxy server:
Option A:	A proxy server may act as a firewall by responding to input packets in the manner of an application while blocking other packets.
Option B:	A proxy server is a gateway from one network to another for a specific network application
Option C:	It performs its tasks or functions as a proxy on behalf of the network user;
Option D:	All of the Above
Q9.	Which of the following is a feature of Kerberos?
Option A:	It does not require time synchronization
Option B:	It provides centralized authentication for remote access servers
Option C:	It uses tickets
Option D:	It uses SAML for SSO
Q10.	__________ operates in the transport mode or the tunnel mode.
Option A:	IPSec
Option B:	SSL
Option C:	PGP
Option D:	none of the above
Q11.	_______ is actually an IETF version of______.
Option A:	TLS; TSS
Option B:	SSL; TLS
Option C:	TSL; SSL
Option D:	SSL; SLT
Q12.	The combination of key exchange,hash, and encryption algorithms defines a _________ for each SSL session.
Option A:	list of protocols
Option B:	cipher suite
Option C:	list of keys
Option D:	none of the above
Q13.	If the same key is used to encrypt and decrypt a message, this is known as?
Option A:	Symmetric encryption
Option B:	Asymmetric encryption
Option C:	Encryption doesn't exist!
Option D:	Same-key encryption
Q14.	Information that is readable without performing any cryptographic operations.
Option A:	cryptography
Option B:	plaintext
Option C:	encryption
Option D:	decryption
Q15.	The DES Algorithm Cipher System consists of _____________rounds (iterations)

	each with a round key
Option A:	12
Option B:	18
Option C:	9
Option D:	16
Q16.	SHA-1 produces a hash value of
Option A:	256 bits
Option B:	180 bits
Option C:	160 bits
Option D:	128 bits
Q17.	In SHA-512, the message is divided into blocks of size ___ bits for the hash computation.
Option A:	1024
Option B:	512
Option C:	256
Option D:	1248
Q18.	What is the maximum length of the message (in bits) that can be taken by SHA-512?
Option A:	2^64
Option B:	2^256
Option C:	2^192
Option D:	2^128
Q19.	What is the value of ipad in the HMAC structure?
Option A:	00111110
Option B:	10110110
Option C:	00110010
Option D:	01110110
Q20.	What is the value of opad in the HMAC structure?
Option A:	00111110
Option B:	00110010
Option C:	10110110
Option D:	01011100

Q2.	**Solve any Two Questions out of Three** **10 marks each**
A	*What are block cipher modes? Explain any 2 in detail.*
B	*Explain Kerberos Protocol in detail.*
C	Perform encryption and decryption using RSA algorithm with p = 7, q = 11, e = 17 and M = 8.

Q3.	
A	**Solve any Two** **5 marks each**
i.	*What is significance of digital signature on a certificate? Justify.*
ii.	*Write short note on Email Security.*
iii.	*Write short note on Honeypots.*
B	**Solve any One** **10 marks each**
i.	*Explain Diffie Hellman Key Exchange Algorithm with suitable example.*
ii.	*What is firewall? Explain different types of firewalls with their advantages.*