University of Mumbai
Examination 2020

Program: Information Technology Engineering
Curriculum Scheme: Rev. 2016
Examination: Third Year Semester V
Course Code: ITC 504 and Course Name: CNS

Time: 1 hour Max. Marks: 50

==========

For the students:- 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
Q21.	The DES algorithm has a initial key length of
Option A:	128 bits
Option B:	32 bits
Option C:	64 bits
Option D:	16 bits
Q22.	In the DES algorithm the round key is _____ bit and the Round Input is _____bits.
Option A:	48, 32
Option B:	64,32
Option C:	56, 24
Option D:	32, 32

Q23.	AES uses a _____ bit block size and a key size of _____ bits.
Option A:	128; 128 or 256
Option B:	64; 128 or 192
Option C:	256; 128, 192, or 256
Option D:	128; 128, 192, or 256
Q24.	In AES the 4×4 bytes matrix key is transformed into a keys of size _____
Option A:	32 words
Option B:	64 words
Option C:	44 words
Option D:	54 words
Q25.	For the Knapsack: {1 6 8 15 24}, find the plain text code if the ciphertext is 38.
Option A:	10010
Option B:	01001
Option C:	01110
Option D:	01101