These are sample MCQs to indicate pattern, may or may not appear in examination

University of Mumbai

Online Examination 2020

Program: BE Computer Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester VI

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

Time: 1hour Max. Marks: 50

Q1.	Schnorr signature is a digital signature scheme known for its --------
Option A:	simplicity
Option B:	efficiency
Option C:	generates short signatures
Option D:	keys can be typically 1024 or 2048 bits long

Q2.	A transposition cipher reorders (permutes) symbols in a ____.
Option A:	block of packets
Option B:	block of slots
Option C:	block of signals
Option D:	block of symbols

Q3.	A _____ tries to formulate a web resource occupied or busy its users
Option A:	Phishing attack
Option B:	DoS attack
Option C:	Website attack
Option D:	MiTM attack

Q4.	= 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the ciphe
Option A:	C=80
Option B:	C=92
Option C:	C=56
Option D:	C=23

Q5.	Find feature of kerberos
Option A:	Based on Certificate
Option B:	Ideal for the www
Option C:	uses private key encryption
Option D:	The service is not free

Q6.	t, Shamir, Adleman cryptosystem with p=7 and q=9. Encrypt M=24 to find ciphertext. The C
Option A:	42
Option B:	93
Option C:	114
Option D:	103

Q7.	____ ensures that sensitive information are accessed only by an authorized person
Option A:	Availability
Option B:	Cryptanalysis
Option C:	Confidentiality
Option D:	Integrity

Q8.	Password-based authentication can be divided into two broad categories: _____ and _____.
Option A:	fixed; variable
Option B:	time-stamped; fixed
Option C:	fixed; one-time
Option D:	fixed; two-time

Q9.	What is the expanded key size of AES-192?
Option A:	44 words
Option B:	52 words
Option C:	66 words
Option D:	36 words

Q10.	What is the full-form of CMAC?
Option A:	Code-based MAC
Option B:	Cipher-based MAC
Option C:	Construct-based MAC
Option D:	Collective-based MAC

Q11.	the process of giving individuals different levels of access to system objects based on their i
Option A:	Threat
Option B:	Authorization
Option C:	Authentication
Option D:	Encryption

Q12.	The 4×4 byte matrices in the AES algorithm are called
Option A:	States
Option B:	Words
Option C:	Transitions
Option D:	Permutations

Q13.	Which of these systems use timestamps as an expiration date?
Option A:	Public-Key Certificates
Option B:	Public announcements
Option C:	Publicly available directories
Option D:	Public-Key authority

Q14.	Calculate the number of subkeys required in RC5 for 18 rounds of computation.
Option A:	40
Option B:	36

Option C:	38
Option D:	34

Q15.	The number of unique substitution boxes in DES after the 48 bit XOR operation are
Option A:	8
Option B:	4
Option C:	6
Option D:	12

Q16.	DoS threats to overload a server as it sends a large number of requests requiring resources
Option A:	Network Layer DoS
Option B:	Physical Layer DoS
Option C:	Transport Layer DoS
Option D:	Application Layer DoS

Q17.	__ a weakness in a security system; and ____ = circumstances that have a potential to caus
Option A:	Vulnerability, threat
Option B:	Vulnerability, attack
Option C:	Attack, threat
Option D:	Threat, vulnerability

Q18.	In _____ attack, the attacker doesn't actively take over another user to perform the attack
Option A:	phishing
Option B:	spoofing
Option C:	hijacking
Option D:	vishing

Q19.	Which is not the property of digital signature
Option A:	It must verify the author and the date and the time of the signature
Option B:	it must to authenticate the contents at the time of the signature
Option C:	It must be verifiable by third parties,to resolve disputes.
Option D:	It does protect the two parties against each other

Q20.	_____ means to prove the identity of the entity that tries to access the system's resources.
Option A:	Message authentication
Option B:	Entity authentication
Option C:	Message confidentiality
Option D:	Entity confidentiality

Q21.	If GCD of two numbers is 1, then the two numbers are said to be _____
Option A:	Prime numbers
Option B:	Composite numbers
Option C:	Co-prime numbers
Option D:	Rational numbers

Q22.	Which is not the property of digital signature
Option A:	It must verify the author and the date and the time of the signature
Option B:	it must to authenticate the contents at the time of the signature
Option C:	It must be verifiable by third parties,to resolve disputes.
Option D:	It does protect the two parties against each other

Q23.	the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
Option A:	Scaling of the existing bits
Option B:	Duplication of the existing bits
Option C:	Addition of zero
Option D:	Addition of ones

Q24.	DNS stands for _____
Option A:	Data Name System
Option B:	Domain Name Server
Option C:	Domain Name System
Option D:	Domain's Naming System

Q25.	ın attack in which _____ code is inserted into strings that are later passed to an instan
Option A:	malicious
Option B:	redundant
Option C:	clean
Option D:	non malicious