

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 2012

Examination: Final Year Semester VII

Course Code:CPC702 and Course Name:Cryptography and System Security

Time: 1hour

Max. Marks: 50

Note to the students:- All the Questions are compulsory and carry equal marks .

Q1.	In cryptography, the order of the letters in a message is rearranged by _____
Option A:	transpositional ciphers
Option B:	substitution ciphers
Option C:	quadratic ciphers
Option D:	Binary ciphers

Q2.	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

Q3.	In _____ attacks, the attacker manages to get an application to execute an SQL query created by the attacker.
Option A:	SQL injection
Option B:	SQL
Option C:	Direct
Option D:	Application

Q4.	In RSA, $\Phi(n) =$ _____ in terms of p and q.
Option A:	$(p)/(q)$
Option B:	$(p)(q)$
Option C:	$(p-1)(q-1)$

Option D:	$(p+1)(q+1)$
-----------	--------------

Q5.	What are the characteristics of anomaly based IDS?
Option A:	It models the normal usage of network as a noise characterization
Option B:	It doesn't detect novel attacks
Option C:	Anything distinct from the noise is not assumed to be intrusion activity
Option D:	It detects based on signature

Q6.	If a single symbol in plaintext is changed, then several or all symbols in ciphertext will also be changed, this property of cipher
Option A:	Diffusion
Option B:	Confusion
Option C:	Fusion
Option D:	Conversion

Q7.	Blowfish encrypts blocks of plaintext which have size
Option A:	256 bits
Option B:	64 bits
Option C:	72 bits
Option D:	128 bits

Q8.	PGP encrypts data by using a block cipher called _____
Option A:	International data encryption algorithm
Option B:	Private data encryption algorithm
Option C:	Internet data encryption algorithm
Option D:	Local data encryption algorithm

Q9.	Snooping threatens which of the goal ?
Option A:	Integrity
Option B:	Confidentiality
Option C:	Availability
Option D:	Consistency

Q10.	Which of the following is not a characteristic of a virus?
------	--

Option A:	Virus destroy and modify user data
Option B:	Virus is a standalone program
Option C:	Virus is a code embedded in a legitimate program
Option D:	Virus cannot be detected

Q11.	IPSec is designed to provide security at the _____
Option A:	Transport layer
Option B:	Network layer
Option C:	Application layer
Option D:	Session layer

Q12.	For $p = 11$ and $q = 19$ and choose $e=17$. Apply RSA algorithm where message=5 and find the cipher text.
Option A:	C=80
Option B:	C=92
Option C:	C=56
Option D:	C=23

Q13.	Confusion hides relationship between ____ and ____.
Option A:	Ciphertext, plaintext
Option B:	Ciphertext, key
Option C:	Plaintext, key
Option D:	plaintext, text,

Q14.	What is trap door?
Option A:	It is trap door in WarGames
Option B:	It is a hole in software left by designer
Option C:	It is a Trojan horse
Option D:	It is a virus which traps and locks user terminal

Q15.	The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key
Option A:	12
Option B:	10
Option C:	16

Option D:	8
-----------	---

Q16.	What is the advantage of the multiplication method?
Option A:	only 2 steps are involved
Option B:	using constant
Option C:	value of m not critical
Option D:	simple multiplication

Q17.	WPA2 is used for security in _____
Option A:	Ethernet
Option B:	Bluetooth
Option C:	Wi-Fi
Option D:	Email

Q18.	In which of the below attack, attacker impersonates somebody else?
Option A:	Masquerading
Option B:	Replaying
Option C:	Repudiation
Option D:	Masking

Q19.	What is the PGP stand for?
Option A:	Permuted Gap Permission
Option B:	Permuted Great Privacy
Option C:	Pretty Good Permission
Option D:	Pretty Good Privacy.

Q20.	What is not an encryption standard?
Option A:	AES
Option B:	TES
Option C:	DES
Option D:	Triple DES

Q21.	Access matrix model for user authentication contains _____
------	--

Option A:	a list of classes
Option B:	a list of sectors
Option C:	a function which returns an object's type
Option D:	a list of cylinders

Q22.	In playfair cipher, Number of characters in plaintext are ___ to number of characters in ciphertext.
Option A:	greater than
Option B:	always equal
Option C:	less than
Option D:	less than or equal

Q23.	What is the average retrieval time when n keys hash to the same slot?
Option A:	$\Theta(n)$
Option B:	$\Theta(n^2)$
Option C:	$\Theta(n \log n)$
Option D:	$\text{Big-Oh}(n^2)$

Q24.	For a client-server authentication, the client requests from the KDC a _____ for access to a specific asset.
Option A:	ticket
Option B:	local
Option C:	token
Option D:	user

Q25.	When an attempt is to make a machine or network resource unavailable to its intended users, the attack is called
Option A:	denial-of-service attack
Option B:	slow read attack
Option C:	spoofed attack
Option D:	starvation attack

