University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: BE Computer Engineering
Curriculum Scheme: Rev2016
Examination: Third Year Semester VI
Course Code: CSC604 and Course Name: Cryptography & System Security
Time: 1 hour Max. Marks: 50

==========

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

Q1.	Confidentiality prevents _____
Option A:	unauthorized creation, modification, or deletion of information
Option B:	Unauthorized disclosure and use of information
Option C:	Unauthorized delay or denial of information
Option D:	Authorised access to the resources
Q2.	If the security of the information is compromised against any action then it is called as what?
Option A:	Security attack
Option B:	Security service
Option C:	Security alert
Option D:	Security mechanism
Q3.	In an asymmetric-key cipher, the receiver uses which key for decrypting the Cipher Text?
Option A:	Public Key
Option B:	Private Key
Option C:	Session Key
Option D:	Both Public and Private Key
Q4.	A public key cipher uses_____
Option A:	1 key
Option B:	2 key
Option C:	3 key
Option D:	4 key
Q5.	ElGamal encryption system belongs to which Encryption Algorithm?
Option A:	Symmetric key encryption algorithm
Option B:	Asymmetric key encryption algorithm
Option C:	Not an encryption algorithm
Option D:	A block cipher method
Q6.	X.509 certificate recommends which cryptographic algorithm?
Option A:	RSA
Option B:	AES
Option C:	DES
Option D:	Elliptic Curve
Q7.	Hashed message is signed by a sender using
Option A:	His public key

Option B:	His private key
Option C:	Receiver's public key
Option D:	Receiver's private key
Q8.	The standard for certificates used on internet is
Option A:	X.25
Option B:	X.301
Option C:	X.409
Option D:	X.509
Q9.	Timestamped Digital Signatures are designed to prevent
Option A:	Replay Attack
Option B:	Chosen plaintext Attack
Option C:	Key only Attack
Option D:	Known plaintext Attack
Q10.	What kind of attacks would be possible on Password Authentication?
Option A:	Eavesdropping and Dictionary Attack
Option B:	Key only Attack and Dictionary Attack
Option C:	Known-message Attack and eavesdropping
Option D:	Chosen Message attack and Key only Attack
Q11.	To provide network connection between the internet and network device _____ firewall is used.
Option A:	Microsoft Firewall
Option B:	CISCO Firewall
Option C:	Hardware Firewall
Option D:	software Firewall
Q12.	Firewall is defined the set of rules to observe the each incoming / outgoing _____ to the network
Option A:	File
Option B:	Email
Option C:	Data Packet
Option D:	Updates
Q13.	Infected computers and other systems within the botnet are called _____
Option A:	Killers
Option B:	Vampires
Option C:	Zombies
Option D:	Gargoyles
Q14.	In Digital Signature, Whose keys are used for Signing and Verifying the Document?
Option A:	Receiver's Public key and Private Key respectively
Option B:	Sender's Public key and Private Key respectively
Option C:	Sender's Private Key and Public key respectively
Option D:	Receiver's Private Key and Public key respectively

Q15.	The secret key between members needs to be created as a _____ key when two members contact KDC.
Option A:	Public Key
Option B:	Private key
Option C:	Session Key
Option D:	Complimentary Key
Q16.	Which cryptographic algorithm is used in CMAC?
Option A:	Triple DES and AES
Option B:	DES
Option C:	RC-4
Option D:	AES
Q17.	A collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level is which of the following?.
Option A:	IPSec
Option B:	SSL
Option C:	PGP
Option D:	SMTP
Q18.	_____ are computer programs that are designed by attackers to gain root or administrative access to your computer.
Option A:	Backdoors
Option B:	Rootkits
Option C:	Malware
Option D:	Anti Adware
Q19.	How do you prevent SQL injection?
Option A:	Escape queries
Option B:	Interrupt requests
Option C:	Merge tables
Option D:	Validate input
Q20.	Which one of the following algorithm is not used in asymmetric-key cryptography?
Option A:	RSA
Option B:	Deffie Hellman
Option C:	Electronic code book
Option D:	DSA
Q21.	Convert the given plaintext **"exam"** into ciphertext using the Additive cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2? (Note: Assign integers from 0 to 25 for the Alphabets A - Z)
Option A:	**zcog**
Option B:	**czgo**
Option C:	**ozcg**

Option D:	**gzco**
Q22.	What is the meaning of the notation "**X<<Y>>**" used in Public Key Infrastructure ?
Option A:	Certificate is issued by the authority Y to an Entity X.
Option B:	Certificate is issued by the authority X to an Entity Y.
Option C:	Certificate of X is included in Y's Certificate
Option D:	Certificate of Y is included in X's Certificate
Q23.	Which of the following statement is true according to the DSS and RSA digital Signature Scheme?
Option A:	Computation of DSS Signature is faster than computation of RSA Signature when using the same **'p'**
Option B:	Computation of DSS Signature is faster than computation of RSA Signature when using the different **'p' value**
Option C:	Computation of DSS Signature is slower than computation of RSA Signature when using the same **'p' value**
Option D:	Computation of RSA Signature is faster than computation of DSS Signature when using the same **'p' value**
Q24.	In ElGamal Digital Signature, how the second signature S2 is computed?
Option A:	S2 = e1 ^ r mod p
Option B:	S2 = (M - dS1) inverse(r) mod (p-1)
Option C:	S2 = (M - dS1) mod (p-1)
Option D:	S2 = (M - dS1) mod p
Q25.	ARP spoofing is commonly used to_____
Option A:	link an attacker’s IP to a legitimate network MAC address
Option B:	link an attacker’s MAC to a legitimate network IP address
Option C:	link an attacker’s URL to a legitimate network IP address
Option D:	link an attacker’s MAC to a legitimate network URL address

University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: BE Computer Engineering
Curriculum Scheme: Rev2016
Examination: Third Year Semester VI
Course Code: CSC604 and Course Name: Cryptography & System Security
Time: 1 hour Max. Marks: 50

==========

Question	Correct Option (Enter either 'A' or 'B' or 'C' or 'D')
Q1.	B
Q2.	A
Q3.	B
Q4	B
Q5	B
Q6	A
Q7	B
Q8.	D
Q9.	A
Q10.	A
Q11.	C
Q12.	C
Q13.	C
Q14.	C
Q15.	C
Q16.	A
Q17.	A
Q18.	B
Q19.	A
Q20.	C
Q21.	D
Q22.	B
Q23.	A
Q24.	B
Q25.	B