University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: TE Information Technology Engineering
Curriculum Scheme: Rev2016
Examination: Third Year Semester V
Course Code: ITC504 and Course Name: Cryptography and Network Security
Time: 1 hour Max. Marks: 50
==========

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

Q1.	Example of passive attack is
Option A:	Masquerade attack
Option B:	playback attack
Option C:	Traffic analysis
Option D:	Denial of service attack
Q2.	In asymmetric key cryptography, the key used by the sender and the receiver is……..
Option A:	Shared
Option B:	Different
Option C:	Secret
Option D:	Same
Q3.	What is the number of possible 3 x 3 affine cipher transformations ?
Option A:	168
Option B:	840
Option C:	1024
Option D:	1344
Q4.	Which key exchange algorithm suffers from man in the middle attack
Option A:	Diffie Hellman

Option B:	AES
Option C:	RSA
Option D:	Knapsack
Q5.	In ElGamal what happens if C1 and C2 are swapped during transition
Option A:	receiver cannot decrypt
Option B:	decryption remains same
Option C:	both will be swapped
Option D:	difficult to decrypt
Q6.	Which Cryptographic system uses C1 = (e1r) mod p and C1 = (e2r x P) mod p at the encryption side?
Option A:	RSA
Option B:	Elgamal
Option C:	Rabin
Option D:	Knapsack
Q7.	What is the expanded key size of AES-192?
Option A:	36 words
Option B:	52 words
Option C:	60 words
Option D:	40 words
Q8.	The expansion P-Box in DES expands ----- bits to ------- bits
Option A:	32 to bits 48 bits
Option B:	48 bits to 56 bits
Option C:	32 bits to 56 bits
Option D:	32 bits to 42 bits

Q9.	MD5 is a widely used hash function for producing hash value of _____
Option A:	256 bits
Option B:	160 bits
Option C:	128 bits
Option D:	191 bits
Q10.	What is the maximum length of the message (in bits) that can be taken by SHA-512?
Option A:	2^128
Option B:	2^256
Option C:	2^64
Option D:	2^192
Q11.	Cryptographic hash function takes an arbitrary length of data and returns
Option A:	Fixed size bit string
Option B:	Variable size bit string
Option C:	Both fixed size bit string and variable size bit string
Option D:	Same size of the data
Q12.	Which of the following field in Digital Certificate is optional?
Option A:	Certificate validity Period
Option B:	Subject's Name
Option C:	Extensions
Option D:	Subject's Public Key information
Q13.	What is the number of round computation steps in the SHA-256 algorithm?

Option A:	80
Option B:	76
Option C:	64
Option D:	70
Q14.	Which system uses a trusted third party interface?
Option A:	Public-Key Certificates
Option B:	Public announcements
Option C:	Publicly available directories
Option D:	Public-Key authority
Q15.	Responsibility of Certification Authority for digital signature is used to authenticate the
Option A:	Hash function used
Option B:	private key of subscribers
Option C:	Public key of subscribers
Option D:	Key used in DES
Q16.	The Firewall protecting a Target Server can become exhausted due to
Option A:	Network flooding
Option B:	ICMP flooding
Option C:	UDP flooding
Option D:	Host Machine flooding
Q17.	Due to unpredictable behaviors of users and network, a number of false alarms is generated by which IDS
Option A:	IDPS
Option B:	Anamoly based IDS
Option C:	Signature based detection

Option D:	Stateful based detection
Q18.	The Protocol which provides authentication, integrity and data confidentiality in IPSec is
Option A:	Authentication Header and Encapsulating security payload
Option B:	Authentication Header and security payload
Option C:	Authentication Header ,Remote Security payload
Option D:	Authentication Header and High security payload
Q19.	Packet Filter Firewall is also called as
Option A:	Policy filter
Option B:	Analysis filter
Option C:	Policy router
Option D:	Screening filter
Q20.	In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of
Option A:	512 Bit Blocks
Option B:	1024 bit Block
Option C:	2048 bits Block
Option D:	256 bits block
Q21.	IPSec provide security at the _____ layer
Option A:	Application
Option B:	Transport
Option C:	Network
Option D:	Data link

Q22.	SSL Layer is located between _____and _____.
Option A:	Transport layer, Network layer
Option B:	Application layer, Transport layer
Option C:	Data link layer and physical layer
Option D:	Network layer and data link layer
Q23.	In PGP- Digital enveloping we encrypt symmetric key With_____.
Option A:	Sender's Private Key
Option B:	Sender's public key
Option C:	Receiver's Private Key
Option D:	Receiver's Public Key
Q24.	Key management in IPSec is done by _____.
Option A:	Tunnel mode
Option B:	Encapsulating Security payload
Option C:	Authentication Header
Option D:	Internet key exchange
Q25.	Number of round keys in AES is
Option A:	Nr
Option B:	Nr+2
Option C:	Nr+1
Option D:	Nr-1

University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: Information Technology Engineering
Curriculum Scheme: Rev2016
Examination: Third Year Semester V
Course Code: ITC504 and Course Name: Cryptography and Network Security
Time: 1 hour Max. Marks: 50

==========

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