Program: BE Information Technology Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester V

Course Code: ITC504 and Course Name: Cryptography & Network Security

Time: 1 hour Max. Marks: 50

==========

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

Q1.	The division of message into packets is function of_____ layer of OSI model
Option A:	Physical
Option B:	Network
Option C:	Data-Link
Option D:	transport
Q2.	Which of the following is not a type of mono alphabetic cipher?
Option A:	additive cipher
Option B:	multiplicative cipher
Option C:	affine cipher
Option D:	hill cipher
Q3.	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation
Option A:	1 and 3
Option B:	2 and 3
Option C:	3 and 4
Option D:	2 and 4
Q4.	A small program that changes the way a computer operates
Option A:	Worm
Option B:	Trojan
Option C:	Bomb

Option D:	Virus
Q5.	A block cipher processes the data blocks of
Option A:	Different Size
Option B:	Equal Size
Option C:	Plaintext
Option D:	fixed size
Q6.	Advanced Encryption Standard uses _____round for 128-bit keys and _____rounds for 192-bit keys and 14 rounds for 256-bit keys.
Option A:	10, 12
Option B:	16, 32
Option C:	48, 32
Option D:	64, 10
Q7.	In Decryption process of AES, which Of the following process Is NOT conducted in Reverse order ?
Option A:	Add round key
Option B:	Shift rows
Option C:	Byte Transposition
Option D:	Mix Columns
Q8.	DES uses a key generator to generate sixteen _____ round keys
Option A:	32-bit
Option B:	56-bit
Option C:	48-bit
Option D:	64-bit
Q9.	ECB and CBC are _____ ciphers
Option A:	Block
Option B:	Stream
Option C:	Fields
Option D:	Both stream & Feilds
Q10.	What is the responsibility of certifying authority
Option A:	Share Message Authentication code
Option B:	Issues private keys
Option C:	Share digital signature
Option D:	Issues the digital signature
Q11.	PKI is a combination of
Option A:	Symmetric keys encryption with digital certificates
Option B:	Private and public keys but does not use digital certificates
Option C:	CHAP
Option D:	Digital certificates, public-key cryptography, and certificate authorities that

	provide enterprise wide security
Q12.	Which is the original message digest algorithm
Option A:	AES
Option B:	RSA
Option C:	SHA
Option D:	MD
Q13.	Message Authentication:
Option A:	A mechanism of source used to notify the sharing of message
Option B:	A mechanism of source used to notify the integrity of message
Option C:	A mechanism of source used to notify the availability of message
Option D:	A mechanism of source used to notify the redundancy of message
Q14.	A Schnorr signature is a digital signature produced by which algorithm.?
Option A:	AES signature
Option B:	DSA signature
Option C:	Schnorr signature
Option D:	RSA signature
Q15.	The _____ uses MD5 and SHA-1 hash algorithm?
Option A:	EL signature
Option B:	DAA signature
Option C:	DSS signature
Option D:	RSA signature
Q16.	Needham-Schroeder Protocol
Option A:	Used to create key for communication between A & B
Option B:	Used to securely distribute an old session key for communications between A & B
Option C:	Used to securely distribute a new session key for communications between A & B
Option D:	Used to create a private keys for communications between A & B
Q17.	digital signatures provide the ability to:
Option A:	Verify author, date & time of signature, authenticate message contents
Option B:	Only verify date & time of signature
Option C:	Only verify time of signature
Option D:	Only verify message contents
Q18.	_____is used to flood random ports on a remote host with numerous UDP packets
Option A:	MAC addresses
Option B:	UDP Flood

Option C:	IP Addresses
Option D:	TCP Flood
Q19.	Honeypot in network/computer system
Option A:	Used to gain information about how cybercriminals operate.
Option B:	Used to raise an alarm on finding of suspicious activity
Option C:	Used to restrict an illegal access withn network/computer
Option D:	Used to authenticate every single user of network/system
Q20.	An analysis method used by some IDS that looks for instances that are not considered normal behavior is
Option A:	Anomaly Based IDS.
Option B:	Signature Based IDS
Option C:	Host Based IDS
Option D:	Network based IDS
Q21.	Network Layer Firewall Works as
Option A:	Frame Filter
Option B:	Packet Filter
Option C:	Network Filter
Option D:	Bit Filter
Q22.	an attacker sends IP packets from a false (or "spoofed") source address in order to disguise itself, is known as_____
Option A:	IP spoofing.
Option B:	ARP Spoofing
Option C:	Sniffing
Option D:	forgery
Q23.	_____ provides privacy, integrity, and authentication in e-mail.
Option A:	IPSec
Option B:	SSL
Option C:	PGP
Option D:	TLS
Q24.	_____ is an Internet standard approach to e-mail security that incorporates the same functionality as PGP
Option A:	S/MIME
Option B:	PGP
Option C:	ESP
Option D:	MIME
Q25.	AH in IPSec protocol stands for_____
Option A:	Authentication Header
Option B:	Asynchronous Header

Option C:	Authorized Headed
Option D:	Asymmetric Header