	QUESTION	A
1	Assurance Of data secracy is called __	Availability
2	Assurance of no change in data during transmission is called___	confidentiality
3	Assurance for available of data, resources to authorised user is refe	Availability
4	____ is a passive kind of attack.	Release of message cor
5	____ is not a kind of passive attack.	Release of message cor
6	____ a is method to encode plain text into cipher text.	Encipherment
7	We can define ____ process as: y = E(k,X)	assymetric encryption
8	In ____ type of attack, attacker guesses all the possible password b	cryptoanalysis
9	_____ is not a type of attack on encrypted text.	cipher text only
10	Caeser cipher is a ____ techniques.	substitution
11	If plain text is " viva" , using key as 4 by applying ceaser cipher wha	aiae
12	Key size of monoalphabetic algorithm is___	26
13	_____ algorithm is also known as One time pad.	vernam
14	In ____ type of techniques original message id hidden in normal me	steganography
15	_____ is not a stream cipher encryption.	vegenere
16	DES algorithm have ___ bits plain text block.	64
17	DES algorithm have ___ number of rounds.	4
18	key size of DES algorithm is___	64
19	In DES algorithm ____ phase convert key into 48 bit.	expansion
20	The principle of ____ ensures that the sender of a message can not	authentication
21	The four primary security principles related to a message are____	conidentiality,authentic
22	In substitution cipher, the following happens:	characters are replaced
23	The process of writing the text as diagonals and reading it as sequer	Rail Fence techniques
24	The matrix theory is used in the ___ technique.	Hill cipher
25	RSA is _____ type of algorithm.	symmetric
26	DES stands for___	Data Encryption Standa
27	For plain text "hellostudent" encrypted text using Railfence using de	hlteeounlsdt
28	In ___ attack person pretend as a authorized person.	Replay
29	OFB stands for _____	Output Feedback
30	In _____ type of algorithm 5*5 matrix is used.	Cesear cipher
31	Consider plaintext " college" and key=2, find cipher text using Railfence algorithm____.	cleeolg
32	In ___ text from secret message are overwritten with pencil or any	character marking
33	In ___ key pair (public and private) is used.	asymetric
34	In ___ type of algorithm two large prime numbers are selected by t	RSA

B	C	D	CORRECT
confidentiality	integrity	Authentica	confidentiality
Authentication	Availability	integrity	integrity
confidentiality	integrity	Authentica	Availability
Replay	Denial of service	Masquerad	Release of message content
Replay	Traffic analyis	evasdroppi	Replay
X.800	Digital Signature	Access Con	Encipherment
symetric encryption	symmetric decryptio	asymetric c	symetric encryption
expression analysis	symetric analysis	brute force	brute force
plain text only	chosen plain ext	chosen cipl	plain text only
transposition	substitution and trar	hybrid encr	substitution
zmze	kikr	mlmg	zmze
4	2	32	26
monoalphabetic	ceaser	vigenere	vernam
substitution	transposition	analysis	steganography
vernam	RSA	playfair	RSA
62	56	52	64
12	16	22	16
62	56	52	56
key transformation	key substitution	s- box subs	key transformation
availability	access control	non repudi	non repudiation
confidentiality, acces	authentication,authe	availabilty,a	conidentiality,authentication,integrity,non repudiation
rows are replaced by	columns are replace	non of the	characters are replaced by other character
one time pad	block cipher	key cipher	Rail Fence techniques
monoalphabetic	Play fair	vigenere	Play fair
asymetric	both	none of the	asymetric
Data Encryption Solut	Data Encryption Star	Data Encry	Data Encryption Standard
hlelotsuedtn	shtuldleohetn	dlhoeltsuet	hlteeounlsdt
Masquared	Logic bomb	Trojan Hors	Masquared
On Feedback	Open Feedback	Over Feedb	Output Feedback
playfair	Reil fence	Monoalpha	Playfair
olgcele	clgoeec	eeclolg	cleeolg
invisible ink	pin punctures	type writte	character marking
symmetric	both	none of the	asymetric
DES	AES	playfair	RSA

QNO	QUESTION	A
1	___ type of algorithm is used as key exchange algorithm	deffie hellman
2	____ suffers from Man-in -the-Middle attack.	RSA
3	Man in the Middle attack is also called as____	Bucket Brigade attack
4	MAC stands for__	message authenticatio
5	Denial of receipt of message by destination is __ type of attack.	source repudiation
6	Denial of transmission of message by source is __ type of attack.	source repudiation
7	Release of message to any unauthenticated user is ___type of attack.	disclosure
8	A ___functions are mathematical function that converts one value into a	key
9	Reverse of hash function doesn't give original value. It resist to reach ori	pre image resistance
10	When two different inputs finds same hash value , then it is called as___	collision
11	SHA stands for__	standard hash algorith
12	Process of trying to break any cipher text message to obtain the original	cryptanalysis
13	CHAP stands for__	challenge handshake a
14	EAP stands for_____	Extensible Authentication protocol
15		
16	When attacker breaks A's private key it s called as_____	universal forgery
17	In SHA padding is done in such a way that the length of message is ____ bits short of multiple of 512.	28
18	AAA protocol refers to__	Authentication
19	DSS stands for___	digital signature stand
20	Kerbores is a ___ protocol.	Authentication
21	In kerbores TGS stands for __	Ticket Granting Syster
22	In PKIX ___ relates to registration process.	registration authority
23	___ issue certificate.	CA
24	The __standard defines the structure of a digital certificate.	X.109
25	___ is not a function performed by PKIX.	registration
26	In ___ attack attacker forges a signature for a particular message chosen by attacker.	universal forgery
27	When attacker known senders public key and based on that he attack is refered as__	key only attack
28	____ is not a element of public key cryptosystem.	encryptio/decryption
29	In _____ type attack attempts to use all possible permutation and combination.	Brute force
30	___ maps a message of any length into fixed length value as authenticator.	hash function
31	___ is a function of the message and a secret key that produces a fixed length value as authenticator.	MAC
32	____is finger print or the summary of a message.	encryption message
33	SHA -1 produces hash value of __ bits.	160
34	SHA follows ___ step.	padding

B	C	D	ANS
RSA	DES	AES	deffie hellman
DES	AES	deffie hellman	deffie hellman
phishing attack	brute force	none of these	Bucket Brigade attack
message approved	message accept code	message audit code	message authentication code
destination repudi	content recovery	none of these	destination repudiation
destination repudi	content recovery	none of these	source repudiation
content of modific	traffic analysis	timing modification	disclosure
hash	map	all	hash
original resistance	value resistance	reverse resistance	pre image resistance
input double	hash double	none of these	collision
secure hash Algori	same hash algorithm	sample hash algorith	secure hash Algorithm
HMAC	MAC	SHA	cryptanalysis
cipher hello auther	cipher handshake auther	change hello authent	challenge handshake authentication pr

Encrypt Authentication protocol	Extended Authority Process	End Authority Protocol	Extensible Authentication protocol
Encrypt known	Message Known	Total Break	Total Break
56	128	64	64
Authorisation	Accounting	All of these	All of these
data sign standarc	data secure standard	data signature soluti	digital signature standard
access system	allocation	advance	Authentication
Ticket Granting Se	Team Granting Service	Team Granting Syste	Ticket Granting Server
CRL	end entity	registration entity	registration authority
CRA	CLR	AGS	CA
TCP/IP	ASN.1	X.509	X.509
revocation request	certification	introduction	introduction
Total Break	selective forgery	existential forgery	selective forgery
known message at	total break	forgery	key only attack
key exchange	digital signature	key secrecy	key secrecy

MD5	SHA	MD	Brute force
message function	encryption	decryption	hash function
hash	encryption	signature client	MAC
message digest	decryption message	key digest	message digest
256	384	512	160
append length	divide input in 512 block	all of the above	all of the above

ɔtocol

QN	QUESTION	A	B	C	D	CORRECT
1	Security feature offered by PGP_____.	Encryption	Non repudiation	Integrity	All Above	All Above
2	PGP stands for__ In PGP, __ phase creates message digest of email message using SHA-1 algorithm. Resulting message digest is encrypted with sender's private key .	pretty good	private goal publ	public and get	none of the ab	pretty good privacy
3		digital certifi	encryption	compression	padding	digital certificate
4	ZIP program is used for _____.	Compressio n	Deletion	Loading	Encryption	Compression
5	PGP uses___	public key cr	private key crypt	public and priv	none of the ab	public and private key cryp
6	Data compression means__	deleting rep	uniformdisributic	deleting repea	none of the ab	deleting repeated characte
7	PGP doesnot support ___ algorithm for encryption	AES	DES-3	IDEA	COLUMNAR	COLUMNAR
8	In PGP session key is encrypted with__ algorithm.	RSA	AES	IDEA	CAST	RSA
9	In PGP message is encrypted with__ algorithm.	RSA	CAST	MD	secret key	CAST
10	PGP is used for___	emails	file encryption	email and file e	none of the ab	email and file encryption
11	S/MIME stands for	standard mu	standard mail int	Secure/Multip	secure mail int	Secure/Multipurpose Inte
12	___defines a format for text messages that are sent using e	EAF-532	RFC128	EAF 128	RFC 532	RFC 532
13	In S/MIME __ algorithm is used for encrypting symmetric s	deffie hellma	RSA	DES	DSS	deffie hellman
14	In S/MIME __ algorithm is used for symmetric key enryptio	RSA	DES-3	DSS	Deffie hellmar	DES-3
15	killing of user threads threats leads to ___ type attack.	denial of ser	integrity	authentication	confidentiality	denial of service
16	Modification of message during transmission is __ attack	confidentiali	integrity	authentication	denial of servi	integrity
17	When either client or server detects error then ___- protoc	Alert	Handshake	Common	Cipher Spec	Alert
18	In SSL connection between users is__	peer to peer	multipoint	peer to peer a	any one from	peer to peer
19	SSL record protocol provides__	confidentiali	integrity	confidentiality	availability	confidentiality and integrit
20	____ protocol allows the server and client to authenticate	Alert	Handshake	records	Encryption	Handshake
21	__ provides a secure communication channel among all the	SET	PGP	MIME	none of the ab	SET
22	___user seize or control monitoring system or supresses a	misfeaser	clandestine	masquerader	All Above	clandestine
23	Access to the password file is limited to one or a very few a	access contr	available control	secure one wa	information cc	access control
24	In ___, Set of rules are created and check whether behavio	stastical dete	rule based detec	expert detectic	secure detecti	rule based detection
25	_____type of virus infects the system area of a disk.	Rabbit Virus	Boot Sector Virus	Multipartite Virus	Macro Virus	Boot Sector Virus
26	_____is not a phase of Virus life cycle.	Dismissed	Triggering	Propagation	Dormant	Dismissed
27	In dormant phase virus becomes_____	Inactive	Duplicate	Replicate	Completion	Inactive

28	In _____ phase the virus replicates itself and attaches itself to some program.	Execution	Dormant	Propagation	Triggering	Propagation
1	___ type of algorithm is used as key exchange algorithm	deffie hellma	RSA	DES	AES	deffie hellman
2	____ suffers from Man-in -the-Middle attack.	RSA	DES	AES	deffie hellman	deffie hellman
3	Man in the Middle attack is also called as____	Bucket Briga	phishing attack	brute force	none of these	Bucket Brigade attack
4	MAC stands for__	message aut	message approv	message accep	message audit	message authentication cc
5	Denial of receipt of message by destination is __ type of at	source repu	destination repu	content recove	none of these	destination repudiation
6	Denial of transmission of message by source is __ type of a	source repu	destination repu	content recove	none of these	source repudiation
7	Release of message to any unauthenticated user is ___type	disclosure	content of modif	traffic analysis	timing modific	disclosure
8	A ___functions are mathematical function that converts on	key	hash	map	all	hash
9	Reverse of hash function doesn't give original value. It resis	pre image re	original resistanc	value resistanc	reverse resista	pre image resistance
10	When two different inputs finds same hash value , then it i	collision	input double	hash double	none of these	collision
11	SHA stands for__	standard has	secure hash Algo	same hash alg	sample hash a	secure hash Algorithm
12	Process of trying to break any cipher text message to obta	cryptanalysis	HMAC	MAC	SHA	cryptanalysis
13	CHAP stands for__	challenge ha	cipher hello auth	cipher handsha	change hello a	challenge handshake auth
14						
15	EAP stands for_____	Extensible Authenticati on protocol	Encrypt Authentication protocol	Extended Authority Process	End Authority Protocol	Extensible Authentication protocol
16	When attacker breaks A's private key it s called as_____	universal forgery	Encrypt known	Message Known	Total Break	Total Break
17	In SHA padding is done in such a way that the length of message is ____ bits short of multiple of 512.	28	56	128	64	64
18	AAA protocol refers to__	Authenticati	Authorisation	Accounting	All of these	All of these
19	DSS stands for___	digital signat	data sign	standa	data secure sta	data signature	digital signature standard
20	Kerbores is a ___ protocol.	Authenticati	access system	allocation	advance	Authentication
21	In kerbores TGS stands for __	Ticket Granti	Ticket Granting S	Team Granting	Team Granting	Ticket Granting Server
22	In PKIX ___ relates to registration process.	registration a	CRL	end entity	registration er	registration authority
23	___ issue certificate.	CA	CRA	CLR	AGS	CA
24	The __standard defines the structure of a digital certificate.	X.109	TCP/IP	ASN.1	X.509	X.509
25	___ is not a function performed by PKIX.	registration	revocation reque	certification	introduction	introduction
26	In ___ attack attacker forges a signature for a particular message chosen by attacker.	universal forgery	Total Break	selective forge	existential for	selective forgery

27	When attacker known senders public key and based on that he attack is refered as__	key only atta	known message	total break	forgery	key only attack
28	____ is not a element of public key cryptosystem.	encryptio/de	key exchange	digital signatur	key secrecy	key secrecy
29	In _____ type attack attempts to use all possible permutation and combination.	Brute force	MD5	SHA	MD	Brute force
30	___ maps a message of any length into fixed length value as authenticator.	hash functio	message functio	encryption	decryption	hash function
31	___ is a function of the message and a secret key that produces a fixed length value as authenticator.	MAC	hash	encryption	signature clien	MAC
32	____is finger print or the summary of a message.	encryption n	message digest	decryption me	key digest	message digest
33	SHA -1 produces hash value of __ bits.	160	256	384	512	160
34	SHA follows ___ step.	padding	append length	divide input in	all of the abov	all of the above

1	Assurance Of data secracy is called __	Availability	confidentiality	integrity	Authentication	confidentiality
2	Assurance of no change in data during transmission is calle	confidentiali	Authentication	Availability	integrity	integrity
3	Assurance for available of data, resources to authorised us	Availability	confidentiality	integrity	Authentication	Availability
4	____ is a passive kind of attack.	Release of m	Replay	Denial of servi	Masquerade	Release of message conter
5	____ is not a kind of passive attack.	Release of m	Replay	Traffic analyis	evasdropping	Replay
6	____ a is method to encode plain text into cipher text.	Encipherme	X.800	Digital Signatu	Access Contro	Encipherment
7	We can define ____ process as: y = E(k,X)	assymetric e	symetric encrypt	symmetric dec	asymetric dec	symetric encryption
8	In ____ type of attack, attacker guesses all the possible pas	cryptoanalys	expression analy	symetric analy	brute force	brute force
9	_____ is not a type of attack on encrypted text.	cipher text o	plain text only	chosen plain e	chosen cipher	plain text only
10	Caeser cipher is a ____ techniques.	substitution	transposition	substitution ar	hybrid encrypt	substitution
11	If plain text is " viva" , using key as 4 by applying ceaser cip	aiae	zmze	kikr	mlmg	zmze
12	Key size of monoalphabetic algorithm is___	26	4	2	32	26
13	_____ algorithm is also known as One time pad.	vernam	monoalphabetic	ceaser	vigenere	vernam
14	In ____ type of techniques original message id hidden in nc	steganograp	substitution	transposition	analysis	steganography
15	_____ is not a stream cipher encryption.	vegenere	vernam	RSA	playfair	RSA
16	DES algorithm have ___ bits plain text block.	64	62	56	52	64
17	DES algorithm have ___ number of rounds.	4	12	16	22	16
18	key size of DES algorithm is___	64	62	56	52	56
19	In DES algorithm ____ phase convert key into 48 bit.	expansion	key transformati	key substitutio	s- box substitu	key transformation
20	The principle of ____ ensures that the sender of a message	authenticati	availability	access control	non repudiatic	non repudiation
21	The four primary security principles related to a message a	conidentialit	confidentiality, a	authentication	availabilty,acc	conidentiality,authenticati
22	In substitution cipher, the following happens:	characters a	rows are replace	columns are re	non of the abc	characters are replaced by

23	The process of writing the text as diagonals and reading it a	Rail Fence te	one time pad	block cipher	key cipher	Rail Fence techniques
24	The matrix theory is used in the ___ technique.	Hill cipher	monoalphabetic	Play fair	vigenere	Play fair
25	RSA is _____ type of algorithm.	symmetric	asymetric	both	none of these	asymetric
26	DES stands for___	Data Encrypt	Data Encryption	Data Encryptio	Data Encryptic	Data Encryption Standard
27	For plain text "hellostudent" encrypted text using Railfence	hlteeounlsdt	hlelotsuedtn	shtuldleohetn	dlhoeltsuetn	hlteeounlsdt
28	In ___ attack person pretend as a authorized person.	Replay	Masquared	Logic bomb	Trojan Horse	Masquared
29	OFB stands for _____	Output Feed	On Feedback	Open Feedbac	Over Feedbac	Output Feedback
30	In _____ type of algorithm 5*5 matrix is used.	Cesear ciphe	playfair	Reil fence	Monoalphabe	Playfair
31	Consider plaintext " college" and key=2, find cipher text using Railfence algorithm____.	cleeolg	olgcele	clgoeec	eeclolg	cleeolg
32	In ___ text from secret message are overwritten with penc	character ma	invisible ink	pin punctures	type writter ri	character marking
33	In ___ key pair (public and private) is used.	asymetric	symmetric	both	none of these	asymetric
34	In ___ type of algorithm two large prime numbers are sele	RSA	DES	AES	playfair	RSA

ɔtosystem
ers and uniform distribution of character

rnet Mail Extension

:y

ɔde

entication protocol

nt

on,integrity,non repudiation

other character