National Testing Agency

Question Paper Name:	Cryptography
Subject Name:	Cryptography
Creation Date:	2018-12-02 17:35:44
Duration:	180
Total Marks:	100
Display Marks:	Yes
Share Answer Key With Delivery Engine:	Yes
Actual Answer Key:	Yes

Cryptography

Group Number :	1
Group Id :	416529108
Group Maximum Duration :	0
Group Minimum Duration :	120
Revisit allowed for view? :	No
Revisit allowed for edit? :	No
Break time:	0
Group Marks:	100

Cryptography

Section Id :	416529108
Section Number :	1
Section type :	Online
Mandatory or Optional:	Mandatory
Number of Questions:	100
Number of Questions to be attempted:	100
Section Marks:	100
Display Number Panel:	Yes
Group All Questions:	No

Sub-Section Number:	1
Sub-Section Id:	416529117
Question Shuffling Allowed :	Yes

Question Number : 1 Question Id : 4165298506 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

When someone without your knowledge acquires a piece of information and used it to commit fraud, that is called

A. Identity Theft
B. Blue jacking
C. Tab nabbing
D. None

Question Number : 2 Question Id : 4165298507 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The _____ cipher reorders the plaintext characters to create a ciphertext.

A. Substitution

B. Transposition

C. Either (a) or (b)

D. Neither (a) nor (b)

Question Number : 3 Question Id : 4165298508 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In which year IBM founded Crypto group:

A. 1960

B. 1970

C. 1980

D. 1990

Question Number : 4 Question Id : 4165298509 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

A threat profile is a set of

A. only threats

B. only vulnerabilities

C. both threats and vulnerabilities

D. passwords

Question Number : 5 Question Id : 4165298510 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The _____is the original message before transformation.

A. ciphertext

B. plaintext

C. secret-text

D. none of the above

Question Number : 6 Question Id : 4165298511 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In Decentralised Key Control, session key can be established by using how many steps?

A. 1

B. 2

C. 3

D. None of these

Question Number : 7 Question Id : 4165298512 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The de facto industry standard for digital signature is _____

A. RSA

B. DSA

C. ECDSA

D. none of the above

Question Number : 8 Question Id : 4165298513 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

A trusted authority that certifies individuals' identities and creates digital certificates is called a ____.
A. certificate authority
B. certificate repository
C. local registration authority
D. registration authority

Question Number : 9 Question Id : 4165298514 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

When someone without your knowledge acquires a piece of information and used it to commit fraud, that is called:
A. Identity Theft
B. Blue jacking
C. Tab nabbing
D. None

Question Number : 10 Question Id : 4165298515 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The structure of HMAC is specified in
A. RFC2104
B. RFC2204
C. RFC1204
D. RFC4021

Question Number : 11 Question Id : 4165298516 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The most effective way of protecting against SQL injection is?
A. using an intrusion detection system to detect attacks
B. whitelisting input (e.g. only allowing alphanumerical characters and spaces)
C. use of prepared statements or parametrized queries
D. segmenting database accounts and minimizing their user rights

Question Number : 12 Question Id : 4165298517 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Most unpopular Email security algorithm among PGP, PEM and S/MIME is:
A. PGP
B. S/MIME
C. PEM
D. none of the above

Question Number : 13 Question Id : 4165298518 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The minimum number of colors needed to color a graph having n (>3) vertices and 2 edges is
1
2
3
4

Question Number : 14 Question Id : 4165298519 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Transport Mode of IPSec operates between
End point of communication
Peers
Routers
Switch

Question Number : 15 Question Id : 4165298520 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Kerberos use _____
A. TLS & SSL
B. Symmetric Key Cryptography and Timestamps
C. IPSec
D. None of these

Question Number : 16 Question Id : 4165298521 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following requirement is not listed in first report of Kerberos?
A.Intruders
B. Secure
C. Reliable
D. Transparent

Question Number : 17 Question Id : 4165298522 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Data Encryption Standard algorithm was proposed by
A. IBM
B. Intel
C. IEEE
C. IEEE

Question Number : 18 Question Id : 4165298523 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

What is data encryption standard (DES)?
A. A Stream Cipher
B. A Bit Cipher
C. A Block Cipher
D. A Substitution Cipher

Question Number : 19 Question Id : 4165298524 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Key distribution can be achieved by
A. A can select a key and physically deliver it to B.
B. A third party can select the key and physically deliver it to A and B
C. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
D. All of Above

Question Number : 20 Question Id : 4165298525 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

if N entities wish to communicate in pairs, we need N(N-1)]/2 session keys at any one time, then how many master keys are needed?
A. N-1
B. N(N-1)
C. N
D. None of these

Question Number : 21 Question Id : 4165298526 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the Following is not a type of session key:
A. Data-encrypting key
B. PIN-encrypting key
C. File-encrypting key
D. Record-encryption key

Question Number : 22 Question Id : 4165298527 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Federal Information Processing Standards have been developed for use by :
A. U. S. Government.
B. Canadian Army
C. UN.forces
D. CBI

Question Number : 23 Question Id : 4165298528 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

. ISO/IEC 9798 -3 standards defines Entity Authentication using
A. using public-key techniques
B. using symmetric encipherment
C. using keyed one-way functions
D. None of the above

Question Number : 24 Question Id : 4165298529 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Digital Signatures provides
A. Authentication
B. Non-Repudiation
C. Both a) and b)
D. Neither a) nor b)

Question Number : 25 Question Id : 4165298530 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

_____ is the science and art of transforming messages in order to make them secure and resistant to attacks.
A. Cryptography
B. Cryptoanalysis
C. either (a) or (b)
D. neither (a) nor (b)

Question Number : 26 Question Id : 4165298531 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

. Sender and Receiver share the same key in
A. Symmetric Cryptography
B. Asymmetric Cryptography
C. None of these
D. Both A and B

Question Number : 27 Question Id : 4165298532 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Cryptanalysis can be defined as:
A. Making and breaking secret codes
B. making of secret codes
C. The breaking of secret codes
D. None of these

Question Number : 28 Question Id : 4165298533 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Kerberos is a _____?
A. Authentication Protocol
B. Packet Filter
C. Static Firewall
D. Antivirus

Question Number : 29 Question Id : 4165298534 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is not the essential service that access control systems provide
A. Authentication
B. Authorization
C. access approval
D. Tokenization

Question Number : 30 Question Id : 4165298535 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

AES algorithm is published as
A. FIPS 196
B. FIPS 197
C. FIPS 198
D. none of above

Question Number : 31 Question Id : 4165298536 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The entities that can perform actions are called
A. Subjects
B. Objects
C. Boxes
D. Code blocks

Question Number : 32 Question Id : 4165298537 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The number of colours required to properly colour the vertices of every planer graph is.
A. 2
B. 3
C. 4
D. 5

Question Number : 33 Question Id : 4165298538 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Pretty Good Privacy uses _____.

A. symmetric key encryption
B. public key encryption
C. both a) and b)
D. neither a) nor b)

Question Number : 34 Question Id : 4165298539 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The data structure required for Breadth First Traversal on a graph is

A. Queue
B. Stack
C. Array
D. Tree

Question Number : 35 Question Id : 4165298540 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

A hash function guarantees integrity of a message. It guarantees that message has not be.

A. replaced
B. overview
C. changed
D. left

Question Number : 36 Question Id : 4165298541 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which two of the following attacks are examples of identity theft?

A. Trojan Horse
B. Spoofing
C. Back Door
D. Both b and c

Question Number : 37 Question Id : 4165298542 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

MAC, in network security, stands for.

A. message authentication code
B. message authentication connection
C. message authentication control
D. message authentication cipher

Question Number : 38 Question Id : 4165298543 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

What should be the first step in implementing a database security program?

A. Perform a full user/role audit
B. Turn on native database auditing
C. Mask production data going to development systems
D. Define database configuration standards

Question Number : 39 Question Id : 4165298544 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is a computer security component?
A. Senior management involvement
B. Non – Planned responses
C. Electronic safes
D. None of these

Question Number : 40 Question Id : 4165298545 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Smart card users are required to use a _____ to be authenticated
A. PIN
B. Password
C. Biometric scan
D. All of the above

Question Number : 41 Question Id : 4165298546 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

A digital signature needs a.
A. Private key system
B. Symmetric key
C. Public key system
D. DES

Question Number : 42 Question Id : 4165298547 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

OpenPGP is defined by the OpenPGP Working Group of the Internet Engineering Task Force IETF, standard ------
A. RFC 4880
B. RFC 822
C. both (a) and (b)
D. none of the above

Question Number : 43 Question Id : 4165298548 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In PEM, Encoding is done using _____ coding.
A. Base 16
B. Base 32
C. Base 64
D. none of the above

Question Number : 44 Question Id : 4165298549 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Ciphers of today are called round ciphers because they involve
A. Single Round
B. Double Rounds
C. Multiple Round
D. Round about

Question Number : 45 Question Id : 4165298550 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In IDEA, the key size is
A. 128 bytes
B. 128 bits
C. 256 bytes
D. 256 bits

Question Number : 46 Question Id : 4165298551 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

DES, IDEA, RC2, RC4 and Rinjdael are examples of
A. Symmetric key algorithms
B. Asymmetric key algorithms
C. Public key algorithm
D. Private key algorithm

Question Number : 47 Question Id : 4165298552 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

One element of database security is to provide only unauthorized users with:
A. Classes
B. Nodes
C. Passwords
D. Relations

Question Number : 48 Question Id : 4165298553 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The bridge between the logical and physical views of the data is provided by:
A. DBMS
B. Records
C. SQL
D. Tables

Question Number : 49 Question Id : 4165298554 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following exploits computer networks and security holes to reproduce itself?
A. Worm
B. Trojan
C. Virus
D. Email virus

Question Number : 50 Question Id : 4165298555 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

What is the best way to defend against a back door attack?
A. Use of hardware Firewall
B. Use of hardware IDS
C. Software patches
D. None

Question Number : 51 Question Id : 4165298556 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The AH Protocol provides source authentication and data integrity but not
A. Privacy
B. Integrity
C. Non repudiation
D. None of the above

Question Number : 52 Question Id : 4165298557 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The ESP provides

A. Source authorisation

B. Data integration

C. Privacy

Question Number : 53 Question Id : 4165298558 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

SHA-1 has a message digest of.

A. 160 bit

B. 156 bit

C. 120 bit

D. 128 bit

Question Number : 54 Question Id : 4165298559 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Message authentication is a service beyond.

A. Message Confidentiality

B. Message Integrity

C. Message Splashing

D. None of above

Question Number : 55 Question Id : 4165298560 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In Message Confidentiality, transmitted message must make sense to only intended.

A. sender

B. receiver

C. either (a) or (b)

D. neither (a) nor (b)

Question Number : 56 Question Id : 4165298561 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is not based on block cipher?

A. CMAC

B. PMAC

C. HMAC

D. XCBC

Question Number : 57 Question Id : 4165298562 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

What is AS?

A. Autonomous System

B. Application Service

C. Authentication Server

D. None of the above

Question Number : 58 Question Id : 4165298563 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

What are the number of messages exchanged in Kerberos Version 4 Message Exchange
A. 3
B. 5
C. 7
D. 6

Question Number : 59 Question Id : 4165298564 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is not a Cryptographic Technique?
A. Symmetric
B. Hash Function
C. Asymmetric
D. Linear Function

Question Number : 60 Question Id : 4165298565 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is not a trust model?
A. Direct trust
B. Transitive trust
C. Assumptive trust
D. Indirect trust

Question Number : 61 Question Id : 4165298566 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following Cryptographic algorithm not use same key for encryption and decryption?
A. DES
B. RSA
C. AES
D. Monoalphabetic Sustitution

Question Number : 62 Question Id : 4165298567 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is not the component of Symmetric Cipher model
A. Plaintext
B. Encryption Algorithm
C. Secret Key
D. Crypt Analysis

Question Number : 63 Question Id : 4165298568 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Substitution cipher can be of how many types
A. 1
B. 2
C. 3
D. 4

Question Number : 64 Question Id : 4165298569 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The second Beale cipher is an example of what type of cipher?
A. public key
B. book cipher
C. machine cipher
D. monoalphabetic

Question Number : 65 Question Id : 4165298570 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Vernam Cipher is also called as

A. Rail Fence Technique

B. One-time pad

C. Book Cipher

D. Running Key Cipher

Question Number : 66 Question Id : 4165298571 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

A hashing function for digital signature

(i) must give a hashed message which is shorter than the original message

(ii) must be hardware implementable

(iii) two different messages should not give the same hashed message

(iv) is not essential for implementing digital signature

A. i and ii

B. ii and iii

C. i and iii

D. iii and iv

Question Number : 67 Question Id : 4165298572 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

A patent is a set of exclusive right granted to an inventor for any invention for :

A. Limited period of time.

B. Unlimited period of time

C. Lifelong

D. None of above

Question Number : 68 Question Id : 4165298573 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Ehrsam et al. got a patent no 3962539 which became well known as :

A. Tree authentication

B. RSA

C. DES

D. None of the above

Question Number : 69 Question Id : 4165298574 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Diffie Hellman patent defines secured communication over insecure channel without using a :

A. Priori key

B. Public key

C. Secret key

D. None of the above

Question Number : 70 Question Id : 4165298575 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Okamoto (4,625,076) patents provides _____ scheme :

A. DSA Signature

B. IDEA cipher

C. E-Signature

D. All of the above

Question Number : 71 Question Id : 4165298576 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

MAC in security / authentication process means

A. Medium Access Control

B. Money Access control

C. Message Authentication code

D. All of the above

Question Number : 72 Question Id : 4165298577 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Caesar Cipher is an example of

A. Substitution Cipher

B. Transposition Cipher

C. Substitution as well as Transposition Cipher

D. none of the above

Question Number : 73 Question Id : 4165298578 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

AES algorithm is based upon which algorithm

A. Rijndael

B. Serpent

C. Twofish

D. RC6

Question Number : 74 Question Id : 4165298579 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following variable is used to store encrypted key in AES algorithm

A. Rk

B. K

C. both of the above

D. none of the above

Question Number : 75 Question Id : 4165298580 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In cryptography, the order of the letters in a message is rearranged by

A. transposition ciphers

B. substitution ciphers

C. both (a) and (b)

D. none of the mentioned

Question Number : 76 Question Id : 4165298581 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Message authentication is concerned with Source authentication and

A. Virus protection

B. Physical Access Control

C. Data integrity

D. Confidentiality

Question Number : 77 Question Id : 4165298582 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following uses the double encryption?
A. Version 5
B. Version 4
C. Kerri
D. Version 3

Question Number : 78 Question Id : 4165298583 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is not a ticket flag used in Kerberos Version 5?
A. INTIAL
B. POSTDATED
C. INVALID
D. RETURNED

Question Number : 79 Question Id : 4165298584 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

CBC is used in which Kerberos Version?
A. Version 5
B. Version 4
C. Kerri
D. All of the above

Question Number : 80 Question Id : 4165298585 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

How would you be able to protect yourself from phishing?
A. Call your local fish store.
B. Get an Anti-Virus Program
C. Change Passwords Every 4-6 months
D. Option b & c

Question Number : 81 Question Id : 4165298586 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

What term describes masquerading as a trustworthy source such as a bank, and requesting a password, credit card number or other personal information from a user
A. Identity Theft
B. Phishing
C. Phreaking
D. Cybersquatting

Question Number : 82 Question Id : 4165298587 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Corporate executives and industry leaders are often targeted by which type of electronic attack
A. Denial of Service
B. Brute Force
C. Whaling
D. Spear Phishing

Question Number : 83 Question Id : 4165298588 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

SMIME supports
A. Diffie Hellman with DSS or RSA
B. ElGamal with DSS
C. Both of the above
D. None of the above

Question Number : 84 Question Id : 4165298589 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In ACL based model the subject can access an object if
A. the subject appears on the access list
B. object appears on the access list
C. the subject is weak entity
D. the object is weak entity

Question Number : 85 Question Id : 4165298590 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In Playfair Cipher, how the keyword is entered in Matrix row wise
A. From left to right and then bottom to top
B. From right to left and then bottom to top
C. From left to right and then top to bottom
D. From right to left and then top to bottom

Question Number : 86 Question Id : 4165298591 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In which year IBM founded Crypto group:
A. 1960
B. 1970
C. 1980
D. 1990

Question Number : 87 Question Id : 4165298592 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document.
A. Integrity
B. Correctness
C. Authenticity
D. None of above

Question Number : 88 Question Id : 4165298593 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Merkle's patent covers two _____ block ciphers named Khafre and Khufu.
A. Asymmetric key
B. RSA Signature
C. Symmetric key
D. None of above

Question Number : 89 Question Id : 4165298594 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Digital Signature cannot provide _____ for the message
A. Integrity
B. Confidentiality
C. Non-Repudiation
D. Authentication

Question Number : 90 Question Id : 4165298595 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

FIPS 112 and FIPS 113 defines
A. Password usage and data authentication
B. Password usage and key escrow
C. Data authentication and key escrow
D. None of above

Question Number : 91 Question Id : 4165298596 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Encryption and decryption provide secrecy, or confidentiality, but not
A. authentication
B. integrity
C. privacy
D. None of above

Question Number : 92 Question Id : 4165298597 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Relationship between a character in plaintext to a character is
A. Many-to-one relationship
B. One-to-many relationship
C. Many-to-many relationship
D. None

Question Number : 93 Question Id : 4165298598 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In symmetric-key cryptography, key locks and unlocks box is
A. Same
B. Shared
C. Private
D. Public

Question Number : 94 Question Id : 4165298599 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

_____ is the science and art of transforming messages to make them secure and immune to attacks.
A. Cryptography
B. Cryptoanalysis
C. either (a) or (b)
D. neither (a) nor (b)

Question Number : 95 Question Id : 4165298600 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following statement is false?
A. Trust is not a characteristic of a security architecture
B. Trust is balancing of liability and due diligence
C. Trust is the enabling of confidence
D. Trust is defined as a binary relationship

Question Number : 96 Question Id : 4165298601 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

When does entity authentication occurs?

A. At the beginning

B. At the end

C. In between

D. Does not occur at all

Question Number : 97 Question Id : 4165298602 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which field identifies the algorithm used in a digital certificate?

A. Certificate usage

B. Extensions

C. Public key

D. Serial number

Question Number : 98 Question Id : 4165298603 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following types of certificates is self-signed or issued by a superior CA within a hierarchical model?

A. CA certificate

B. Cross-certification certificate

C. End-entity certificate

D. Policy certificate

Question Number : 99 Question Id : 4165298604 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

What is not true about Message Authentication codes?

A. MACs are based on secret symmetric keys

B. MACs accept messages of arbitrary length and generate fixed-size authentication tags

C. It is infeasible to find another message with the same MAC

D. MACs provide non-repudiation.

Question Number : 100 Question Id : 4165298605 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of following is not Application Layer Security

A. S/MIME

B. PGP

C. SET

D. TLS