which one is consider as a type of passive attack:

a. Traffic analysis

b. Modification of messages.

c. Denial of service

d. Masquerade.

Clear my choice

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information, this can be described as:

- a. Confidentiality.
- b. Privacy.
- c. Data confidentiality.
- d. Data integrity.

Clear my choice

Confidentially can be classified into two main categories

Select one:

- a. Privacy
- b. Authentication
- c. Data confidentiality
- d. a+c
- e. b+c

Clear my choice

using Feistel Cipher Structure to find out the ciphertext based on following details:

plaintext: 00111010

Encrypt the message = "WAIT ME AT THE NORTH GATE AT SIX PM", using Row Transposition Cipher where the Key= 4312567.

- a. ARA EOEM MNTP WTTT ATHS TEAX IHGI
- b. IHGI WTTT ARA EOEM MNTP ATHS TEAX
- c. IHGI TEAX ATHS WTTT MNTP EOEM ARA
- d. OTHER.

.....Its purpose is to collect and steal private information from a computer system and and sends it to the hacker

Select one:

- a. DoS attack
- b. Spyware attack
- c. Keylogger attack
- d. All the answers are true

Finish attempt ...

Information Security

rmation Security-Section 1 | Information Security _ Dr Shadi Masadeh | Information Security | مقرراتي الدراسية | الصفحة الرئيسية

In terms of User Authentication Methods classification, the user's fingerprint can be classified as:

a. KBA- (Behavioral biometrics).

b. BBA-(Physiological biometrics).

c. BBA-(Behavioral biometrics).

d. PBA- (Behavioral biometrics).

أخل اختياري

سؤال 1
درجة الإجابة
الدرجة من 2
لم يتم هذا السؤال

terms of parameters and design features of block cipher, Larger block sizes mean:

a. eater security and greater encryption/decryption speed.

b. duce security and reduce encryption/decryption speed.

c. duce security but greater encryption/decryption speed

سؤال 2
درجة الإجابة
الدرجة من 3
لم يتم الإجابة

اكتب هنا للبحث

○ d. greater security but reduced encryption/decryption speed.

Clear my choice

Encrypt the message p= HELLO using Playfair Cipher in order to find out the ciphertext C, if the keyword=thailand.

○ a. C= LDAAZEU

● b. C= LDAZEU

○ c. Other.

◉ d. C= UEZADL

Clear my choice

------- is the process of recognizing a user's identity.

○ a. Accountability.

◉ b. Authentication.

ion 7
ar saved
ed out of
g
ion

The Rail Fence encryption method is based on substitution in order to encrypt plain text

Select one:

- True
- False

ion 8
at
ered
ed out of
g
ion

The assets of a computer system can be categorized as hardware, software, etc. The threat to hardware can be an effect on:

Select one:

- a. Confidentially
- b. Availability & Confidentially
- c. Integrity
- d. Availability

on 7

red

d out of

g
ion

A flaw or weakness in a system's design, implementation, or operation and management that could be
exploited to violate the system's security policy, this can be described as:

- a. Vulnerability.
- b. Threat.
- c. Attack.
- d. Risk.

Clear my choice

estion 8

t yet

If we use RSA, write a correct value of (e) variable if n=35 and ϕ=24 ?

the two users A & B wishes to swap keys and generate shared session key by using **Diffie-Hellman** Key exchange algorithm, Suppose that: **q=13, a=2**, and User A selects the secret value X_A=3, and User B selects the secret value X_B=7, based on that compute the followings:

the Public key of User A (Y_A)

the Public key of User B (Y_B)

the shared secret Key K_{AB}

- a. Y_A =8 and Y_B =11 and K_{AB}= 6.
- b. Y_A =8 and Y_B =11 and K_{AB}= 5.
- c. Y_A =11 and Y_B =8 and K_{AB}= 4.
- d. Y_A =5 and Y_B =8 and K_{AB}= 11.

parameters and design features of symmetric block cipher such as:

- a. brute-force approach.
- b. electronic codebook.
- c. Modes of operation.
- d. Round function.

Clear my choice

Question 3

Answer saved

Marked out of 2

Flag question

___is an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker

Select one:

- a. Phishing
- b. Trojan Horse
- c. Worm
- d. DDoS

Clear my choice

Question 4

Answer saved

Marked out of 6

Remove flag

suppose you have the primes p=2, q=7 using RSA algorithm find out the followings:

Public key (KU)

Private Key (KR)

Ciphertext (C) if the message (M)=2 (Encryption)

Message (M) if the Ciphertext (C)=3 (Decryption)

- a. KU=[5,14], KR=[11,14], C=4 and M=5.
- b. KU=[3, 14], KR=[8, 14], C=5 and M=4.
- c. KU=[2, 14], KR=[9, 14], C=4 and M=4.
- d. KU=[5, 14], KR=[7, 14], C=2 and M=3.

Type here to search

Question 4

Not yet answered

Marked out of 2

Flag question

-------- is the process of recognizing a user's identity.

- a. Confidentiality.
- b. Integrity.
- c. Accountability.
- d. Authentication.

Clear my choice

Next page

when an unauthorized copy of software is made, this will lead to loss of.....

- a. availability.
- b. System integrity.
- c. integrity.
- d. confidentiality.

Clear my choice

Question 12

Not yet answered

Marked out of 2

Flag question

.....An attacker observes and detects the messages transmission in the network

Select one:

- a. Passive attacks
- b. Trojan horse attacks
- c. Active attacks & Passive attacks
- d. Active attacks

Clear my choice

Question 13

Not yet answered

If we use RSA, write a correct value of (e) variable if n=35 and ϕ=24 ?

Select one:

d. Possession-based authentication.

Clear my choice

find out the Ciphertext (C) using Hill Cipher for the plaintext= HELP,
where the matrix key=[3 3]
[2 5]

a. Ciphertext= TAIH

b. Other.

c. Ciphertext= HIAT

d. Ciphertext= ATHI

Clear my choice

.....Its purpose is to collect and steal private information from a computer system and and sends it to the hacker

In terms of User Authentication Methods classification, personal identification number (PIN) can be classified as:

- a. Biometrics-based authentication.
- b. Others mechanisms.
- c. Knowledge-based authentication.
- d. Possession-based authentication.

Clear my choice

in terms of parameters and design features of block cipher, Larger key size mean:

- a. reduce security and reduce encryption/decryption speed.
- b. greater security but reduced encryption/decryption speed.
- c. greater security and greater encryption/decryption speed.
- d. reduce security but greater encryption/decryption speed.

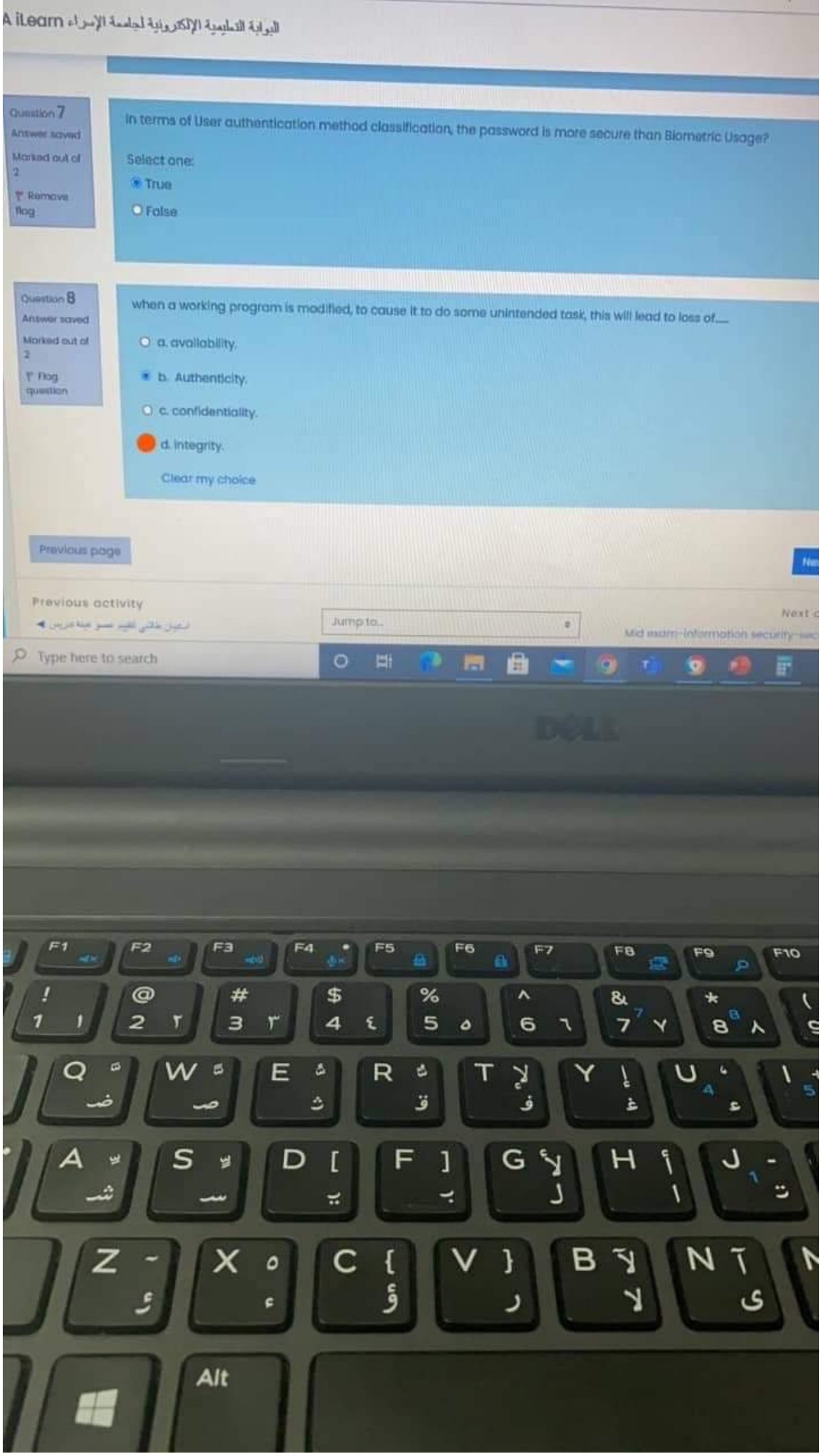
The CIA triad is used to define the required.....

- a. countermeasures that can be used to recover from an attack.
- b. Restrictions on information access including means for protecting.
- c. Timely and reliable access to and use of information.
- d. security objectives in order to protect the information system resources.

The assets of a computer system can be categorized as hardware, software, etc. The threat to hardware can be an effect on:

Select one:

- a. Confidentially
- b. Availability & Confidentially
- c. Integrity
- d. Availability



- b. Y_A =8 and Y_B =11 and K_{AB}= 5.
- c. Y_A =11 and Y_B =8 and K_{AB}= 4.
- d. Y_A =5 and Y_B =8 and K_{AB}= 11.

Fir

Tim

on 14

t

ed

d out of

ion

when a program is deleted to deny access to the users, this will lead to loss of.....

- a. confidentiality.
- b. availability.
- c. Authenticity.
- d. integrity.

Clear my choice

tion 15

ver saved

ed out of

log

suppose you have the primes p=2, q=7 using *RSA* algorithm find out the followings:

Public key (KU)

Private Key (KR)

Ciphertext (C) if the message (M)=2 (Encryption)

in terms of symmetric encryption scheme, the Decryption algorithm takes the plaintext and the secret key to produces the ciphertext.

Select one:

- True
- False

The process of attempting to discover the plaintext or key is known as:

- a. Cryptography.
- b. Cryptographic systems dimensions.
- c. Cryptanalysis.
- d. Conventional encryption.

Clear my choice

find out the Ciphertext (C) using Rail Fence cipher for the plaintext= GOOD MORNING, where the Depth=2.

- a. Ciphertext= GOMRIGODONN
- b. Ciphertext=ODONNGOMRIG
- c. Other.
- d. Ciphertext=GOMRIGNONDOO

Virus binds itself to non-executable files such as image files

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a
deliberate attempt to evade security services and violate the security policy of a system, this can be described as:

- a. Attack.
- b. Threat.
- c. Vulnerability.
- d. Risk.

Clear my choice

which one is consider as a category of active attack:

- a. Eavesdropping.
- b. Modification of messages.
- c. Release of message contents.
- d. Traffic analysis.

Clear my choice

- c. Ciphertext=GOMRIGNONDOO
- d. Other.

in a caesar cipher, if the Key used =26, the encryption of the letter "A" will be :

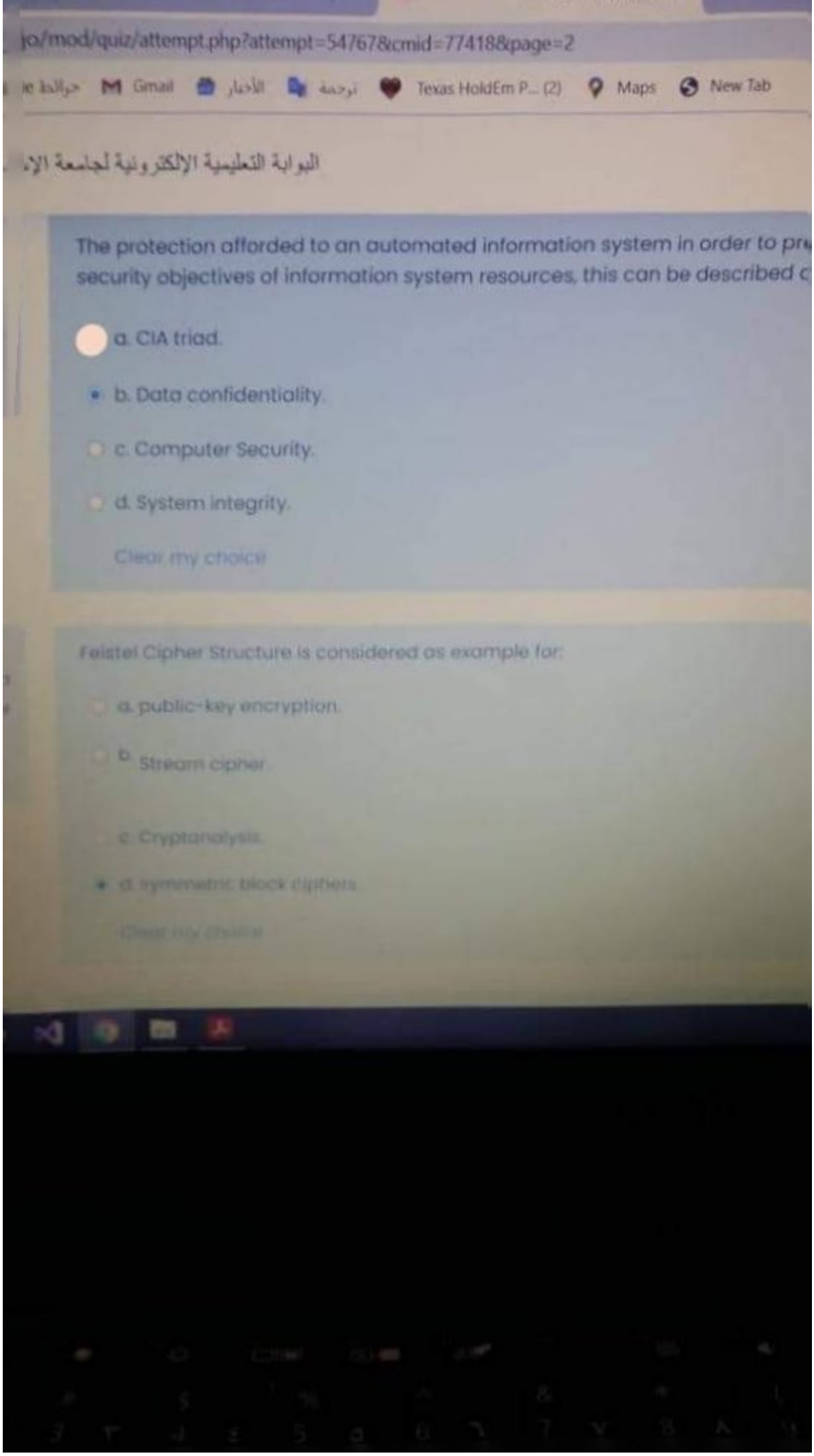
- a. A
- b. B
- c. Z
- d. Y

Clear my choice

A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm, this can be described as:

- a. Vulnerability.
- b. Threat.
- c. Attack.
- d. Risk.

Clear my choice



Information Security

elearn.iu.edu.jo/mod/quiz/attempt.php?attempt=171375&cmid=109085

Isra University: Log... | واتساب | YouTube | Google ترجمة - بحث | مسلسل الأزهار الحزي... | (1) Row Transposit... | What is Eth

iLearn البوابة التعليمية الإلكترونية لجامعة الإسراء

Question 1
Answer saved
Marked out of 2
Flag question

in terms of User Authentication Methods classification, Smart card can be classified as:

- a. Knowledge-based authentication.
- b. Possession-based authentication.
- c. Others mechanisms.
- d. Biometrics-based authentication.

Clear my choice

Question 2
Answer saved
Marked out of 5
Flag question

the two users A & B wishes to swap keys and generate shared session key by using **Diffie-Hellman** Key exchange algorithm. Suppose that: **q=13, α=2**, and User A selects the secret value $X_A=3$, and User B selects the secret value $X_B=7$, based on that compute the followings:

the Public key of User A (Y_A)

the Public key of User B (Y_B)

the shared secret Key K_{AB}

- a. $Y_A=5$ and $Y_B=8$ and $K_{AB}=11$.
- b. $Y_A=8$ and $Y_B=11$ and $K_{AB}=6$.
- c. $Y_A=8$ and $Y_B=11$ and $K_{AB}=5$.
- d. $Y_A=11$ and $Y_B=8$ and $K_{AB}=4$.

Type here to search

the encryption method that uses matrices and matrix multiplication to mix up the plaintext called

- a. Row transposition cipher
- b. Hill cipher
- c. one-time pad
- d. playfair cipher

Clear my choice

In terms of Cryptographic systems dimensions, Cryptographic systems can be classified into symmetric and asymmetric based on:

a. The way in which the plaintext is processed.

b. The type of operations used for transforming plaintext to ciphertext.

c. the nature of the encryption scheme and the information available to the cryptanalyst.

d. The number of keys used.

in terms of symmetric encryption scheme ingredients, the scrambled message produced as output, can be described as:

- a. Ciphertext.
- b. Encryption algorithm.
- c. Plaintext.
- d. Secret key.

In terms of Cryptographic systems dimensions, Cryptographic systems can be classified based on the way in which the plaintext is processed into:

- a. substitution and permutation.
- b. block cipher and stream cipher.
- c. plaintext and ciphertext.
- d. symmetric and asymmetric.

the encryption method that uses matrices and matrix multiplication to mix up the plaintext called

7

d

out of

n

parameters and design features of symmetric block cipher such as:

- a. Modes of operation.
- b. Number of rounds.
- c. brute-force approach.
- d. electronic codebook.

on 8

in terms of symmetric encryption scheme ingredients, what are the inputs of enc

In terms of Cryptographic systems dimensions, Cryptographic systems can be classified based on the way in which the plaintext is processed into:

- a. block cipher and stream cipher.
- b. plaintext and ciphertext.
- c. substitution and permutation.
- d. symmetric and asymmetric.

Clear my choice

parameters and design features of symmetric block cipher such as:

Question 11

Not yet answered

Marked out of 2

Flag question

Feistel Cipher Structure is considered as example for:

- a. public-key encryption.
- b. Stream cipher.
- c. symmetric block ciphers.
- d. Cryptanalysis.

Clear my choice

in terms of symmetric encryption scheme ingredients, performing various substitutions and transformations on the plaintext can be done by:

- a. Secret key.
- b. Ciphertext.
- c. Encryption algorithm.
- d. cryptanalysis.

Clear my choice

In terms of symmetric encryption scheme ingredients, what are the inputs of encryption algorithm:

- a. key and Ciphertext.
- b. only key.
- c. key and plaintext.
- d. transformations function, key and plaintext.

Clear my choice

in terms of symmetric encryption scheme ingredients, what are the inputs of encryption algorithm:

- a. only key.
- b. key and plaintext.
- c. key and Ciphertext
- d. transformations function, key and plaintext

in terms of symmetric encryption scheme ingredients, The exact substitutions and transformations performed by the algorithm depend on.....

- a. Ciphertext.
- b. Encryption algorithm.
- c. Decryption algorithm.
- d. key.

Clear my choice

in terms of symmetric encryption scheme ingredients, the scrambled message produced as output, can be described as:

- a. Ciphertext.
- b. Encryption algorithm.
- c. Secret key.
- d. Plaintext.

Clear my choice

The Rail Fence encryption method is based on substitution in order to encrypt plain text

Select one:

- True
- False

In rail fence cipher we write message letters out diagonally over a number of columns

Select one:

- True
- False

Question 3
Answer saved
Marked out of 2
Flag question

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity, this can be described as:

- a. Privacy.
- b. nonrepudiation.
- c. Authenticity.
- d. Accountability.

Clear my choice

Question 4
Answer saved
Marked out of 2
Flag question

In terms of symmetric encryption scheme, using two different keys will produce the same ciphertexts

Select one:

- True
- False

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources, this can be described as:

- a. Accountability.
- b. Authenticity.
- c. countermeasure.
- d. Computer Security.

D