



NetExam

Sri Lanka Institute of Information Technology

Question 15

Not yet answered

Marked out of 1.0

Flag question

What is the most appropriate term for taking advantage of a weakness in the security of an

Select one:

- ☐ Threat
- ☒ Vulnerability
- ☐ Attack
- ☐ Exploit

MacBook Air



Question 16

Not yet answered
Marked out of 1.0
Flag question

Select incorrect statement regarding One-Time-Pad.

Select one:

- ☐ Key pad used to encrypt the data needs to be true random ✓
- ☒ Vulnerable to cryptanalytic attacks
- ☐ Key pad can only be used once ✓
- ☒ Length of the key pad used for encryption needs to be equal or higher than the length



on 18

t answered

d out of 1.0

question

Which three key security services are required to secure data at transit?

Select one or more:

- ☐ Authorization
- ☐ Accounting
- ☐ Confidentiality
- ☒ Integrity
- ☒ Authentication
- ☐ Anti-replay protection

Moodle



NetExam

Sri Lanka Institute of Information Technology

19

answered
out of 1.0
question

An encryption algorithm use a 22-bit key. What is the size of the key space? (Type only the numerical value)

Answer:

4194304

Next pa

MacBook Air

Moodle



NetExam

Sri Lanka Institute of Information Technology

Implementing proper accountability measures in an information system supports to achieve;

Select one or more:

- ☒ Deterrence
- ☒ Intrusion detection
- ☐ Integrity
- ☐ Authenticity
- ☐ Confidentiality

Next

MacBook Air



21

answered
of 1.0
question

The network security engineer for an e-commerce website requires a security service that prevents clients from claiming that genuine orders done by them are fake. Which security service provides this type of guarantee?

Select one:

- ☒ Authentication ✓
- ☐ Confidentiality
- ☐ Nonrepudiation
- ☐ Integrity
- ☐ Authentication

Next page

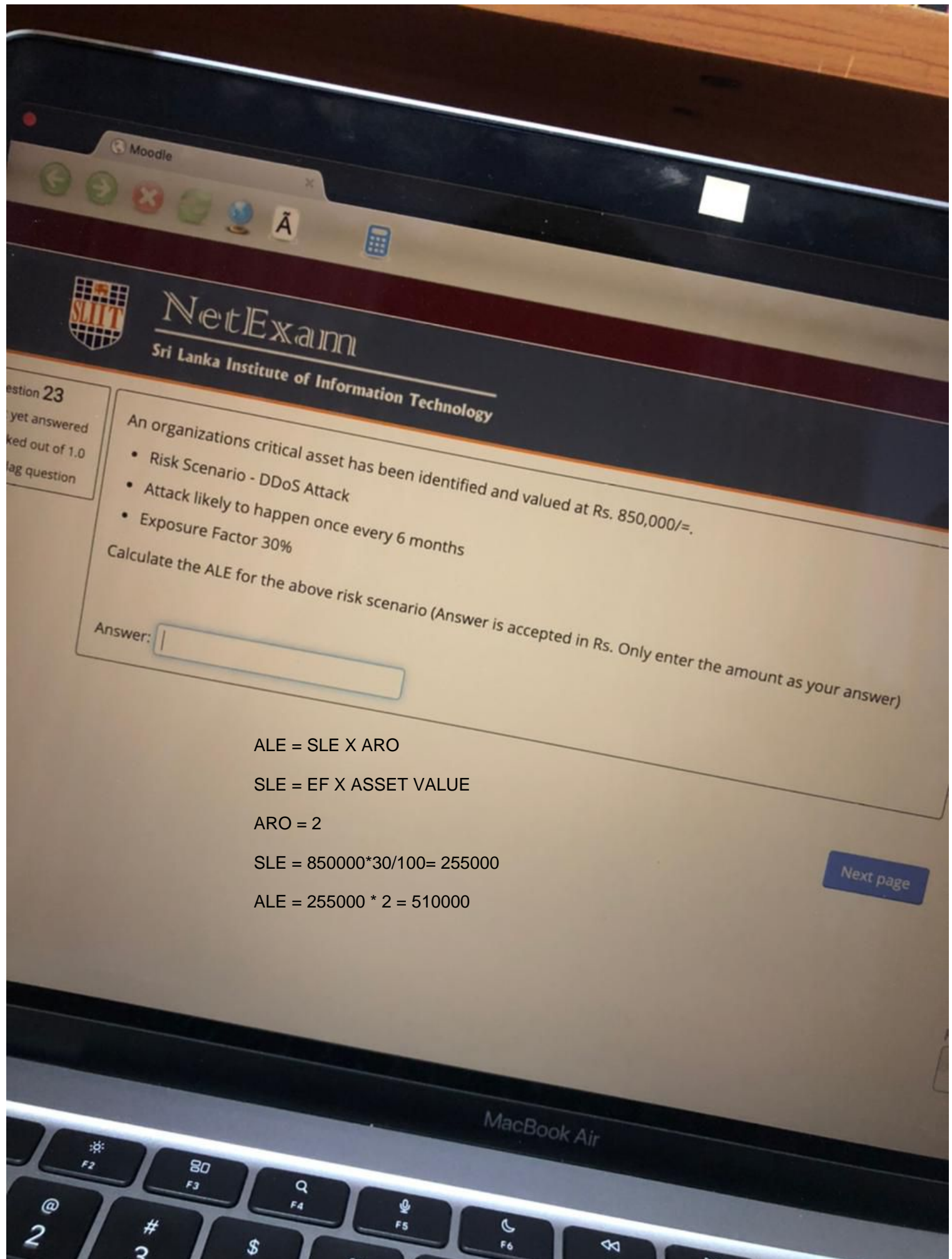


Not a feature available in mobile device management (MDM) solutions developed for BYOD / COPE Security.

Select one or more:

- ☐ Data Encryption
- ☐ Data Wipe
- ☐ Pin Enforcement
- ☐ Software code review
- ☐ Jailbreak Prevention
- ☐ SQL Injection Detection

Next page



$$ALE = SLE \times ARO$$

$$SLE = EF \times \text{ASSET VALUE}$$

$$ARO = 2$$

$$SLE = 850000 \times 30 / 100 = 255000$$

$$ALE = 255000 \times 2 = 510000$$



NetExam

Sri Lanka Institute of Information Technology

The following message was encrypted using a Caesar cipher with a key of 3:

Jrrg wr kdyh

What is the plaintext message?

Answer:

3 (23) good to have
3 (23) muuj zu ngbk



NetExam

Sri Lanka Institute of Information Technology

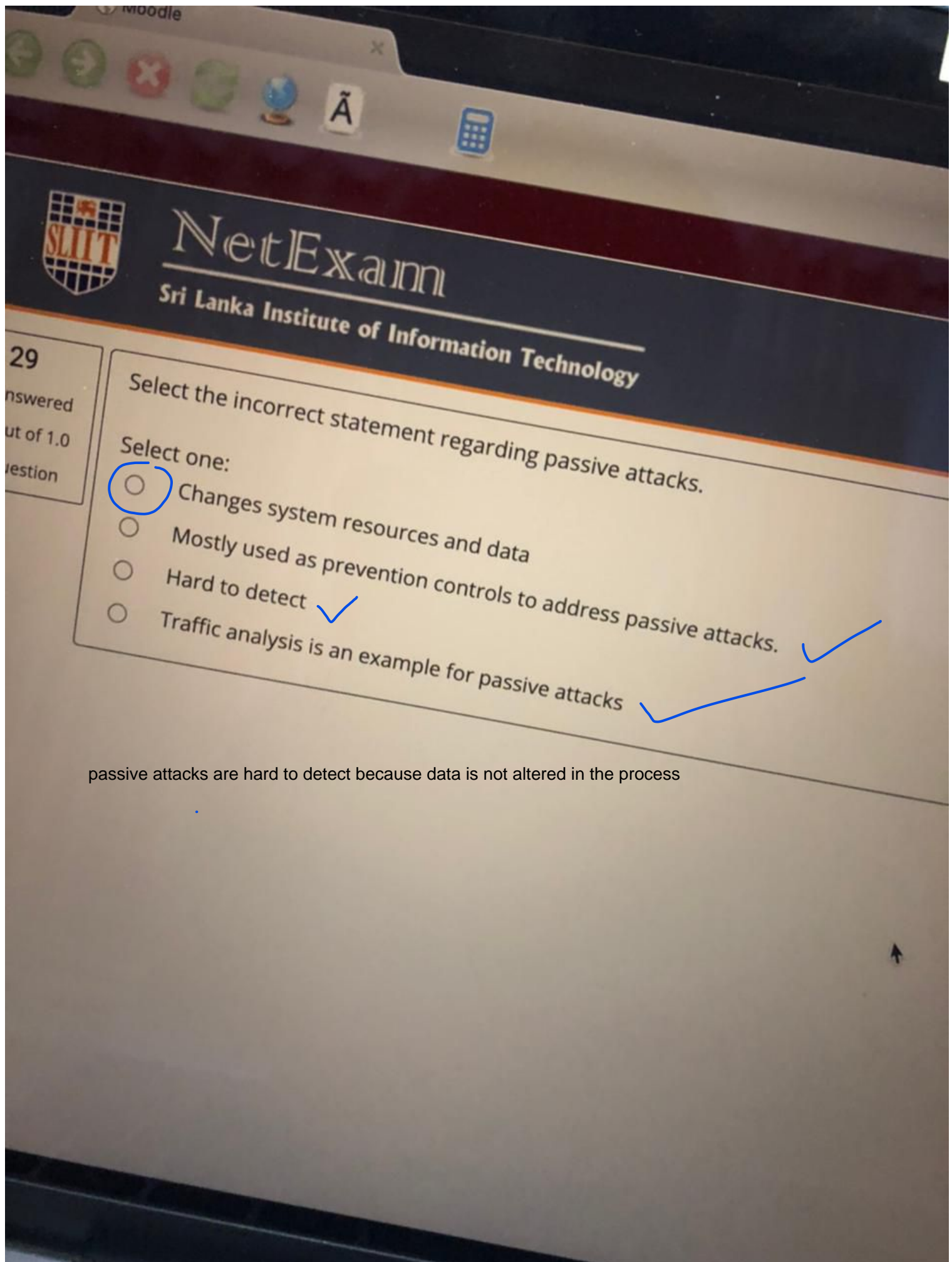
Question 28

Not yet answered
Marked out of 1.0
Flag question

Select passive attack(s) out of the following.

Select one or more:

- ☐ Denial of Service X
- ☐ Replay X
- ☐ Masquerade X
- ☐ Traffic analysis, if the data is encrypted
- ☐ Release of sensitive message contents



passive attacks are hard to detect because data is not altered in the process

Moodle



NetExam

Sri Lanka Institute of Information Technology

Question 27

Not yet answered
Marked out of 1.00
Flag question

Match the description to the suitable security objective.

Assures that the systems and data is available to be accessed by authorized users in a timely manner

Assures only the authorized users can view and access data

Assures that there are no intentional or unintentional unauthorized modifications of data

Assures that the users have the control over their own information being viewed, shared or stored

Choose...

Choose...

Choose...

Choose...

Next page

MacBook Air



Answered
out of 1.0
question

What is the mechanism used by developers of modern cryptographic algorithms to control brute-force attacks?

Select one:

- ☒ Use a key space large enough that it takes more money and more time to conduct a successful attack
- ☐ Utilize statistical analysis to avoid the most common encryption keys
- ☐ Use frequency analysis to assure that the most frequent letters used in the language are not used in the cipher message
- ☐ Use ciphers that requires the attacker to have both cipher-text and plain-text to conduct a successful attack

Next page



NetExam

Sri Lanka Institute of Information Technology

Question 8

Not yet answered

Marked out of 1.0

Flag question

Select the incorrect statement(s) regarding penetration testing.

Select one or more:

- ☒ Allows to identify security vulnerabilities in a system. ✓
- ☐ Is a mechanism use to fix vulnerabilities ✓
- ☐ Measures the compliance of organizations security policies ✓
- ☒ Mostly performed by black hat (bad) hackers
- ☐ Allows system owners to understand how vulnerabilities impact the systems ✓



Select the relevant block cipher mode matching to the description given.

Use to encrypt short amount of data.

Choose... ▼

Use to encrypt large amount of data with patterns.

Choose... ▼

More secure.

Choose... ▼

Both parallel encryption and decryption of blocks are possible.

Choose... ▼

Produce the same cipher text blocks for identical plain text blocks.

Choose... ▼

oodle



NetExam

Sri Lanka Institute of Information Technology

Question 3
Not yet answered
Marked out of 1.0
Flag question

Match the correct Quantitative Risk Analysis Term

Impact of a risk over the asset or percentage of asset loss

Amount that would be lost if the threat was realized once

Expected monetary loss for an asset due to a particular risk over an year

Term used to reflect the probability of threat taking place

- Choose...
- Choose...
- SLE
- ARO
- ~~AV~~
- EF
- ~~ARE~~
- ALE

EF
SLE
ALE
ARO

Next page

Quiz na

Finish attempt

Time left 0:5

30 MULTIPLE CHOICE QUESTIONS

1	2
8	9
15	16
22	23
29	30
FEEDBACK	
31	



NetExam

Sri Lanka Institute of Information Technology

An encryption algorithm use a 18-bit key. What is the size of the key space? (Type only the numerical value)

Answer:

~~2¹⁸~~





NetExam

Sri Lanka Institute of Information Technology

2

answered
out of 1.0
question

Which one of the following terms accurately describes the Caesar cipher?

Select one:

- ☐ Block cipher
- ☐ Strong cipher
- ☐ Transposition cipher
- ☒ Substitution cipher



Next page



NetExam

Sri Lanka Institute of Information Technology

Question 2

Not yet answered

Marked out of 1.0

Flag question

Select incorrect statement regarding One-Time-Pad.

Select one:

- ☐ Key pad can only be used once ✓
- ☐ Key pad used to encrypt the data needs to be true random ✓
- ☐ Vulnerable to cryptanalytic attacks
- ☐ Length of the key pad used for encryption needs to be equal or higher than the length of the message ✓

Next page



NetExam

Sri Lanka Institute of Information Technology

Question 9

Not answered
Marked out of 1.0
Flag question

What is the most appropriate term for taking advantage of a weakness in the security of a computer system?

Select one:

- ☒ Vulnerability
- ☐ Threat
- ☐ Exploit
- ☐ Attack

Select the relevant cipher type for the description.

Substitute one letter for another to create the cipher text from plain text

Caesar cipher is an example of;

Rail fence cipher is an example of;

Do not replace the letters in the cipher text;

permutation table

Choose...

Choose...

Substitution cipher

Transposition cipher

Choose...

Choose...

Choose...



Question 29

Not yet answered

Marked out of 1.0

Flag question

Match the controls to the appropriate control category.

Authentication function of the operating system

Choose...



Business continuity plan

Choose...



Data loss prevention software

Choose...



Security guard

Choose...



Keeping the entrance under lock and key

Choose...



Acceptable user policy

Choose...



Choose...

Administrative control

Physical control

Technical control





NetExam

Sri Lanka Institute of Information Technology

Question 20

Not yet answered

Marked out of 1.00

Flag question

Incapacitation, Corruption, and Obstruction are threat actions that cause _____ threat consequences.

Select one:

- ☐ usurpation
- ☒ disruption
- ☐ unauthorized disclosure
- ☐ deception



Question 23

Not yet answered

Marked out of 1.0

Flag question

What is true about Deterrent controls?

Select one:

- ☐ Designed to discourage errors or irregularities from occurring
- ☐ Updating firewall rules to block an attacking IP address is a Deterrent control
- ☐ Intended to discourage potential attackers and send the message that it is better not to attack
- ☐ Designed to find errors or irregularities after they have occurred



Question **27**

Not yet answered

Marked out of 1.0

Flag question

Which three key security services are required to secure data at transit?

Select one or more:

- ☐ Anti-replay protection
- ☒ Integrity ✓
- ☒ Confidentiality ✓
- ☒ Authentication ✓
- ☐ Accounting
- ☐ Authorization



NetExam

Sri Lanka Institute of Information Technology

Question 24

Not yet answered

Marked out of 1.0

Flag question

Spearphishing is:

Select one:

- ☐ A form of phishing that does not identify the recipient in some way
- ☒ A form of phishing that is only delivered by email ✓
- ☐ A form of phishing that targets only finance employees
- ☐ A form of phishing that identifies the recipient in some way