Moodle

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

Moodle

NetExam

Sri Lanka Institute of Information Technology

stion 16

yet answered

ed out of 1.0

ag 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

Moodle

NetExam

Sri Lanka Institute of Information Technology

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

MacBook Air

Moodle

NetExam

Sri Lanka Institute of Information Technology

19

nswered

ut of 1.0

uestion

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

Answer: $2^{22} = 4,194,304$ keys

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

Moodle

NetExam

Sri Lanka Institute of Information Technology

21

swered

of 1.0

stion

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

Not sure

Next page

MacBook Air

Moodle

NetExam

Sri Lanka Institute of Information Technology

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

MacBook Air

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 23

Not yet answered

Marked out of 1.0

Flag question

An organizations critical asset has been identified and valued at Rs. 850,000/=.

- Risk Scenario - DDoS Attack
- Attack likely to happen once every 6 months
- Exposure Factor 30%

Calculate the ALE for the above risk scenario (Answer is accepted in Rs. Only enter the amount as your answer)

Answer: Rs. 51000

$850000 \times \frac{30}{100} = 255000 \times 2$

$= 510000$

Next page

MacBook Air

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: Good to have

NetExam

Sri Lanka Institute of Information Technology

estion 28

yet answered

ked out of 1.0

lag question

Select passive attack(s) out of the following.

Select one or more:

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

Moodle

NetExam

Sri Lanka Institute of Information Technology

29

nswered

ut of 1.0

uestion

Select the incorrect statement regarding passive attacks.

Select one:

- Changes system resources and data
- Mostly used as prevention controls to address passive attacks.
- Hard to detect
- Traffic analysis is an example for passive attacks

Moodle

NetExam

Sri Lanka Institute of Information Technology

stion 27

yet answered

ed out of 1.0

g 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 — Choose...

Assures only the authorized users can view and access data — Choose...

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

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

Next page

MacBook Air

NetExam

Sri Lanka Institute of Information Technology

swered

t of 1.0

uestion

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

Select one:

- Use a keyspace 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

stion 8

yet answered

ked out of 1.0

Flag question

Select the incorrect statement(s) regarding penetration testing.

Select one or more:

- [x] 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

Moodle

NetExam

Sri Lanka Institute of Information Technology

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...

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

Next page

Quiz na

Finish attemp

Time left 0:5

30 MULTIPU

MATCHING

1 2 8 9 15 16 22 29 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: $2^{18} = 524,288$

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

stion 2

yet answered

ked out of 1.0

lag 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

on 9

et answered

ed out of 1.0

ag question

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

Select one:

- Vulnerabili
- Threat
- Exploit
- Attack

Sri Lanka Institute of Information Technology

Select the relevant cipher type for the description.

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

Caesar cipher is an example of; → S

Rail fence cipher is an example of; → T

Do not replace the letters in the cipher text; permutation table → transposition

Choose...

Choose...

Substitution cipher

Transposition cipher

Choose...

Choose...

Choose...

Sri Lanka Institute of Information Technology

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

20

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

NetExam

Sri Lanka Institute of Information Technology

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

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 3

Not yet answered

Marked out of 1.00

Flag question

Match the controls to the most suitable control category

Login warning banner	Deterrent Controls
Backup of important data	Recovery Controls
Security audit	Preventive controls
Encryption	Detective Controls

NetExam

Sri Lanka Institute of Information Technology

on 22

t answered

d out of

g question

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

Both parallel encryption and decryption of blocks are possible.	ECB	CBC
Use to encrypt large amount of data with patterns.	CBC	CBC
More secure.	CBC	EBC
Produce the same cipher text blocks for identical plain text blocks.	ECB	ECB
Use to encrypt short amount of data.	ECB	ECB

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 23

Not yet answered

Marked out of 1.00

Flag question

Select the incorrect statement(s) regarding penetration testing.

Select one or more:

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

Next page

Finish a

Time le

ACADE

1

30 MU

MATCH

1

8

15

22

29

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 19

Not yet answered

Marked out of 1.00

Flag question

Select the most accurate statement about cryptographic hash functions.

Select one:

- Produce a variable length output
- Use to provide confidentiality.
- Has a fixed length input
- One way hash function which is hard to invert

Next page

Sri Lanka Institute of Information Technology

Match the controls to the most suitable control category

Login warning banner — Choose...

Encryption — Choose...

Backup of important data — Choose...

Security audit — Choose...

- Choose...
- Recovery Controls
- Detective Controls
- Preventive controls
- Deterrent Controls

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 21

Not yet answered

Marked out of 1.00

Flag question

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

Select one or more:

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

Next page

CRC also something like hash

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 20

Not yet answered

Marked out of 1.00

Flag question

Not a suitable risk management mechanism

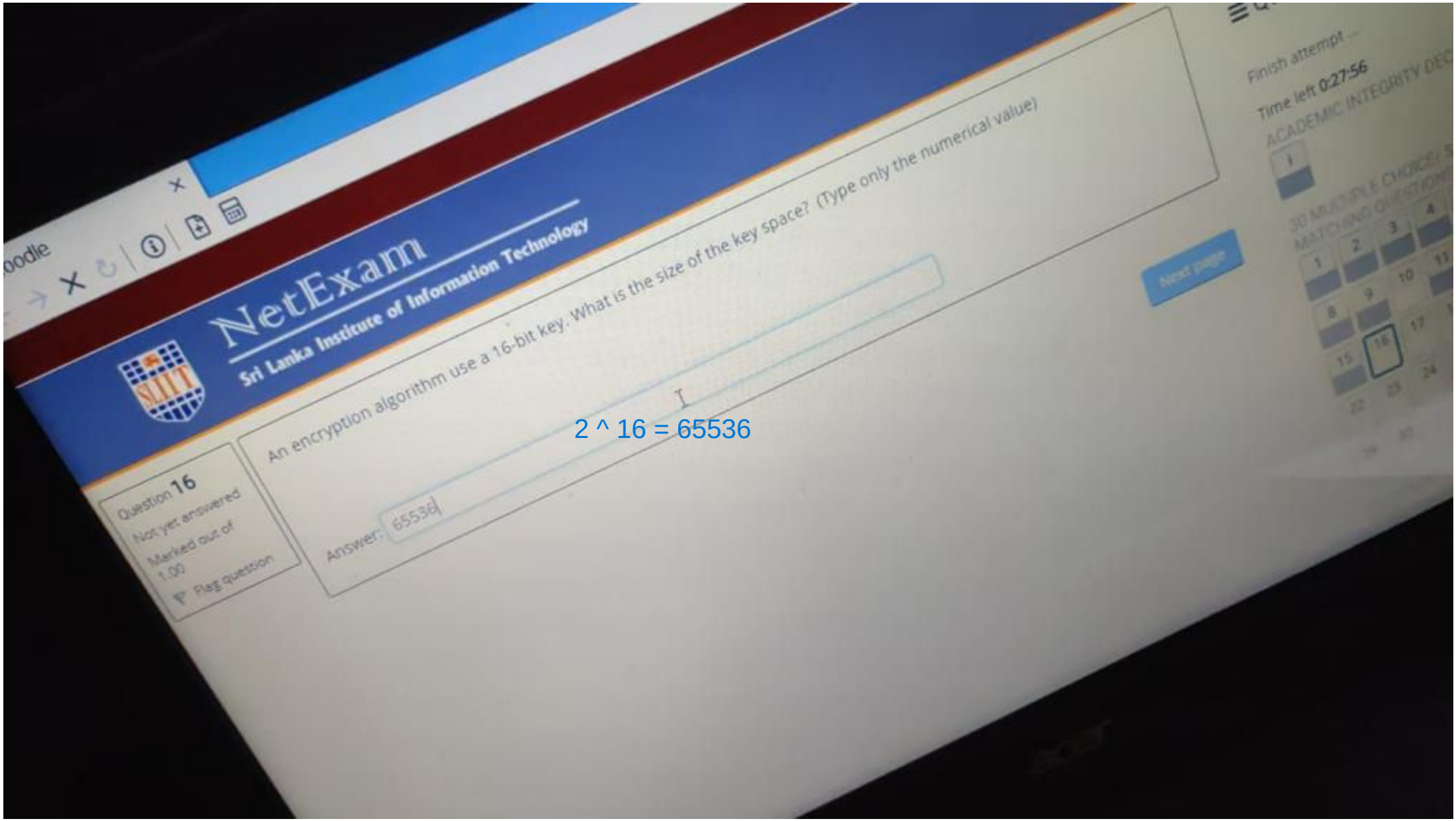
Select one:

- Mitigate the risk
- Transfer the risk
- Accept the risk
- Ignore the risk
- Avoid the risk

Quiz navig

Finish attempt ...

Time left 0:22:53


NetExam
Sri Lanka Institute of Information Technology
An encryption algorithm use a 16-bit key. What is the size of the key space? (Type only the numerical value)
Answer: 65536
Question 16
Not yet answered
Marked out of 1.00
Flag question
Finish attempt ...
Time left 0:27:56
Next page

2 ^ 16 = 65536

Moodle

it20180

NetExam

Sri Lanka Institute of Information Technology

Question **18**

Not yet answered

Marked out of 1.00

Flag question

Select the correct statement regarding keys used for encryption.

Select one:

- The sender and receiver must use the same key when using asymmetric encryption
- The sender and receiver must use two keys: one for symmetric encryption and another for asymmetric encryption
- The sender and receiver must use the same key when using symmetric encryption
- The sender and receiver must use the same keys for both symmetric and asymmetric encryption

NOT SURE

NetExam

Sri Lanka Institute of Information Technology

Question 17

Not yet answered

Marked out of 1.00

Flag question

An attacker intercepts an encrypted message and wants to identify what type of encryption algorithm was used to create the message. Attacker performs a frequency analysis and realize that the frequency of letters in the message closely matches the distribution of letters in the English language. What type of cipher was most likely used to create this cipher-text?

Select one:

- RSA
- AES
- Transposition cipher
- Substitution cipher
- 3DES

Next page

Quiz navigation

Finish attempt ...

Time left 0:26:31

ACADEMIC INTEGRITY DECLARA

30 MULTIPLE CHOICE/ SHORT MATCHING QUESTIONS (30 M

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

NetExam

Sri Lanka Institute of Information Technology

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

Select one:

- usurpation
- unauthorized disclosure
- disruption
- deception

Question 15

Not yet answered

Marked out of 1.00

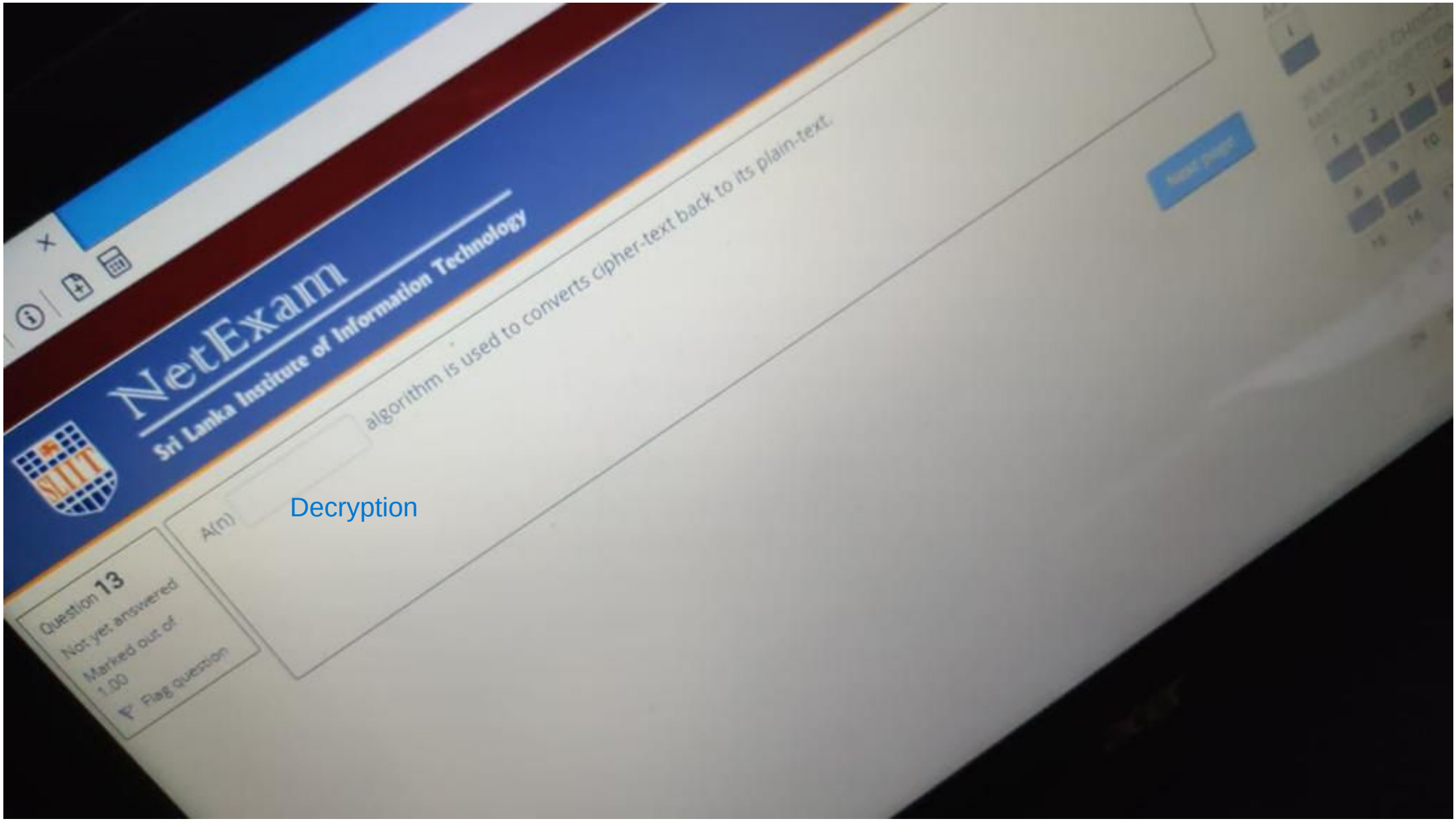
Flag question

Next page

Time

ACADEMIC

30 MULTIPLE CHOICE/ SHORT MATCHING QUESTIONS


NetExam
Sri Lanka Institute of Information Technology
algorithm is used to converts cipher-text back to its plain-text.
A(n)
Decryption
Question 13
Not yet answered
Marked out of 1.00
Flag question

NetExam

Sri Lanka Institute of Information Technology

Gray hat hackers _____ are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage.

Select one:

- White Hat Hackers
- Black Hat Hackers
- Gray Hat Hackers
- Red Hat Hackers

Next page

NetExam

Sri Lanka Institute of Information Technology

Question **8**

Not yet answered

Marked out of 1.00

Flag question

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

Select one:

- Strong cipher
- Substitution cipher
- Block cipher
- Transposition cipher

NetExam

Sri Lanka Institute of Information Technology

Match the description to the suitable security objective.

Assures only the authorized users can view and access data Confidentiality (Not sure)	Authorization
Assures that the systems and data is available to be accessed by authorized users in a timely manner	Authentication
Assures that the users have the control over their own information being viewed, shared or stored	Availability
Assures that there are no intentional or unintentional unauthorized modifications of data	Integrity

Integrity

Next page

NetExam

Sri Lanka Institute of Information Technology

Match the description to the suitable security objective.

Assures only the authorized users can view and access data	Authorization
Assures that the systems and data is available to be accessed by authorized users in a timely manner	Authentication
Assures that the users have the control over their own information being viewed, shared or stored	Availability
Assures that there are no intentional or unintentional unauthorized modifications of data	Integrity

Next page

NetExam

Sri Lanka Institute of Information Technology

Select the incorrect statement regarding passive attacks.

Select one:

- Hard to detect
- Mostly used as prevention controls to address passive attacks.
- Traffic analysis is an example for passive attacks
- Changes system resources and data

NetExam

Sri Lanka Institute of Information Technology

Select the incorrect statement(s) regarding penetration testing.

Select one or more:

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

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 7

Not yet answered

Marked out of 1.00

Flag question

Select incorrect statement regarding One-Time-Pad.

Select one:

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

NetExam

Sri Lanka Institute of Information Technology

An encryption algorithm use a 16-bit key. What is the size of the key space? (Type only the numerical value)

Answer: 2 ^ 16 = 65536

Next page

NetExam

Sri Lanka Institute of Information Technology

6

nswered

out of

question

A network of a IT-based software company consists of 300 workstations used by users and each user makes an average of $30 an hour out of it. Previously, none of the workstations involved in the network had anti-virus software installed. This was because there was no connection to the Internet and the acceptable use policy restricts users from using any external devices, so the risk of viruses was deemed minimal. One of the new implementation provides a broadband connection to the Internet, which employees can now use to send and receive email, and surf the Internet. One of the managers read in a trade magazine that other software companies have reported a 40% chance of viruses infecting their networks annually after installing this method of Internet connectivity, and that it may take up to 5 hours to restore data and applications that is been damaged or destroyed.

What is the annual loss that can be expected due to virus infections? (Type the numerical value only)

Answer:

SLE = EF*ASSET VALUE
= 40% * 300 * 30
= 300 * 30 * 40/100
= 3600

aro = 5

ALE = SLE * ARO
= 3600 * 5
= $ 18000

Next page

NetExam

Sri Lanka Institute of Information Technology

Question **5**

Not yet answered

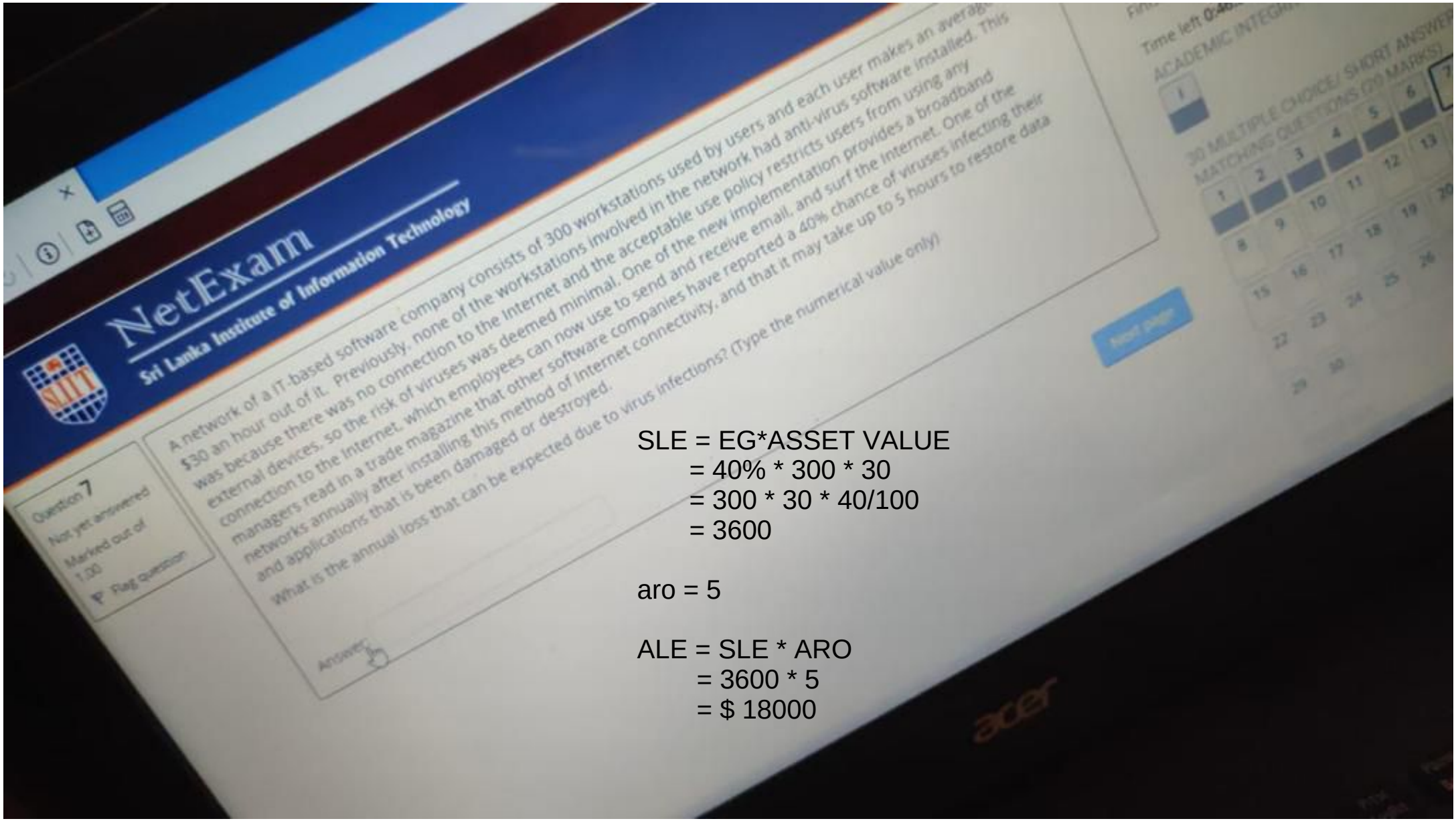
Marked out of 1.00

Flag question

What is the focus of cryptanalysis?

Select one:

- implementing encrypted codes
- Developing secret codes
- Hiding secret codes
- Breaking encrypted codes



SLE = EG*ASSET VALUE
= 40% * 300 * 30
= 300 * 30 * 40/100
= 3600

aro = 5

ALE = SLE * ARO
= 3600 * 5
= $ 18000

Question 1

Not yet answered

Marked out of 1.00

Flag question

Not a suitable risk management mechanism

Select one:

- Accept the risk
- Ignore the risk
- Transfer the risk
- Mitigate the risk
- Avoid the risk

NetExam

Sri Lanka Institute of Information Technology

Question 5

Not yet answered

Marked out of 1.00

Flag question

Select the correct statement(s) regarding block cipher and stream cipher.

Select one or more:

- Block ciphers are faster than stream cipher when they are used to encrypt data transmitted over networks.
- Stream ciphers encrypt 64-bits of data at once.
- Stream ciphers are less secure than Block ciphers in general.
- Block cipher encrypts an entire block of data at once.
- Stream ciphers do not increase the size of the cipher text than that of plain text.

Next page

30 MULTIPLE MATCHING QUES...

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

NetExam

Sri Lanka Institute of Information Technology

Question 6

Not yet answered

Marked out of 1.00

Flag question

Match the controls to the appropriate control category.

Security guard	Physical control
Acceptable user policy	Administrative control
Authentication function of the operating system	Technical control
Business continuity plan	Administrative control
Keeping the entrance under lock and key	Physical control
Data loss prevention software	Technical control

Computer/inform

three distinct

· Physi

Securi

NetExam

Sri Lanka Institute of Information Technology

vered

of

stion

What is true about Deterrent controls?

Select one:

- Designed to find errors or irregularities after they have occurred
- 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 discourage errors or irregularities from occurring

Moodle

NetExam

Sri Lanka Institute of Information Technology

Question 3

Not yet answered

Marked out of 1.00

Flag question

Match the controls to the most suitable control category

Login warning banner	Deterrent Controls
Backup of important data	Recovery Controls
Security audit	Preventive controls
Encryption	Detective Controls