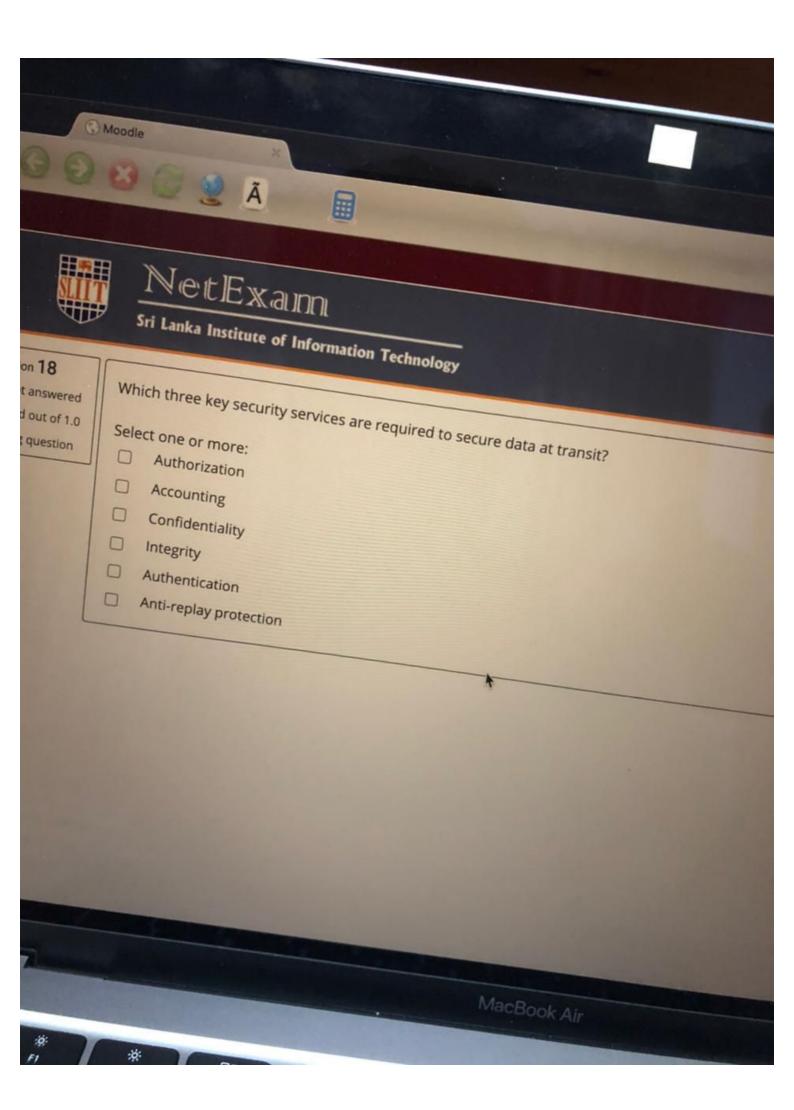
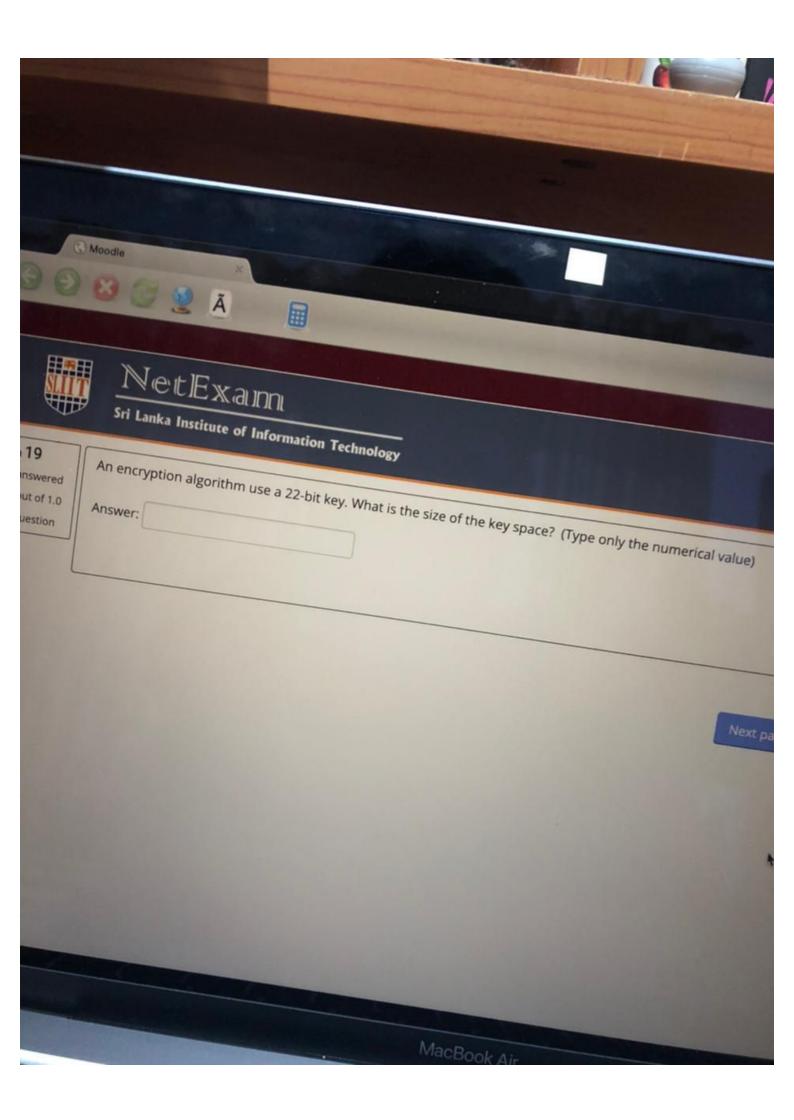
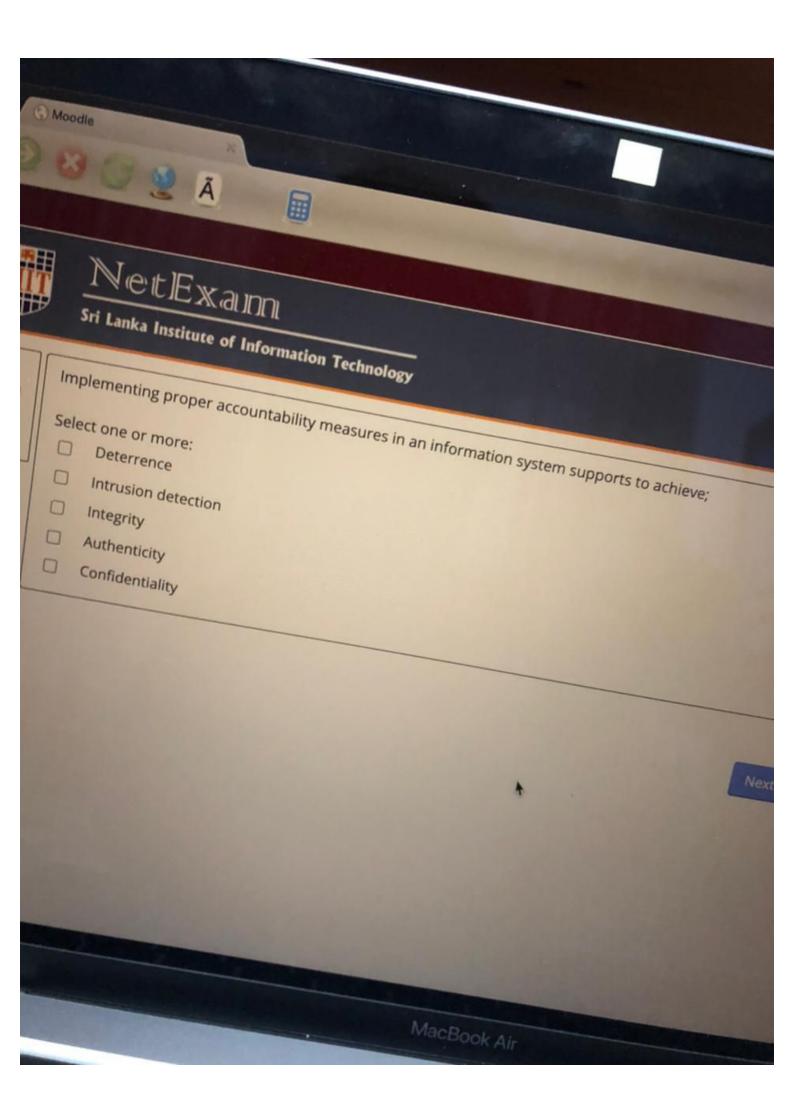


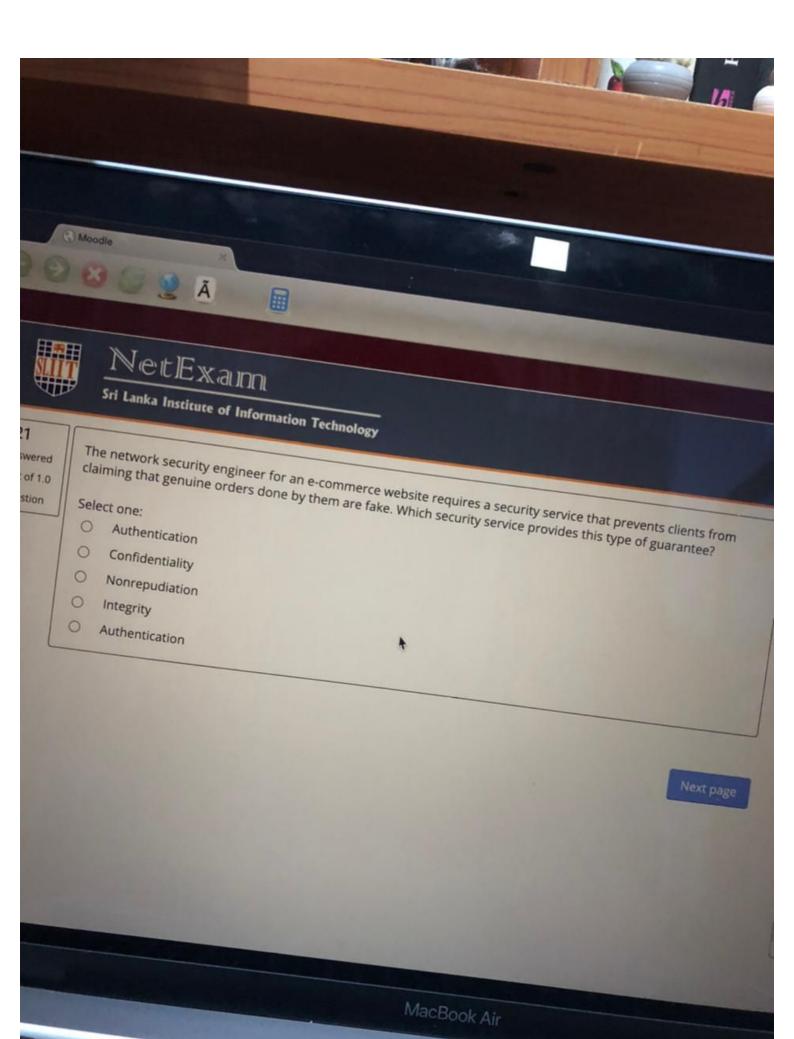
ed out of 1.0 ag question

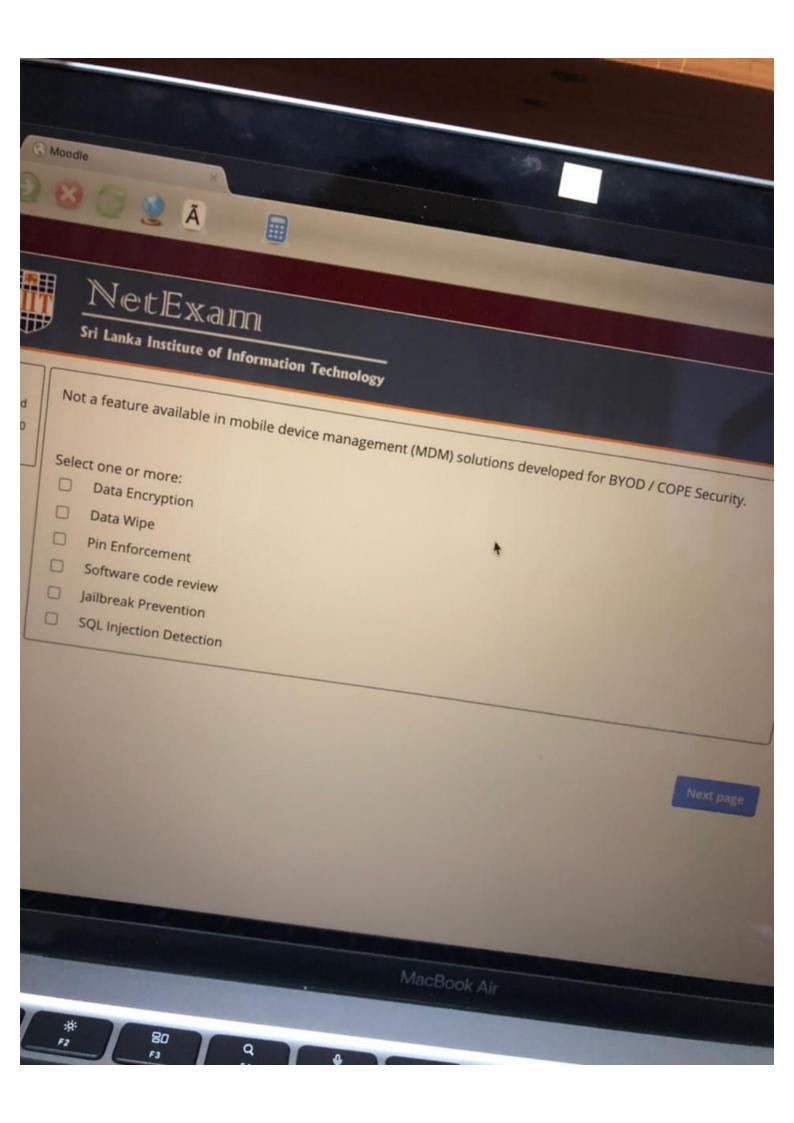
- Key pad used to encrypt the data needs to be true random
- Vulnerable to cryptanalytic attacks
- Key pad can only be used once 0
- Length of the key pad used for encryption needs to be equal or higher than the length

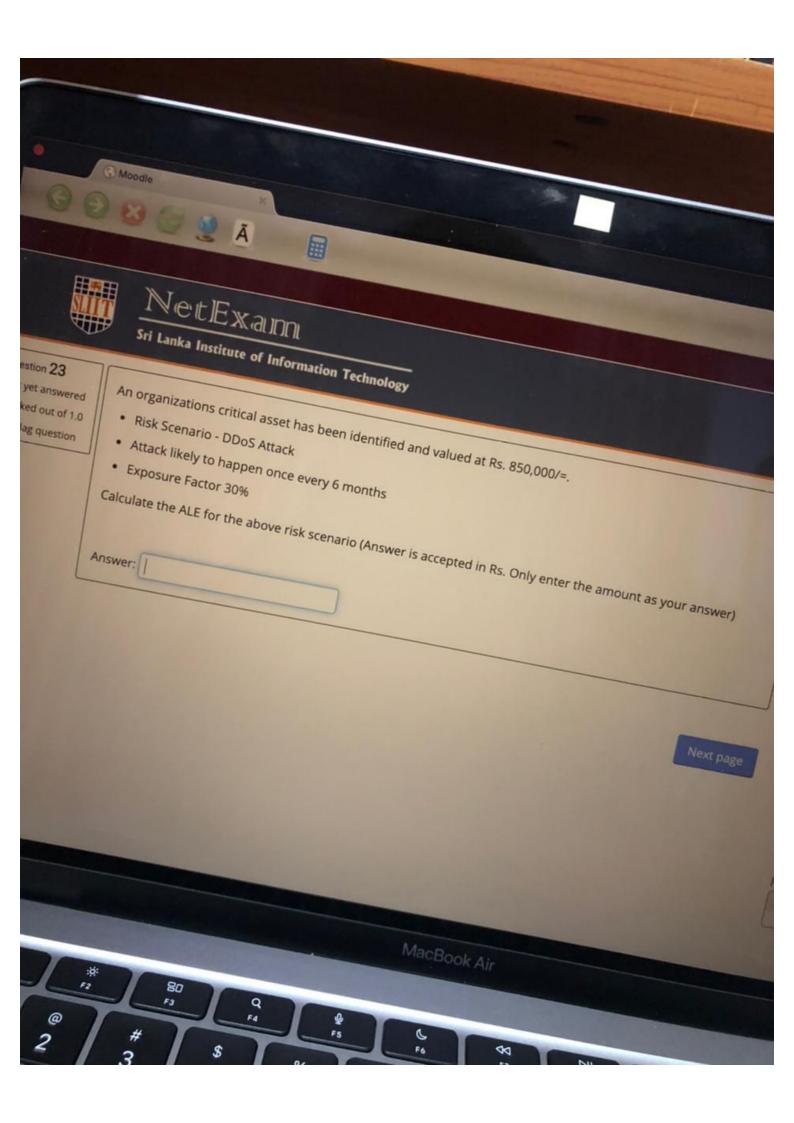


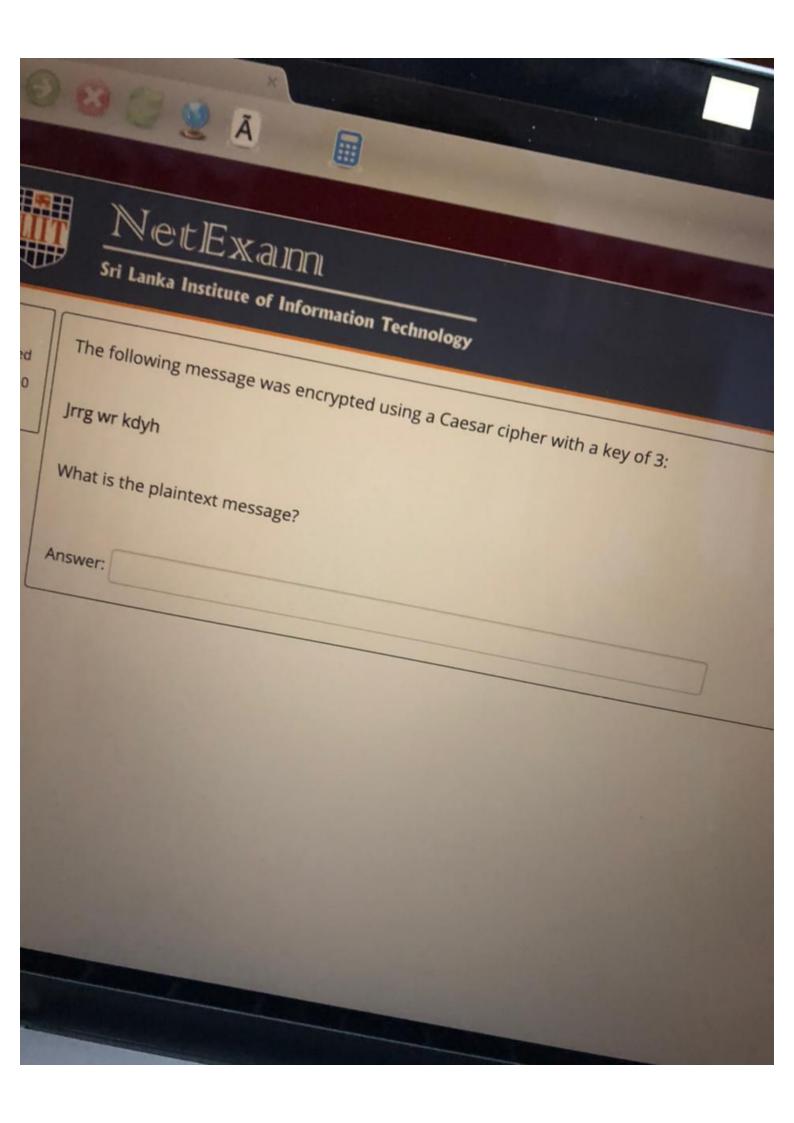


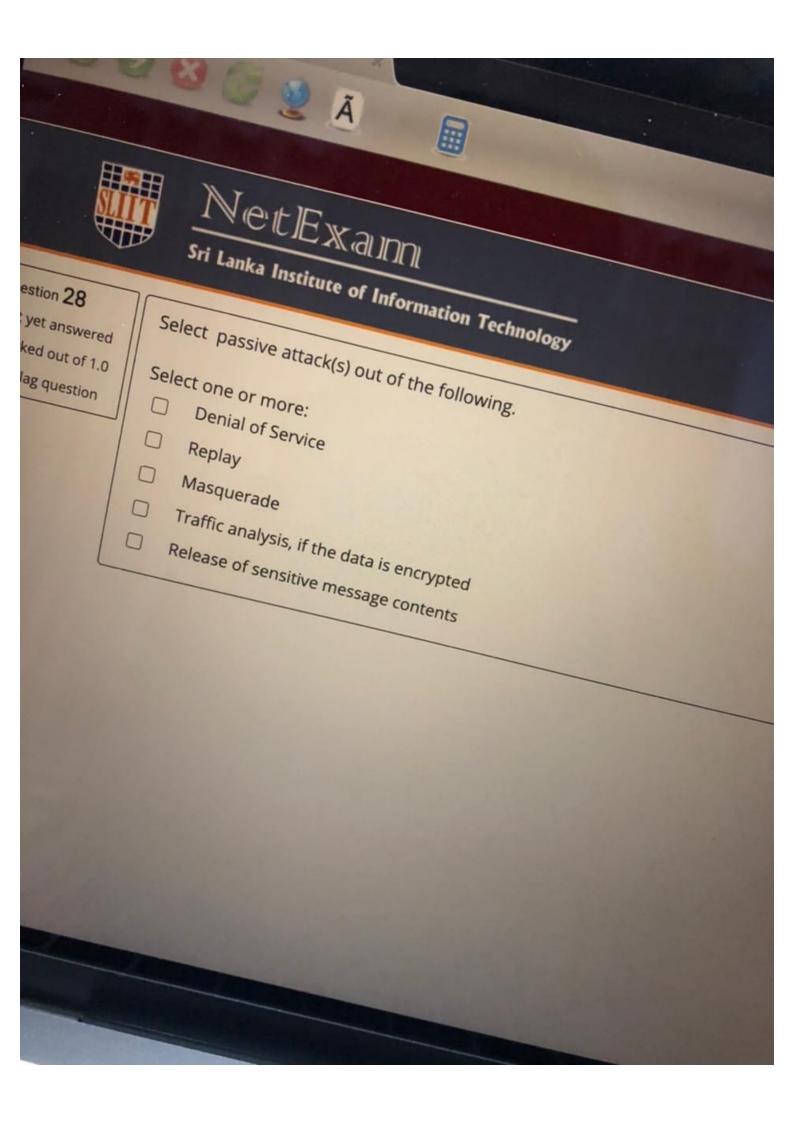


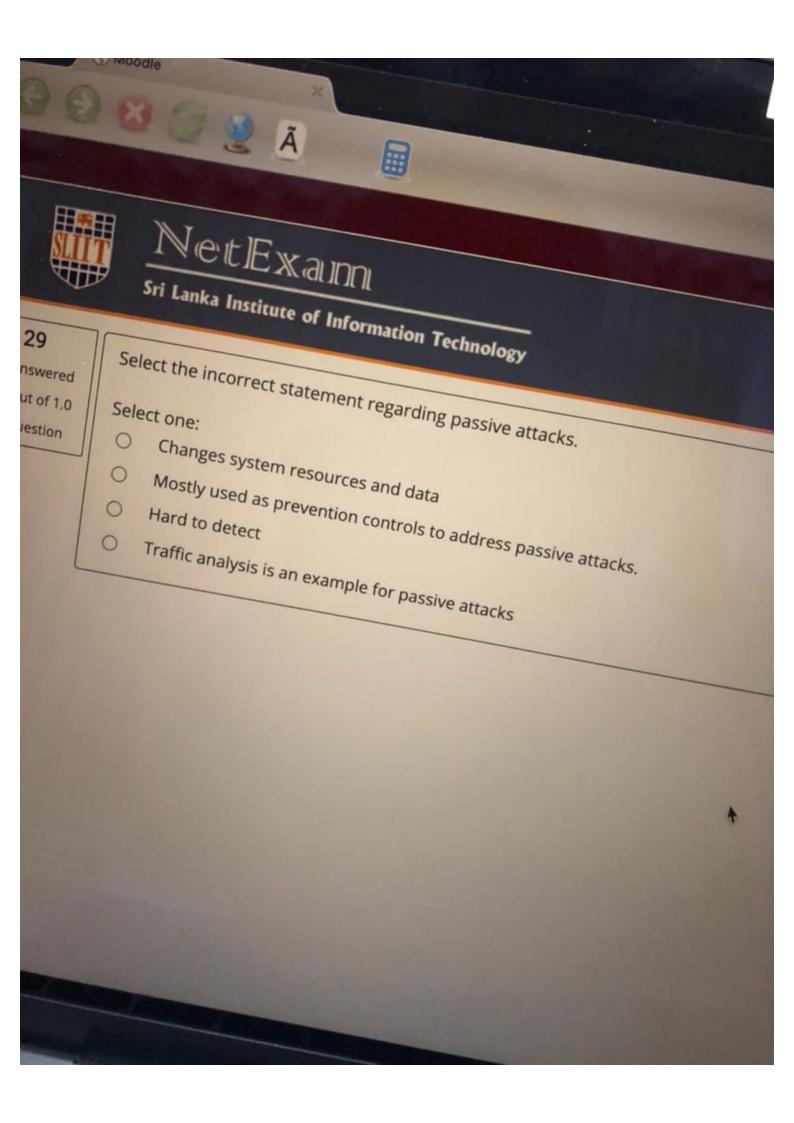


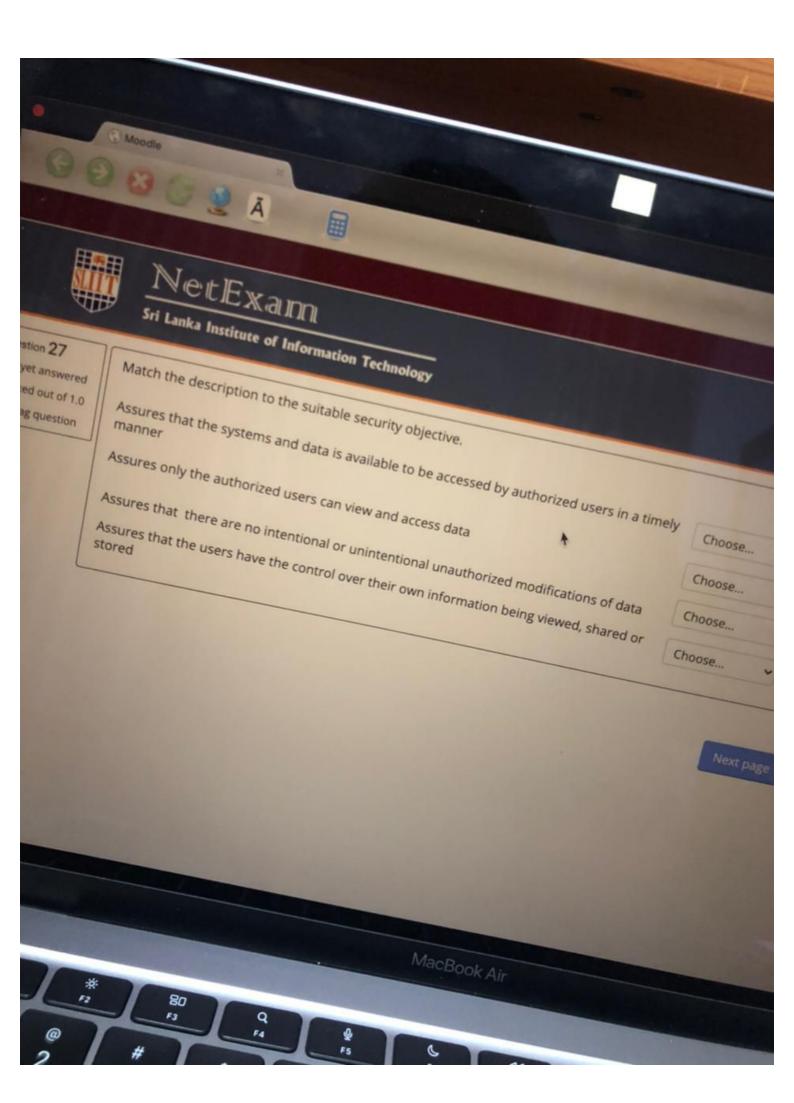














Sri Lanka Institute of Information Technology

swered at of 1.0 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



Sri Lanka Institute of Information Technology

yet answered ked out of 1.0 Select the incorrect statement(s) regarding penetration testing.

Select one or more:

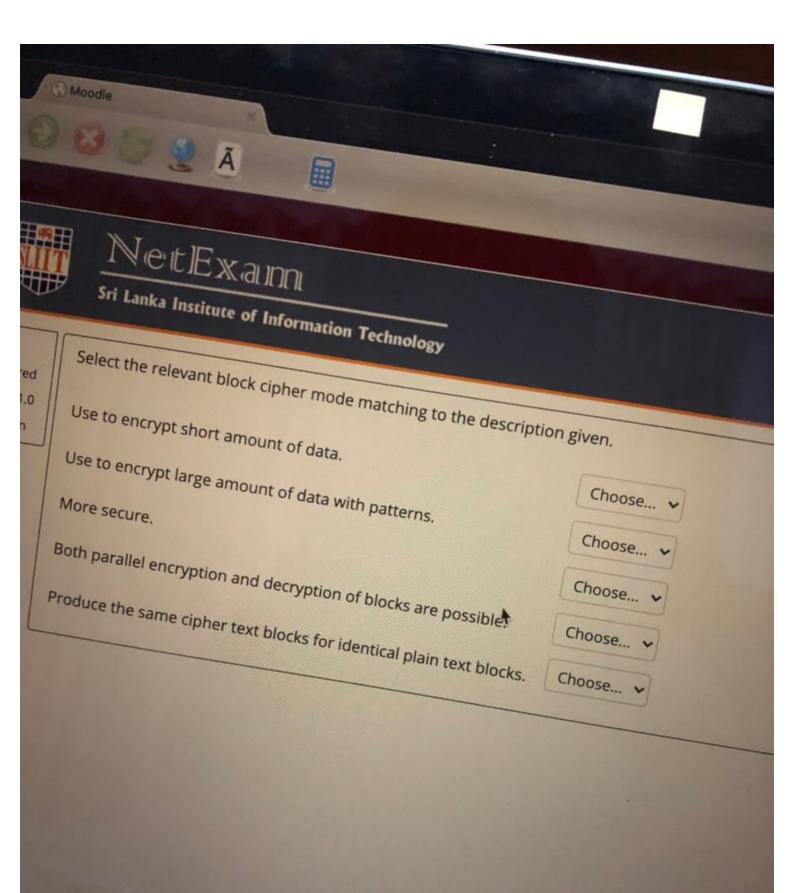
Allows to identify security vulnerabilities in a system.

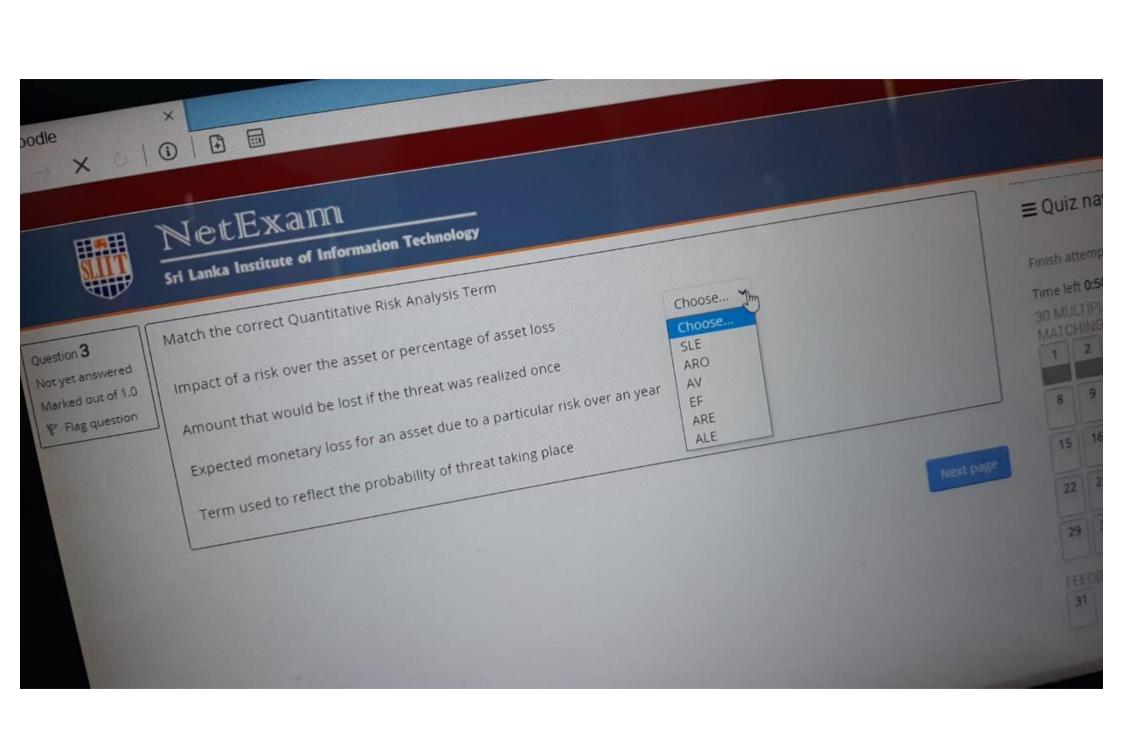
Is a mechanism use to fix vulnerabilities

Measures the compliance of organizations security policies

Mostly performed by black hat (bad) hackers

Allows system owners to understand how vulnerabilities impact the systems







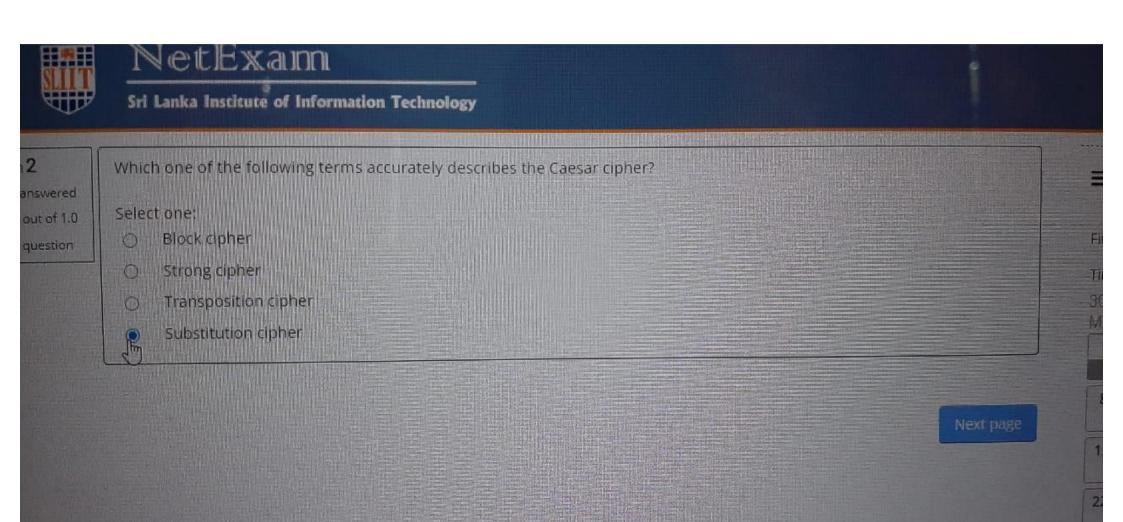
NetExainn

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
		y are definer lear value

Answer:

6



Sri Lanka Institute of Information Technology

ttion 2

yet answered

ked out of 1.0

lag question

Select Incorrect statement regarding One-Time-Pad.

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





Sri Lanka Institute of Information Technology

on **9** et answered ed out of 1.0

ag question

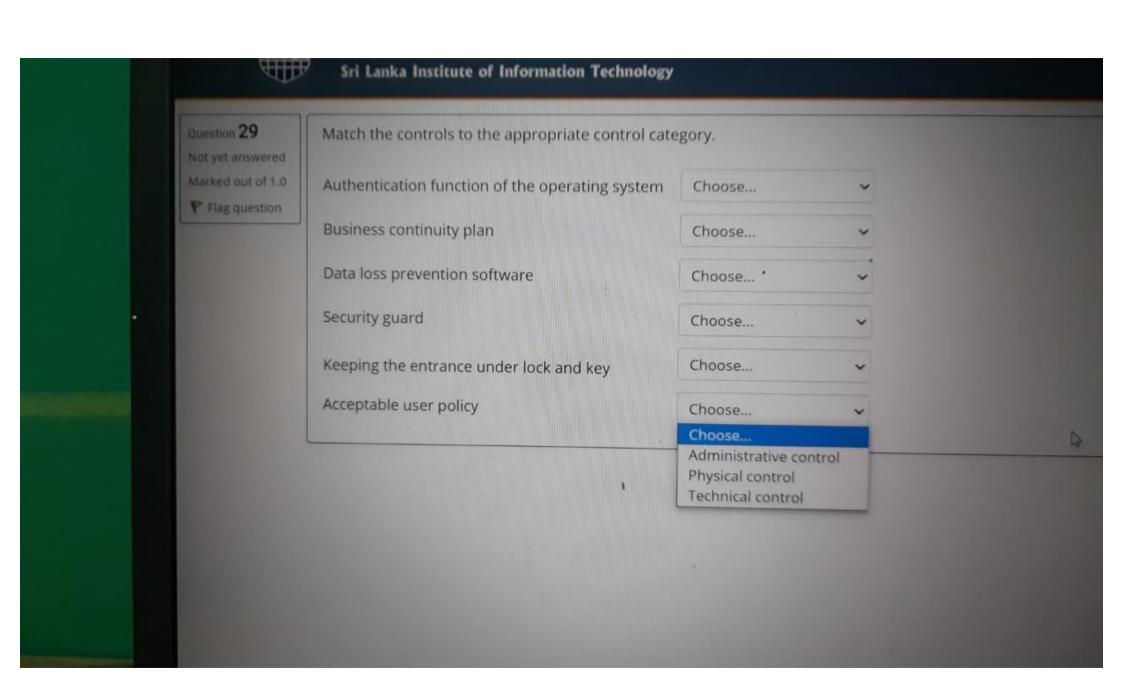
What is the most appropriate term for taking advantage of a weakness in the security of an computer system?

Select one:

- Vulnerabilit
- O Threat
- Exploit
- Attack

B

CIEX alm 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 Caesar cipher is an example of, Rail fence cipher is an example of, o not replace the letters in the cipher text: Choose... Choose... Substitution cipher Transposition cipher Choose... Choose... Choose...





Sri Lanka Institute of Information Technology

an 20

sed out of 1.0

the question

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

- usurpation
- disruption
- unauthorized disclosure
- deception

Sri Lanka Institute of Information Technology

Question 23

Not yet answered Marked out of 1.0

Y Flag question

What is true about Deterrent controls?

- 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
- O Designed to find errors or irregularities after they have occurred



Sri Lanka Institute of Information Technology

Question 27

Not yet answered

Marked out of 1.0

Y Clag 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



Sri Lanka Institute of Information Technology

Question 24

Not yet answered Marked out of 1.0

P Flag question

Spearphishing is:

- 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