

Online Exams

Sri Lanka Institute of Information Technology

Select incorrect statements about stream cipher.

Select one or more:

- ☐ Transform a fixed-length block of plain-text into a common block of cipher text of 64 or 128 bits.
- ☐ Vigenère cipher is an example of a stream cipher.
- ☐ Can be much faster than block cipher when used for data transmitted over networks.
- ☐ Encrypt plain-text one byte or one bit at a time.
- ☐ Size of cipher-text can become larger than plain-text.



Question 15

Not yet answered

Marked out of 1.00

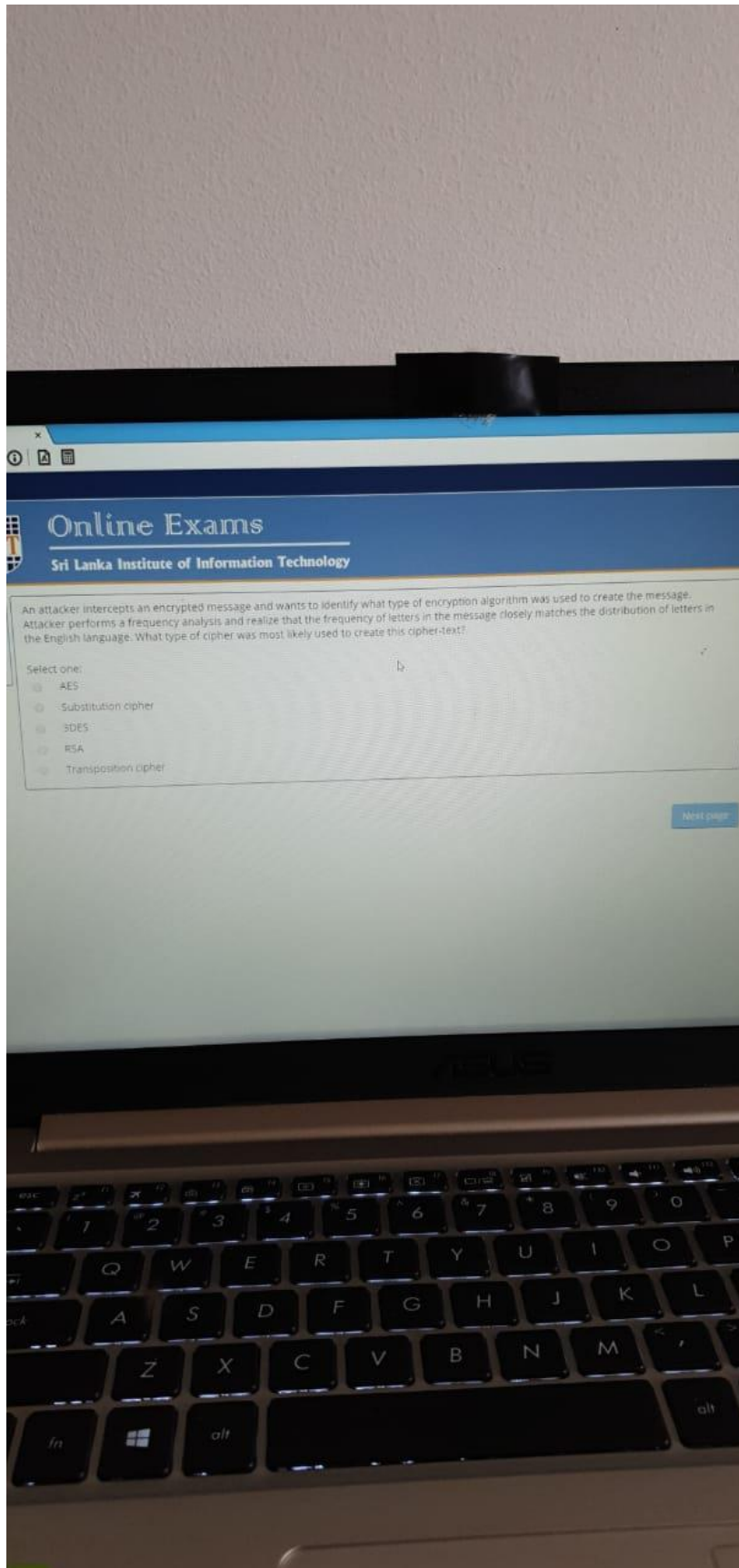
Flag question

Select the incorrect statement about single sign on systems .

Select one:

- ☐ Reduce the overhead of resetting passwords by system administrators
- ☐ Improve administrators ability of managing user accounts and access control
- ☐ Motivate users to use a strong password
- ☐ Reduce the possibility of single point of failure and total compromise of company IT assets

Next page





Online Exams

Sri Lanka Institute of Information Technology

access control policies control access based on the identity of the requestor and on access rules (authorizations) stating what requestors are allowed or not allowed to do.



Online Exams

Sri Lanka Institute of Information Technology

Match the description to the most relevant malicious software type/ category.

Design to provide continuous privileged access to computer systems

Rootkit ▼

Propagate usually by exploiting vulnerabilities

Choose... ▼

Advertising that is integrated in to software

Adware ▼

Malware code consist of portable instructions and works in different platforms

Choose... ▼

Any mechanism that bypass regular security measures when accessing systems

Choose... ▼

← → × ↺ ⓘ A

Sri Lanka Institute of Information Technology

Question 13
Not yet answered
Marked out of 1.00
Flag question

Match the description to the relevant phase of life-cycle of virus.

Releases the payload.	Triggering phase
Gets activated to perform the task virus is designed to perform	Choose...
Does not perform any activity	Choose...
Tries to get infected to other files and systems	Choose...

Choose...

Choose...

Triggering phase

Execution phase

Dormant phase

Propagation phase

Choose...

Next page

Quiz navigation

MULTIPLE CHOICE QUESTIONS

1	2	3
4	5	10
15	16	17
22	23	24
29	30	31
36	37	38
43	44	45
50	51	52
57	58	59
61		

FEEDBACK (0)

file x

× ↺ ⓘ A

Online Exams

Sri Lanka Institute of Information Technology

A(n) tool kit can be used to create sophisticated malware with advance payloads and propagation mechanisms.

Next page



Online Exams

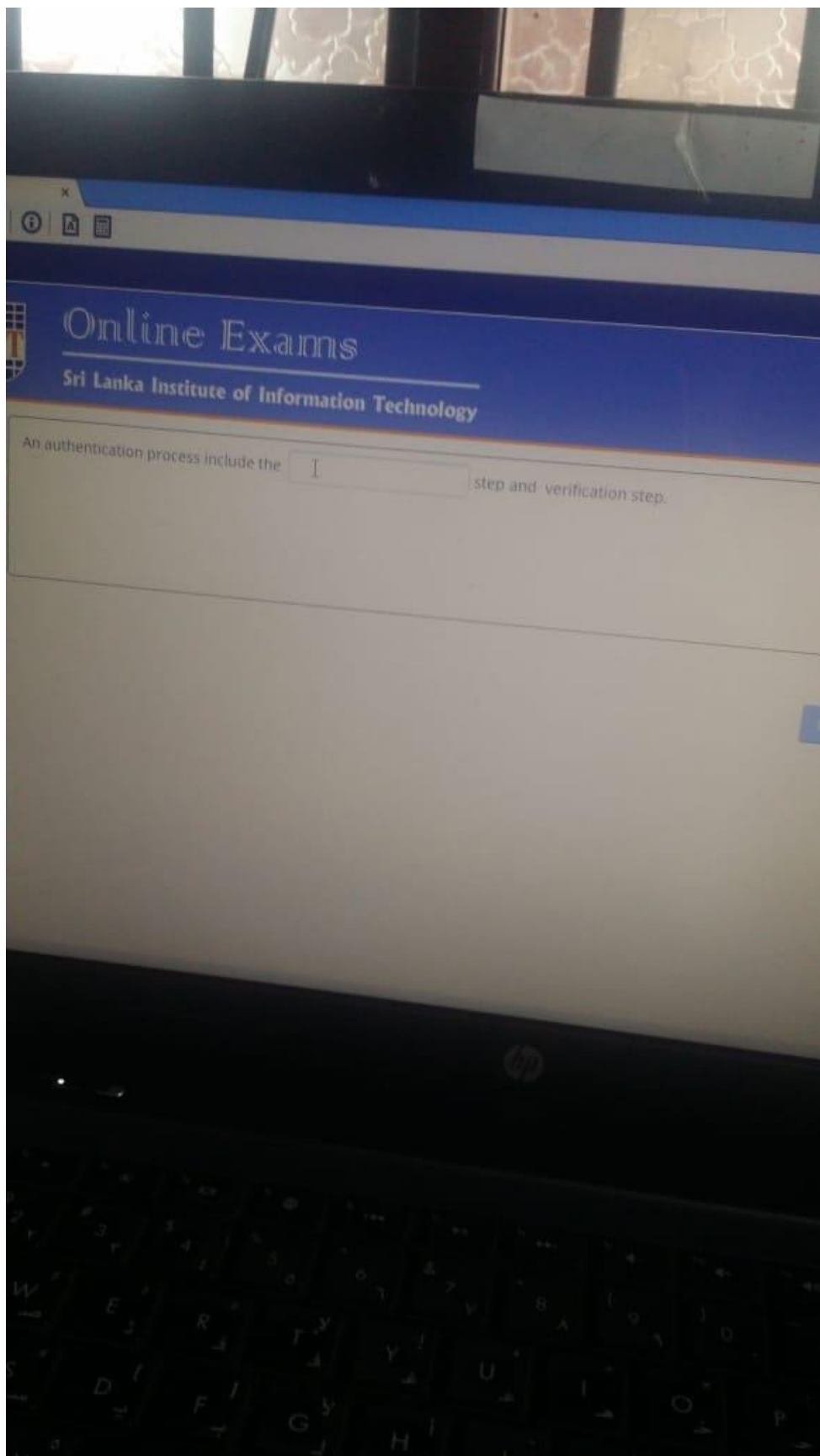
Sri Lanka Institute of Information Technology

wered
of
estion

Recognition by hand writing, voice, typing pattern are examples of _____.

Select one:

- ☐ Static biometrics
- ☐ Face recognition
- ☐ Token authentication
- ☐ Dynamic biometrics





Online Exams

Sri Lanka Institute of Information Technology

4

answered
out of
question

A _____ strategy is one in which the system time to time runs its own password brute force tools to find weak passwords.

Select one:

- ☐ User education
- ☐ Proactive password checking
- ☐ Reactive password checking
- ☐ Computer-generated password

Next page

MUX
QUE
1
9
17
25
33
41
49
57
58



Online Exams

Sri Lanka Institute of Information Technology

Match the controls to the most suitable control category

Encryption

Detective Controls ▼

Backup of important data

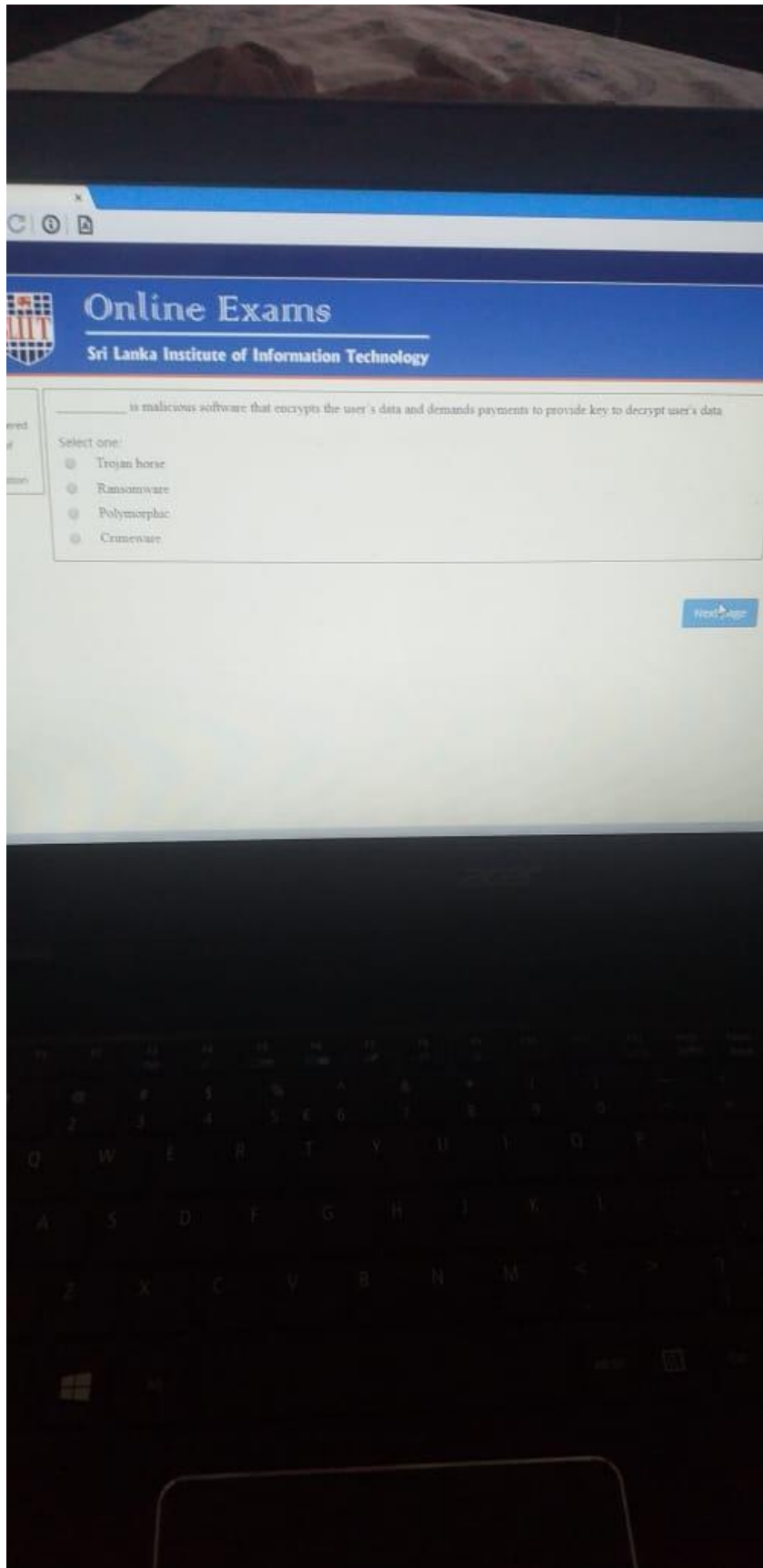
Preventive controls ▼

Security audit

Recovery Controls ▼

Login warning banner

Deterrent Controls ▼



Online Exams

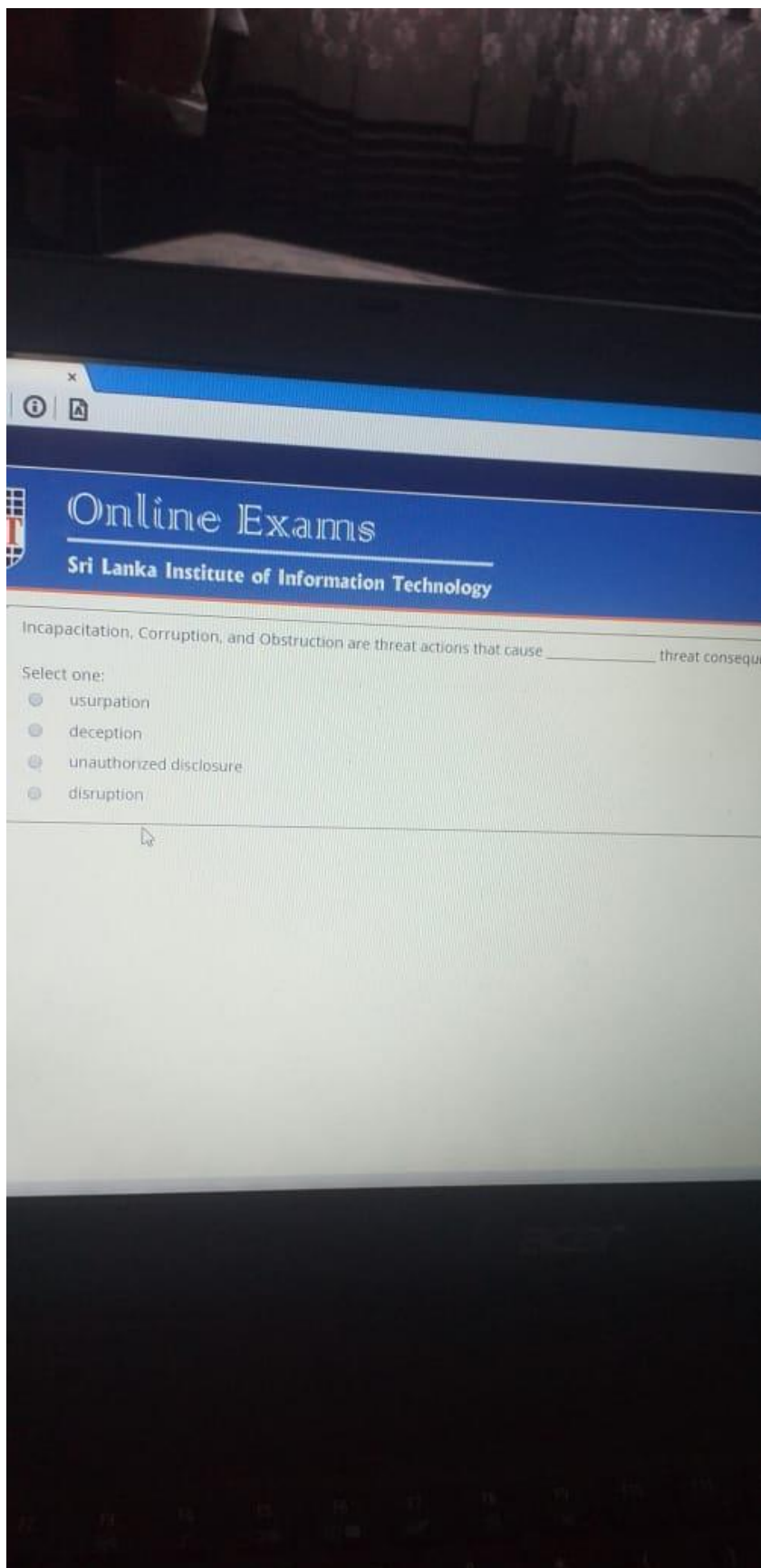
Sri Lanka Institute of Information Technology

_____ is malicious software that encrypts the user's data and demands payments to provide key to decrypt user's data

Select one:

- ☐ Trojan horse
- ☐ Ransomware
- ☐ Polymorphic
- ☐ Crimeware

Next Page



Online Exams

Sri Lanka Institute of Information Technology

Incapacitation, Corruption, and Obstruction are threat actions that cause _____ threat consequence

Select one:

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



Question 19

Not yet answered

Marked out of 1.00

Flag question

_____ Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

Select one:

- ☐ RBAC
- ☐ MAC
- ☐ DAC
- ☐ NAC

Next page

How digital signature creation and verification process is performed for a message transmitted over a network.

Select one:

- ☐ Creation is done by encrypting the hash value of the message with the private key of the sender. Verification is done by decrypting the digital signature with the corresponding public key.
- ☐ Creation is done by encrypting the hash value of the message with the shared key of the sender. Verification is done by decrypting the digital signature with the corresponding shared key.
- ☐ Creation is done by encrypting the hash value of the message with the public key of the sender. Verification is done by decrypting the digital signature with the corresponding private key.
- ☐ Creation is done by encrypting the hash value of the message with the public key of the receiver. Verification is done by decrypting the digital signature with the corresponding private key.



Online Exams

Sri Lanka Institute of Information Technology

A network of a IT-based company consists of 250 workstations used by users and each user makes an average of \$20 an hour out. 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. The new implementation provides a broadband connection to the Internet, which employees can now use to send and receive emails and surf the Internet. One of the managers read in a trade magazine that other software companies have reported a 50% chance of virus infections their networks annually after installing this method of Internet connectivity, and that it may take up to 3 hours to restore 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:



Online Exams

Sri Lanka Institute of Information Technology

Two users Alice and Bob use Diffie-Hellman key exchange with a common prime number $p = 23$ and generator $g = 5$ (which is a primitive root module 23). Let 4 and 3 be the private keys of Alice and Bob respectively. What is the common shared secret key? (Write the numerical value)

Answer:

Match the controls to the appropriate control category.

Security guard

Physical control ▼

Data loss prevention software

Technical control ▼

Authentication function of the operating system

Technical control ▼

Keeping the entrance under lock and key

Physical control ▼

Business continuity plan

Administrative control ▼

Acceptable user policy

Administrative control ▼



Online Exams

Sri Lanka Institute of Information Technology

A(n)

tool kit can be used to create sophisticated malware with advance payloads and propagation mechanisms.

Next page



Online Exams

Sri Lanka Institute of Information Technology

What is the difference between access control list (ACL) and capability ticket (CT).

Select one:

- ☐ There is no difference between ACL and CT.
- ☐ ACL is used for access control while CT are used to define the privileges of users within a system.
- ☐ ACL determines what access rights a user has on different objects while CT lists users and their access rights to access a particular object.
- ☐ ACL lists users and their access rights to access a particular object while CT determines what access rights a user has on different objects.

Next page



Online Exams

Sri Lanka Institute of Information Technology

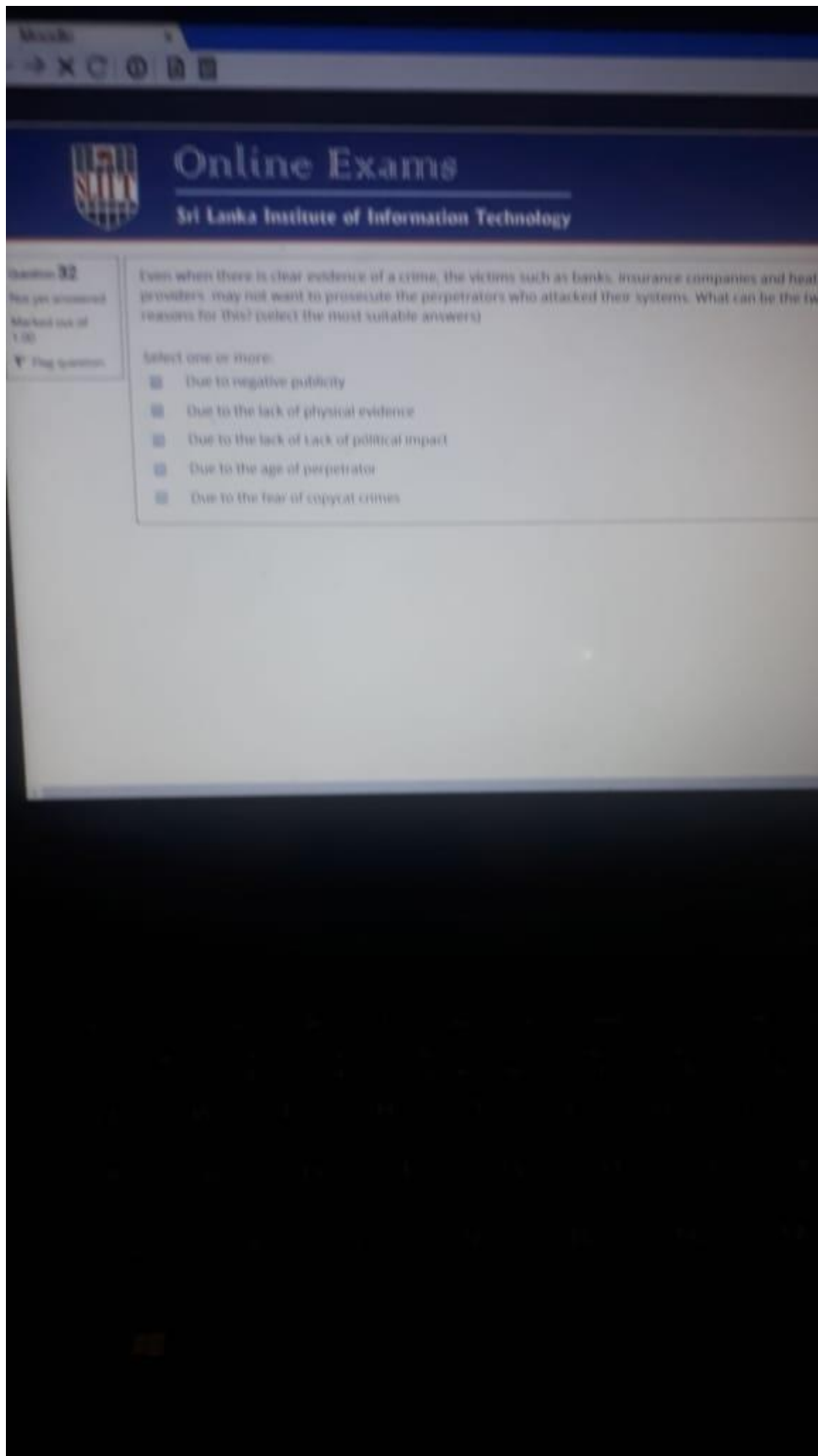
Question 30

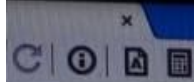
Not yet answered

Marked out of
1.00

🚩 Flag question

A(n) algorithm is used to convert cipher-text back to its plain-text.





Online Exams

Sri Lanka Institute of Information Technology

red

ion

_____ is a form of crime that targets a computer system to acquire information stored on that system, to control the target system without authorization or payment, or to alter the integrity of data or information, or the availability of the computer or server.

Select one:

- ☐ Computers as mediums
- ☐ Computers as storage devices
- ☐ Computers as targets
- ☐ Computers as communication tools



Online Exams

Sri Lanka Institute of Information Technology

Question 17

Not yet answered

Marked out of 1.00

Flag question

How digital signature creation and verification process is performed for a message transmitted over a network.

Select one:

- ☒ Creation is done by encrypting the hash value of the message with the public key of the sender. Verification is done by the receiver of the message by decrypting the digital signature with the corresponding private key.
- ☐ Creation is done by encrypting the hash value of the message with the private key of the sender. Verification is done by the receiver of the message by decrypting the digital signature with the corresponding public key.
- ☐ Creation is done by encrypting the hash value of the message with the shared key of the sender. Verification is done by the receiver of the message by decrypting the digital signature with the corresponding shared key.
- ☐ Creation is done by encrypting the hash value of the message with the public key of the receiver. Verification is done by the receiver of the message by decrypting the digital signature with the corresponding private key.

Next page

Quiz

MULTIPLE QUESTION

1 2

3 4

5 6

7 8

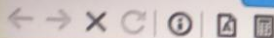
9 10

11 12

13 14

15 16

Moodle



Online Exams

Sri Lanka Institute of Information Technology

Question 18

Not yet answered

Marked out of 1.00

Flag question

Select incorrect statement regarding One-Time-Pad.

Select one:

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



What are the most suitable controls against workstation hijacking?

Select one or more:

- ☐ Automatic logout after certain period inactivity.
- ☐ Use of challenge-response protocols
- ☐ Use of anomaly-based intrusion detection scheme to detect changes in user behaviour.
- ☐ Enforcement of password policy to make password difficult to guess.



Online Exams

Sri Lanka Institute of Information Technology

40

answered

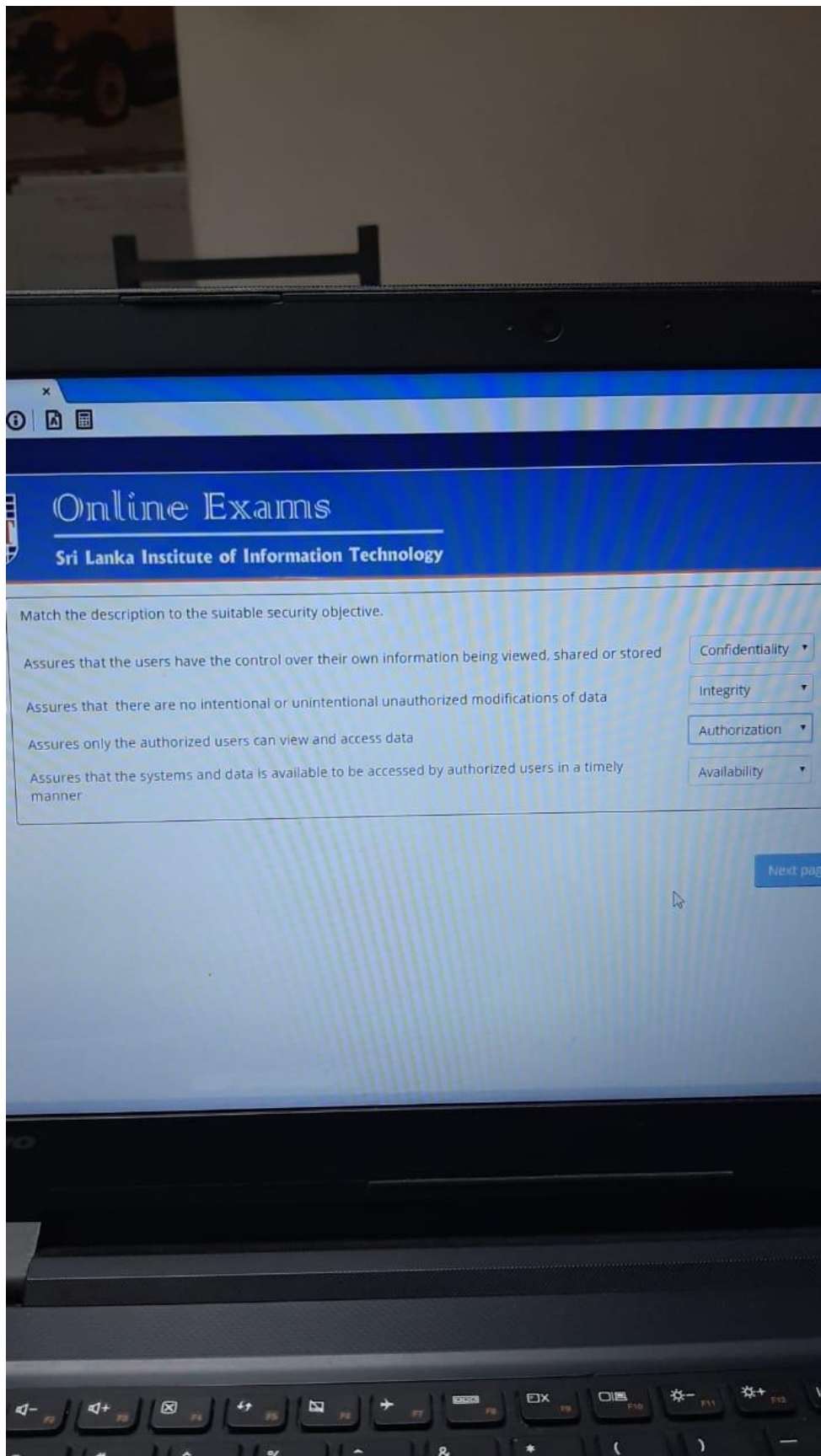
out of

question

Select the correct statement regarding public-key cryptographic algorithms.

Select one:

- ☐ They have secure key lengths ranging from 80 to 256 bits
- ☐ They are relatively slow because they are based on difficult computational algorithms
- ☐ They include DES, RC4, and AES
- ☐ They are also called conventional cryptographic algorithms





Online Exams

Sri Lanka Institute of Information Technology

A network of a IT-based company consists of 250 workstations used by users and each user makes an average of \$20 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 50% chance of viruses infecting their networks annually after installing this method of Internet connectivity, and that it may take up to 3 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:

Next page

≡ Quiz n

MULTIPLE C
QUESTIONS

1	2
9	10
17	18
25	26
33	34
41	42
49	50
57	58



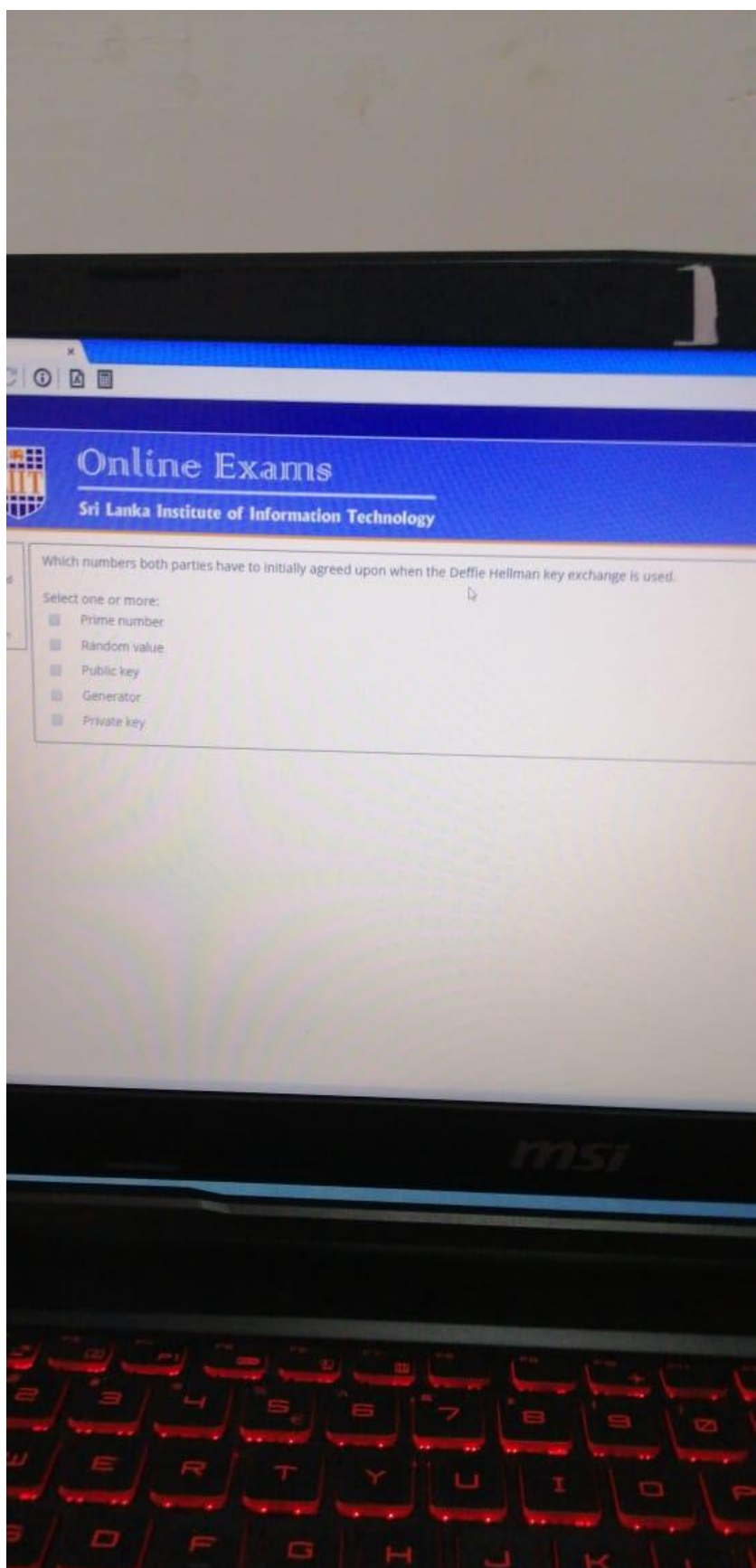
Sri Lanka Institute of Information Technology

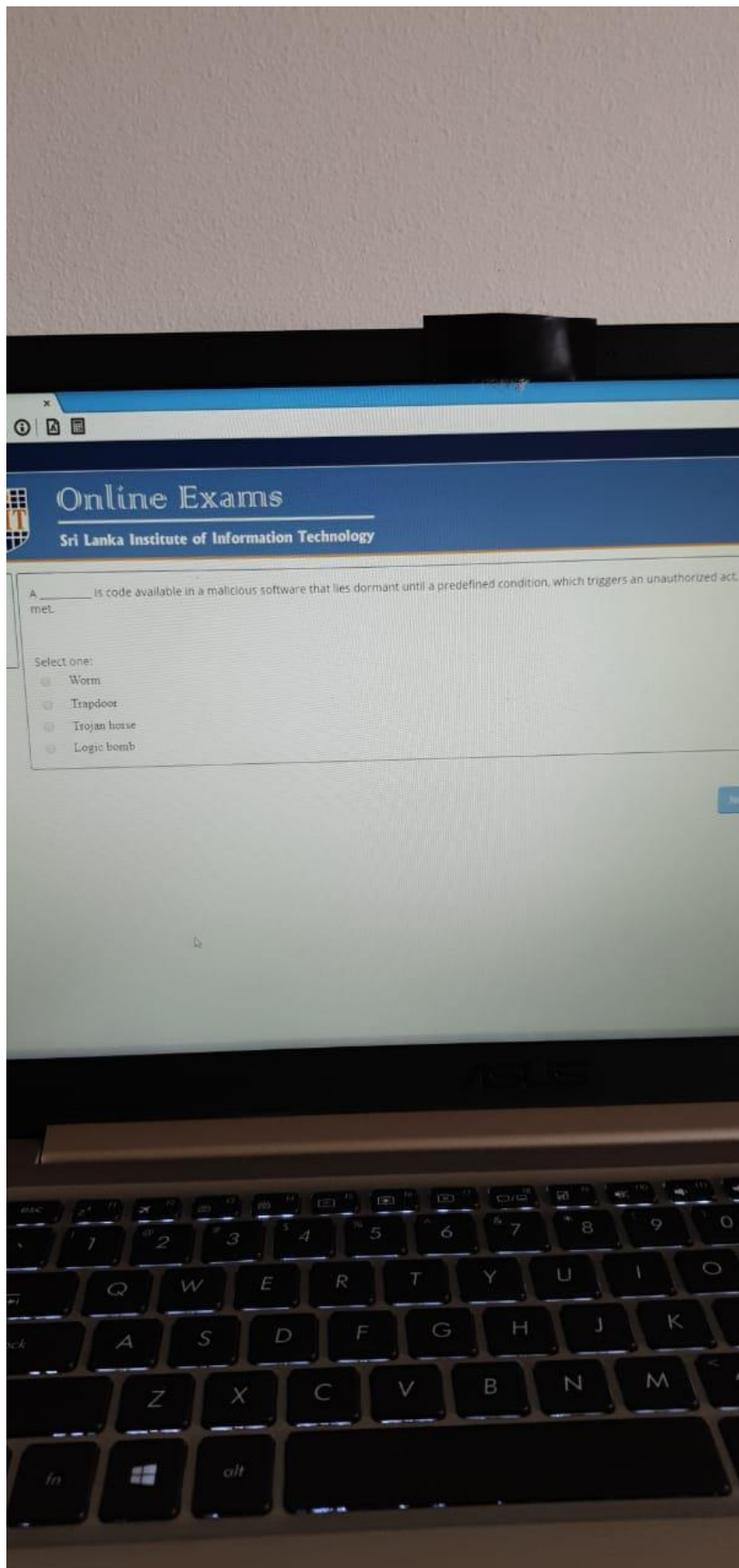
wered
of
estion

_____ protocols are used to counter threats to remote user authentication system

Select one:

- ☐ Challenge-response
- ☐ Communication
- ☐ Denial-of-service
- ☐ File transfer







Online Exams

Sri Lanka Institute of Information Tech

Select Active attacks out of the following.

Select one or more:

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



Two users Alice and Bob use Diffie-Hellman key exchange with a common prime number $p = 23$ and generator $g = 5$ (which is a primitive root module 23). Let 4 and 3 be the private keys of Alice and Bob respectively. What is the common shared secret key? (Write only the numerical value)

Answer:

Next page

Online Exams

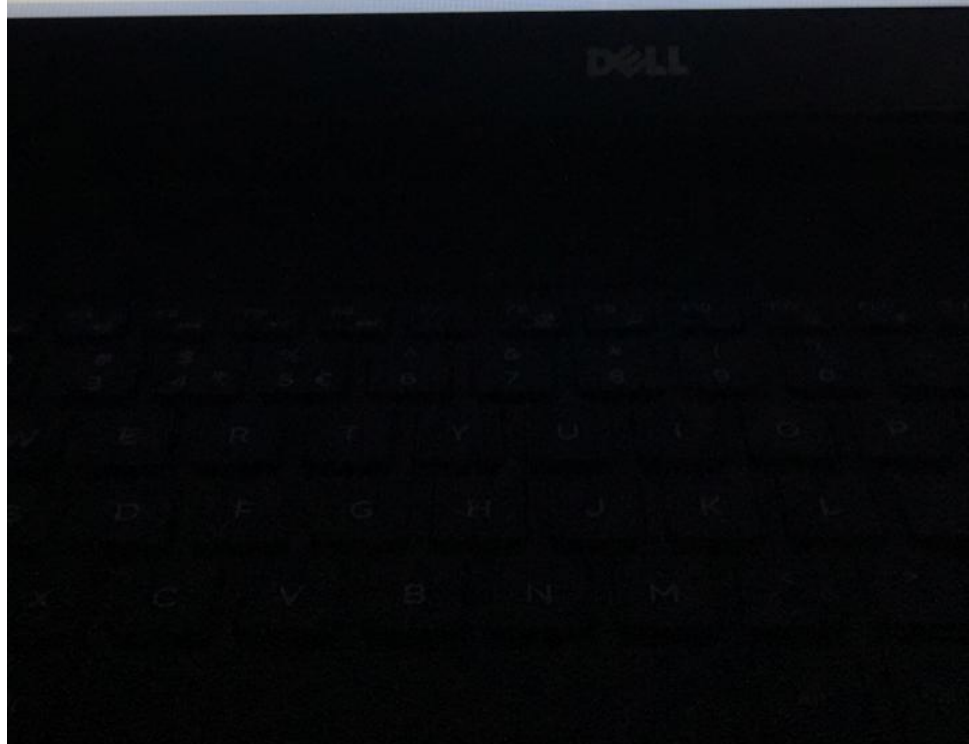
Sri Lanka Institute of Information Technology

A network of a IT-based company consists of 250 workstations used by users and each user makes an average of \$20 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 50% chance of viruses infecting their networks annually after installing this method of Internet connectivity, and that it may take up to 3 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:

Next page





Question 22

Not yet answered

Marked out of
1.00

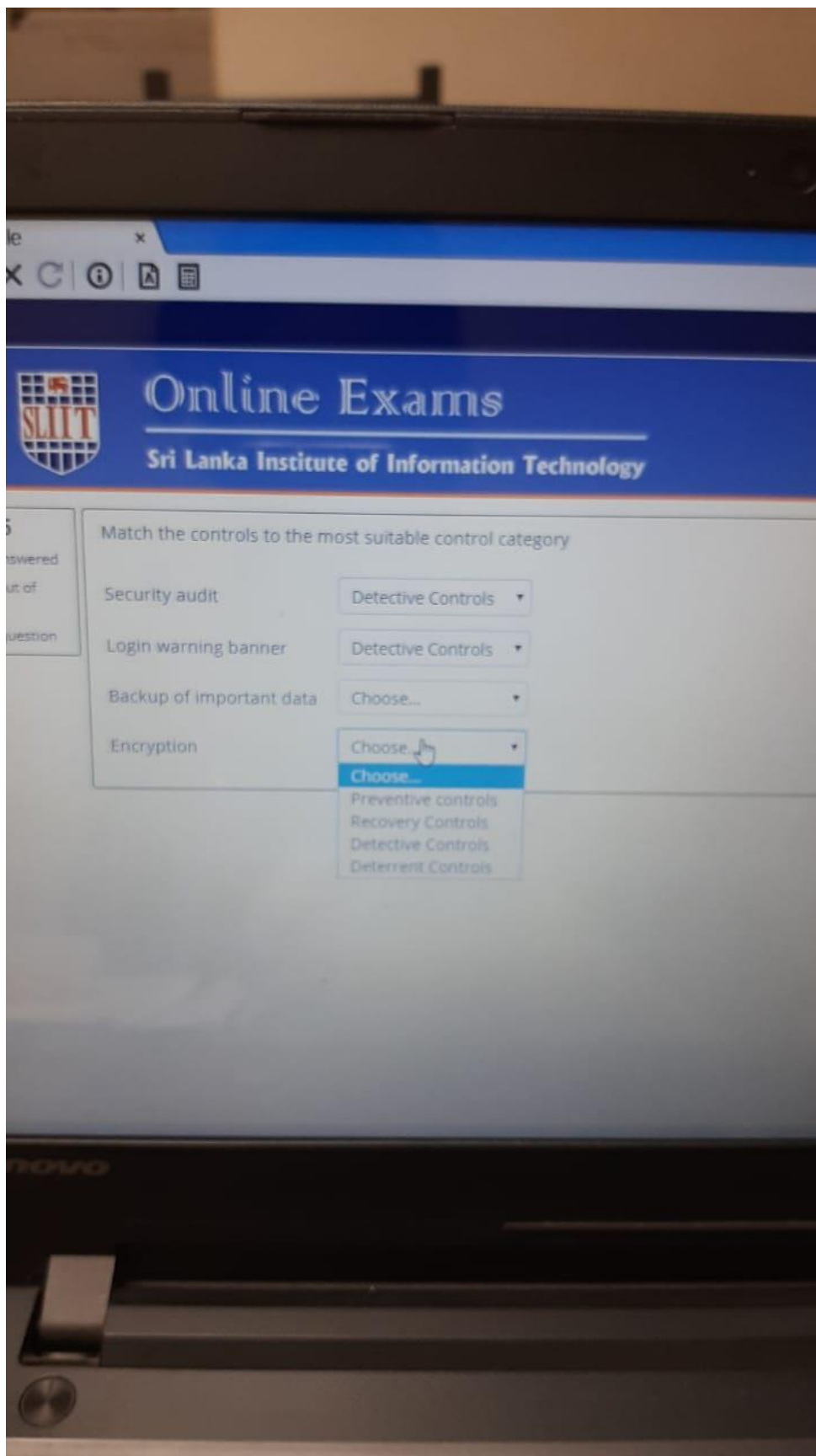
Flag question

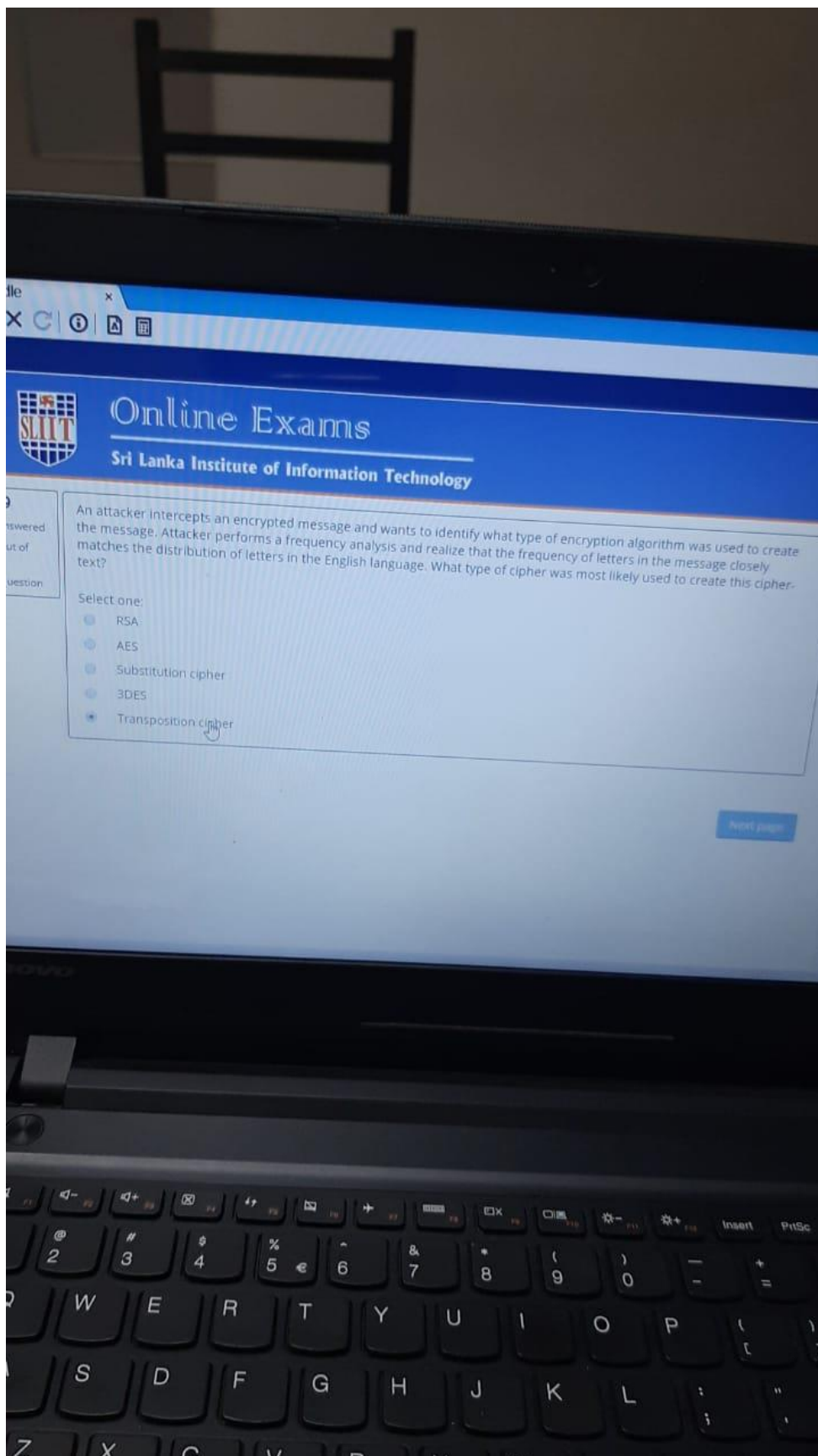
Select the incorrect statement about Role Based Access Control (RBAC) systems.

Select one:

- ☐ One role can be assigned to many users.
- ☐ Users are assigned roles either statically or dynamically
- ☒ Roles can be reused.
- ☐ One user cannot be given access to many roles.
- ☐ Roles are usually defined based on a job function in the organization

Next page







Online Exams

Sri Lanka Institute of Information Technology

Select the incorrect statement with respect to vulnerability assessment.

Select one:

- ☐ Use exploits to penetrate systems
- ☐ Outcome is a list of vulnerabilities and their details
- ☐ Allows to understand threats
- ☐ Is the process of defining, identifying, classifying vulnerabilities in computer systems



Online EXAMS

Sri Lanka Institute of Information Technology

Question 1

Not yet answered

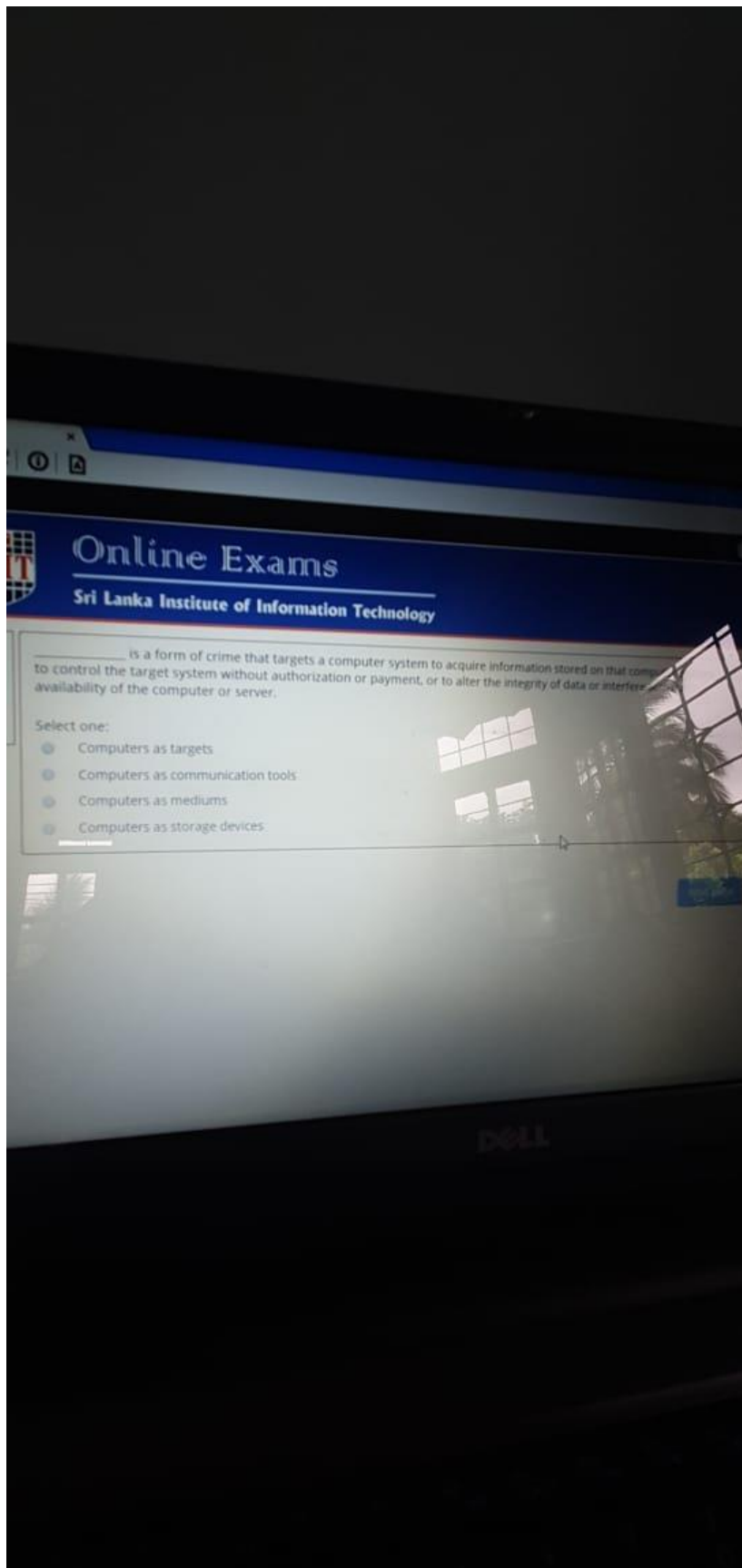
Marked out of


1.00

Flag question

A(n)

algorithm is used to convert cipher-text back to its plain-text.





Online Exams

Sri Lanka Institute of Information Technology

_____ is a form of crime that targets a computer system to acquire information stored on that computer, to control the target system without authorization or payment, or to alter the integrity of data or interfere with the availability of the computer or server.

Select one:

- ☒ Computers as targets
- ☐ Computers as communication tools
- ☐ Computers as mediums
- ☐ Computers as storage devices

DELL



Question 5

Not yet answered

Marked out of 1

Flag question

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

More secure.

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

Use to encrypt short amount of data.

Use to encrypt large amount of data with patterns.

Both parallel encryption and decryption of blocks are possible.

Choose...	▼
Choose...	▼
Choose...	▼
ECB	▼
Choose...	▼
Choose...	▼
Choose...	▼

Question 5

Not yet answered

Marked out of 1.00

Flag question

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

More secure.

CBC

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

CBC

Use to encrypt short amount of data.

ECB

Use to encrypt large amount of data with patterns.

CBC

Both parallel encryption and decryption of blocks are possible.

ECB



Online Exams

Sri Lanka Institute of Information Technology

Question 4
You have answered
1 out of 4
Flag question

Match the description to the relevant access control requirements

Access control systems must use only dependable and accurate details provided by other systems.

Access control system should allow access to be regulated at the level of individual records in files, and individual fields within records.

Authorizations specify which accesses are prohibited; all other accesses are allowed.

Dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.

Controls the functionalities of Administrators dealing with authorization database.

- Choose...

Choose...

Open policies

Reliable inputs

Closed policies

Fine-grained specifications

Administrative policies

Separation of duty

Choose...
- Choose...

Choose...



Select incorrect statements about stream cipher.

Select one or more:

- ☐ Can be much faster than block cipher when used for data transmitted over networks.
- ☒ Size of cipher-text can become larger than plain-text.
- ☐ Encrypt plain-text one byte or one bit at a time.
- ☐ Vigenère cipher is an example of a stream cipher.
- ☐ Transform a fixed-length block of plain-text into a common block of cipher text of 64 or 128 bits.



Online Exams

Sri Lanka Institute of Information Technology

Question 10

Not yet answered

Marked out of 1.00

Flag question

Accumulated Loss Expectancy (ALE) of an organization due to virus attacks to computers is 50000 dollars. Assume that organization can get licensed copies of anti-virus software for all servers and the workstations at a cost of 21000 dollars per year to completely prevent this problem.

What is the benefit organization get by purchasing the antivirus solution? (Hint: perform a cost/benefit analysis to calculate the benefit). (Type the numerical value only)

Answer:

Next page



Question 16

Not yet answered

Marked out of 1

Flag question

Select Active attacks out of the following.

Select one or more:

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



Question 16

Not yet answered

Marked out of 1

Flag question

Select Active attacks out of the following.

Select one or more:

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



Select incorrect statements about stream cipher.

Select one or more:

- ☐ Can be much faster than block cipher when used for data transmitted over networks.
- ☒ Size of cipher-text can become larger than plain-text.
- ☐ Encrypt plain-text one byte or one bit at a time.
- ☐ Vigenère cipher is an example of a stream cipher.
- ☐ Transform a fixed-length block of plain-text into a common block of cipher text of 64 or 128 bits.



Question 19

Not yet answered

Marked out of 1.25

Flag question

An authentication process include the step and verification step.





Question 27

Has yet answered

Marked out of

1.00

Flag question

_____ Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

Select one:

☐ RBAC

☐ DAC

☒ MAC

☐ NAC

Next page



Online Exams

Sri Lanka Institute of Information Technology

Question 18

Not yet answered

Marked out of

1.00

Flag question

Two users Alice and Bob use Diffie-Hellman key exchange with a common prime number $p = 13$ and generator $g = 6$ (which is a primitive root modulo 13). Let 3 and 10 be the private keys of Alice and Bob respectively. What is the common shared secret key? (Write only the numerical value)

Answer:

Next page



Online Exams

Sri Lanka Institute of Information Technology

40

answered
out of
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:

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

Next Question



Online Exams

Sri Lanka Institute of Information Technology

Question 44

Not yet answered

Marked out of 1

Flag question

Match the description to the most relevant malicious software type/ category.

Design to provide continuous privileged access to computer systems

Any mechanism that bypass regular security measures when accessing systems

Advertising that is integrated in to software

Propagate usually by exploiting vulnerabilities

Malware code consist of portable instructions and works in different platforms

Macro virus ▼

Spyware ▼

Adware ▼

Worm ▼

Trapdoor ▼



Online Exams

Sri Lanka Institute of Information Technology

40

answered
out of
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:

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

Next Question

Question 60

Not yet answered

Marked out of 1.00

Flag question

Select the incorrect statement about access control systems.

Select one:

- ☐ Use to prevent legitimate users from accessing unauthorized resources
- ☐ Subjects, objects and access rights are the basic elements of access control systems
- ☐ Implemented based on access control policies such as DAC, MAC and RBAC
- ☐ Access control systems do not depend on inputs coming from other systems such as authentication systems