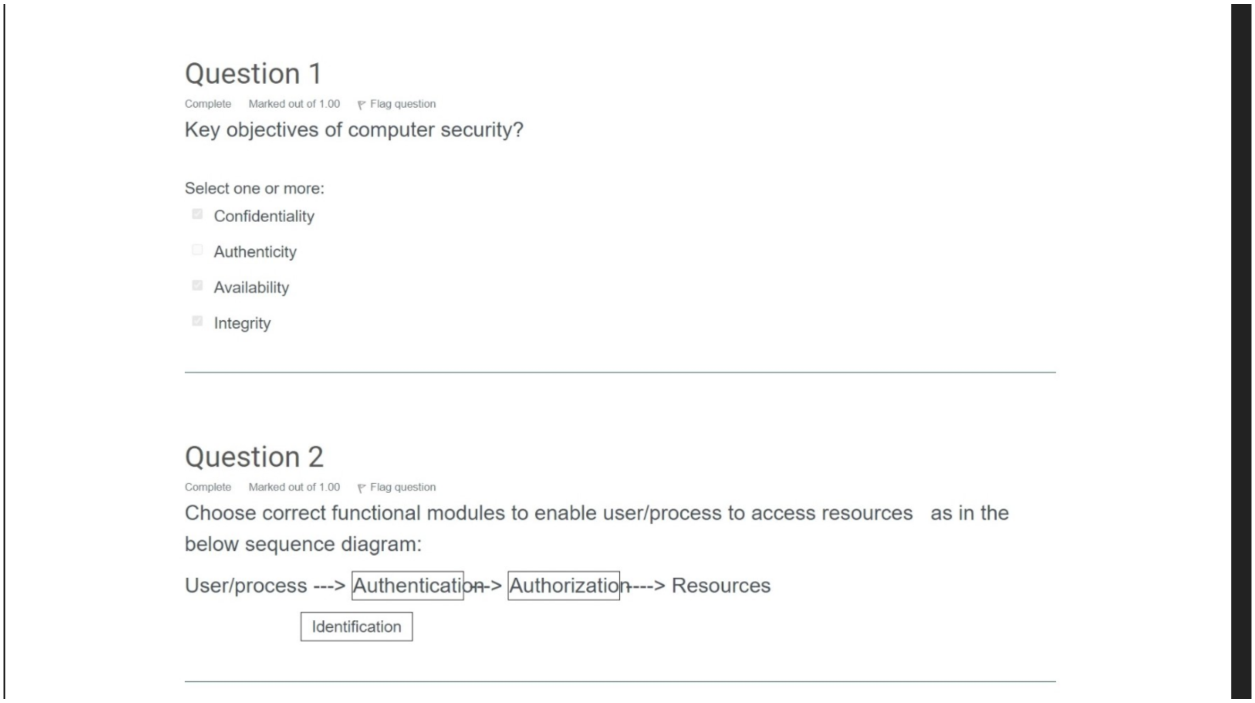


Question 1

Complete   Marked out of 1.00   Flag question

Key objectives of computer security?

Select one or more:

☑ Confidentiality

□ Authenticity

☑ Availability

☑ Integrity

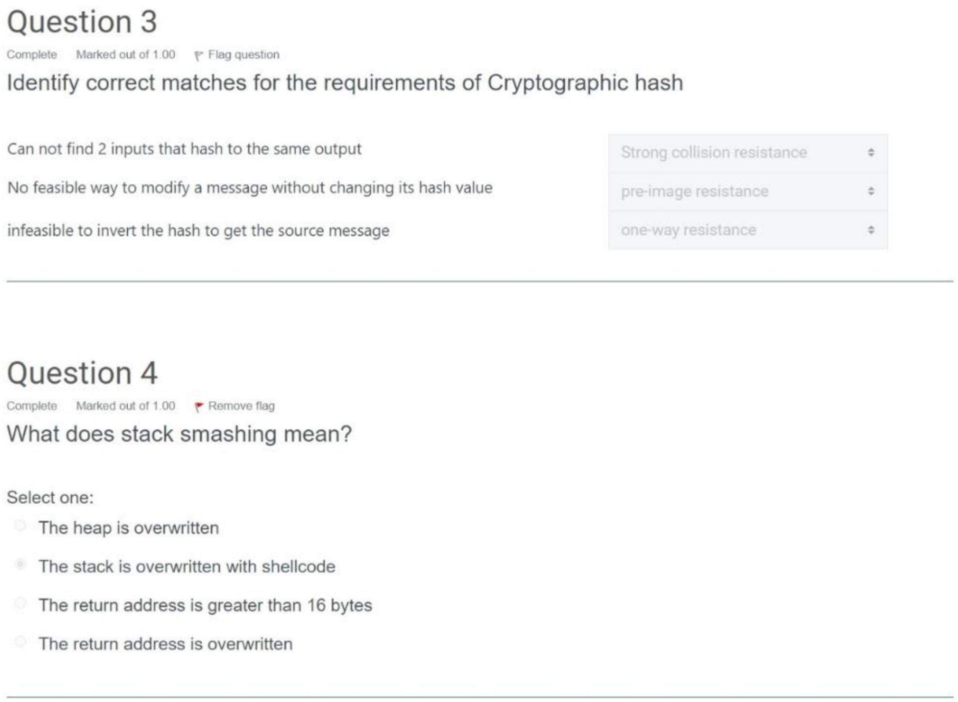
Question 2

Complete   Marked out of 1.00   Flag question

Choose correct functional modules to enable user/process to access resources   as in the below sequence diagram:

User/process ---> Authentication--> Authorization---> Resources

Identification



Question 3

Complete   Marked out of 1.00   Flag question

Identify correct matches for the requirements of Cryptographic hash

Can not find 2 inputs that hash to the same output	Strong collision resistance
No feasible way to modify a message without changing its hash value	pre-image resistance
infeasible to invert the hash to get the source message	one-way resistance

Question 4

Complete   Marked out of 1.00   Remove flag

What does stack smashing mean?

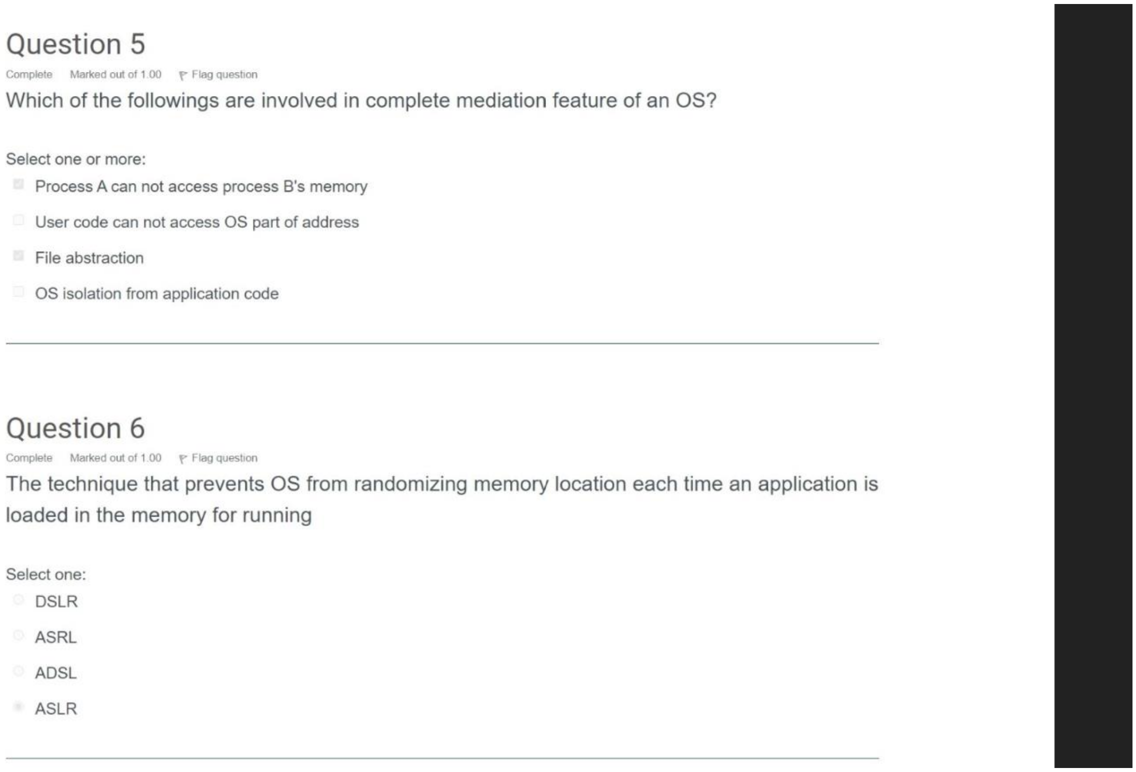
Select one:

○ The heap is overwritten

● The stack is overwritten with shellcode

○ The return address is greater than 16 bytes

○ The return address is overwritten



Question 5

Complete Marked out of 1.00 Flag question

Which of the followings are involved in complete mediation feature of an OS?

Select one or more:

☑ Process A can not access process B's memory

□ User code can not access OS part of address

☑ File abstraction

□ OS isolation from application code

Question 6

Complete Marked out of 1.00 Flag question

The technique that prevents OS from randomizing memory location each time an application is loaded in the memory for running

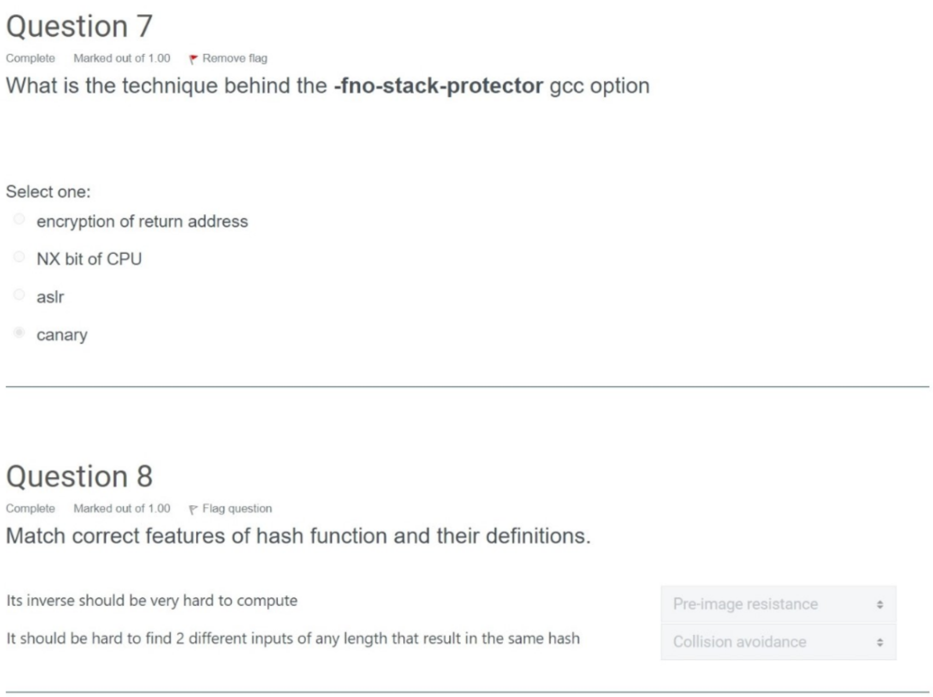
Select one:

○ DSLR

○ ASRL

○ ADSL

● ASLR



Question 7

Complete Marked out of 1.00 Remove flag

What is the technique behind the **-fno-stack-protector** gcc option

Select one:

○ encryption of return address

○ NX bit of CPU

○ aslr

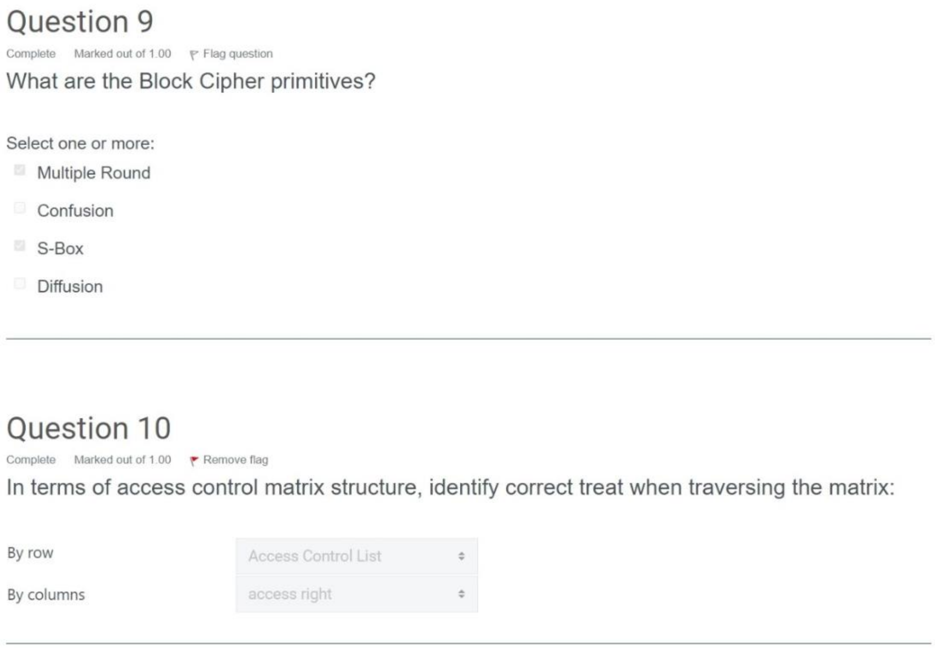
● canary

Question 8

Complete Marked out of 1.00 Flag question

Match correct features of hash function and their definitions.

Its inverse should be very hard to compute	Pre-image resistance
It should be hard to find 2 different inputs of any length that result in the same hash	Collision avoidance



Question 9

Complete Marked out of 1.00 Flag question

What are the Block Cipher primitives?

Select one or more:

☑ Multiple Round

□ Confusion

☑ S-Box

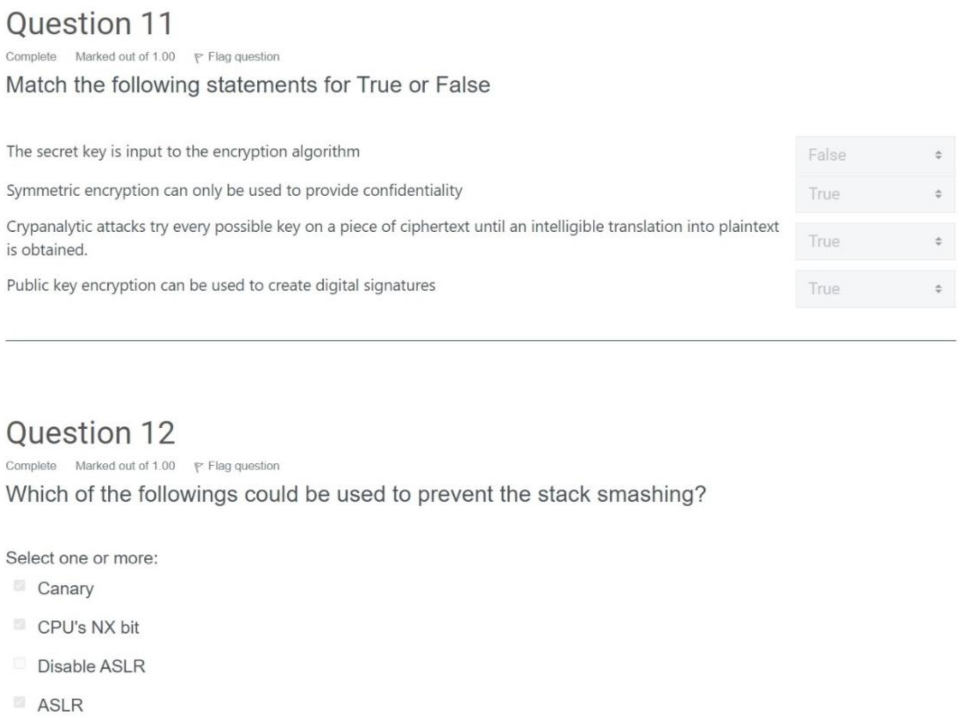
□ Diffusion

Question 10

Complete Marked out of 1.00 Remove flag

In terms of access control matrix structure, identify correct treat when traversing the matrix:

By row	Access Control List
By columns	access right



Question 11

Complete Marked out of 1.00 Flag question

Match the following statements for True or False

The secret key is input to the encryption algorithm	False
Symmetric encryption can only be used to provide confidentiality	True
Crypanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.	True
Public key encryption can be used to create digital signatures	True

Question 12

Complete Marked out of 1.00 Flag question

Which of the followings could be used to prevent the stack smashing?

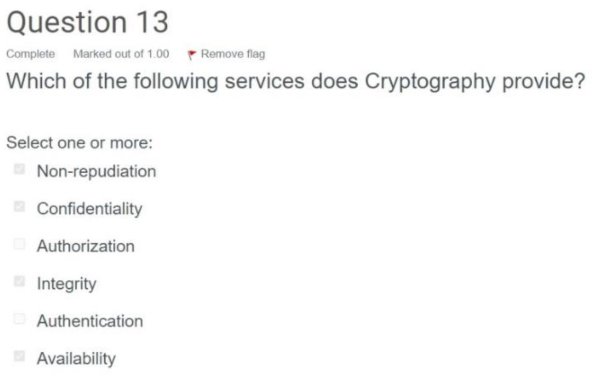
Select one or more:

☑ Canary

☑ CPU's NX bit

□ Disable ASLR

☑ ASLR



Question 13

Complete Marked out of 1.00 Remove flag

Which of the following services does Cryptography provide?

Select one or more:

☑ Non-repudiation

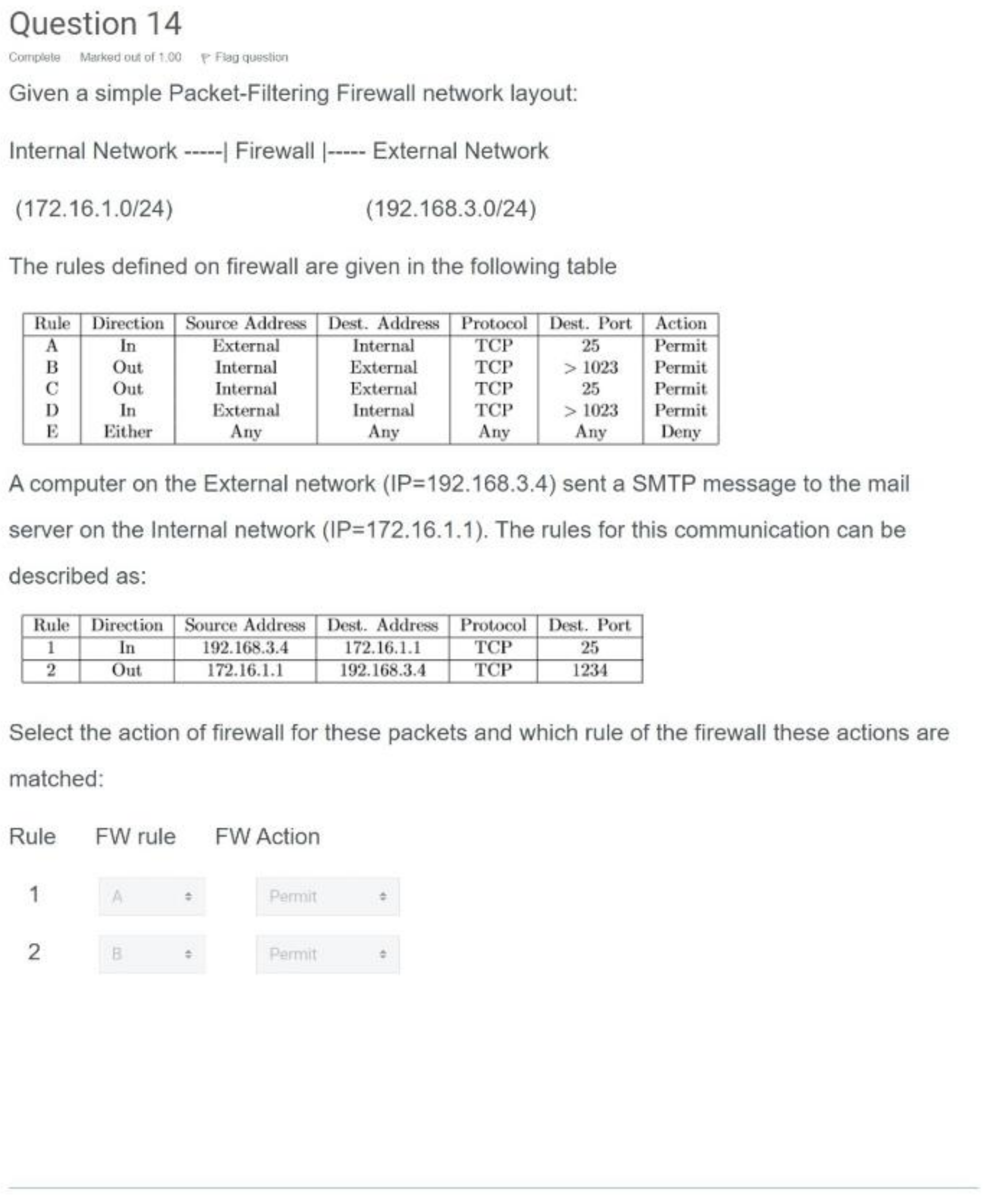
☑ Confidentiality

□ Authorization

☑ Integrity

□ Authentication

☑ Availability



Question 14

Complete Marked out of 1.00 Flag question

Given a simple Packet-Filtering Firewall network layout:

Internal Network -----| Firewall |----- External Network

(172.16.1.0/24) (192.168.3.0/24)

The rules defined on firewall are given in the following table

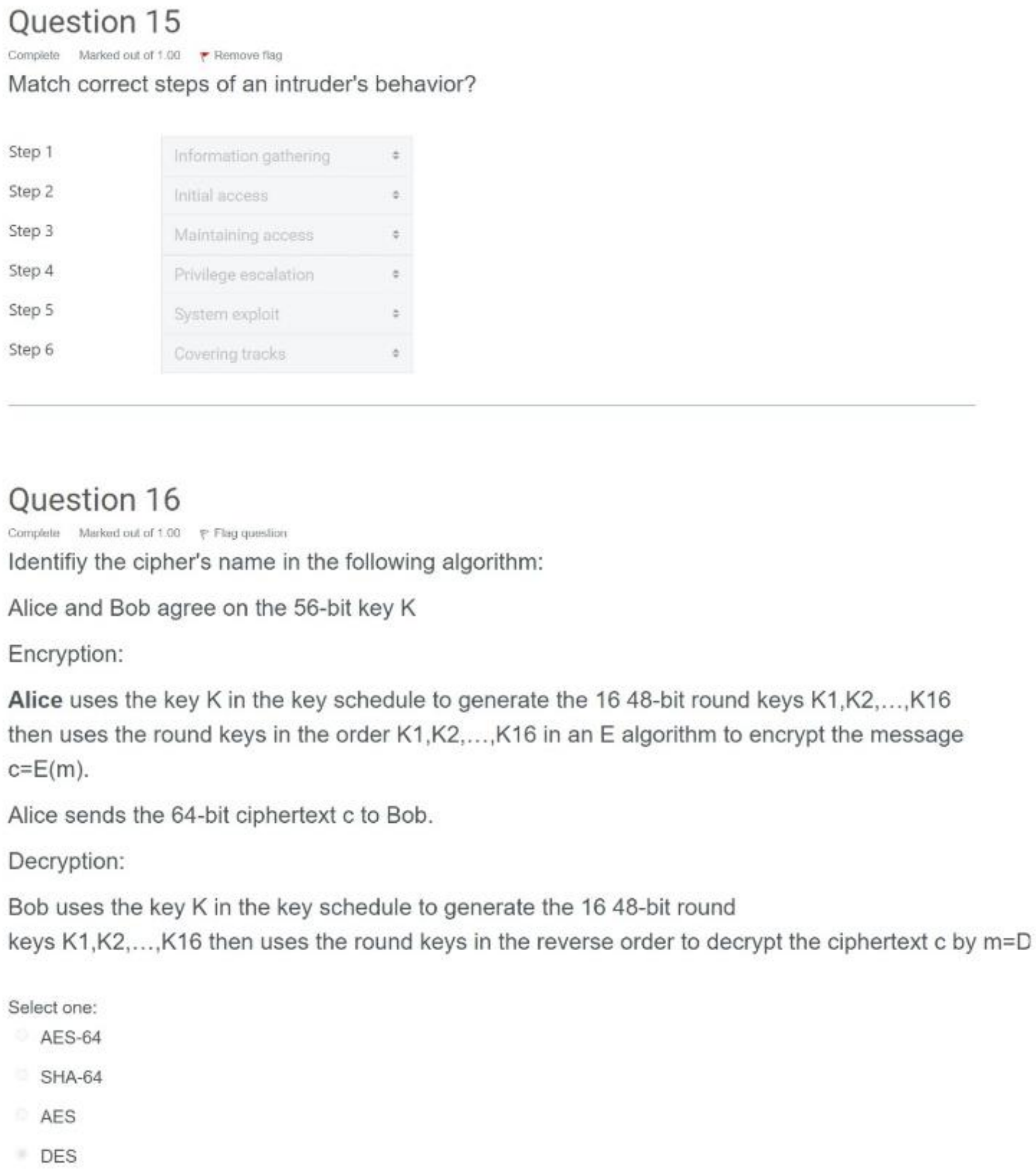
Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

A computer on the External network (IP=192.168.3.4) sent a SMTP message to the mail server on the Internal network (IP=172.16.1.1). The rules for this communication can be described as:

Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port
1	In	192.168.3.4	172.16.1.1	TCP	25
2	Out	172.16.1.1	192.168.3.4	TCP	1234

Select the action of firewall for these packets and which rule of the firewall these actions are matched:

Rule	FW rule	FW Action
1	A	Permit
2	B	Permit



Question 15

Complete Marked out of 1.00 Remove flag

Match correct steps of an intruder's behavior?

Step 1	Information gathering
Step 2	Initial access
Step 3	Maintaining access
Step 4	Privilege escalation
Step 5	System exploit
Step 6	Covering tracks

Question 16

Complete Marked out of 1.00 Flag question

Identifiy the cipher's name in the following algorithm:

Alice and Bob agree on the 56-bit key K

Encryption:

Alice uses the key K in the key schedule to generate the 16 48-bit round keys K1,K2,…,K16 then uses the round keys in the order K1,K2,…,K16 in an E algorithm to encrypt the message c=E(m).

Alice sends the 64-bit ciphertext c to Bob.

Decryption:

Bob uses the key K in the key schedule to generate the 16 48-bit round keys K1,K2,…,K16 then uses the round keys in the reverse order to decrypt the ciphertext c by m=D

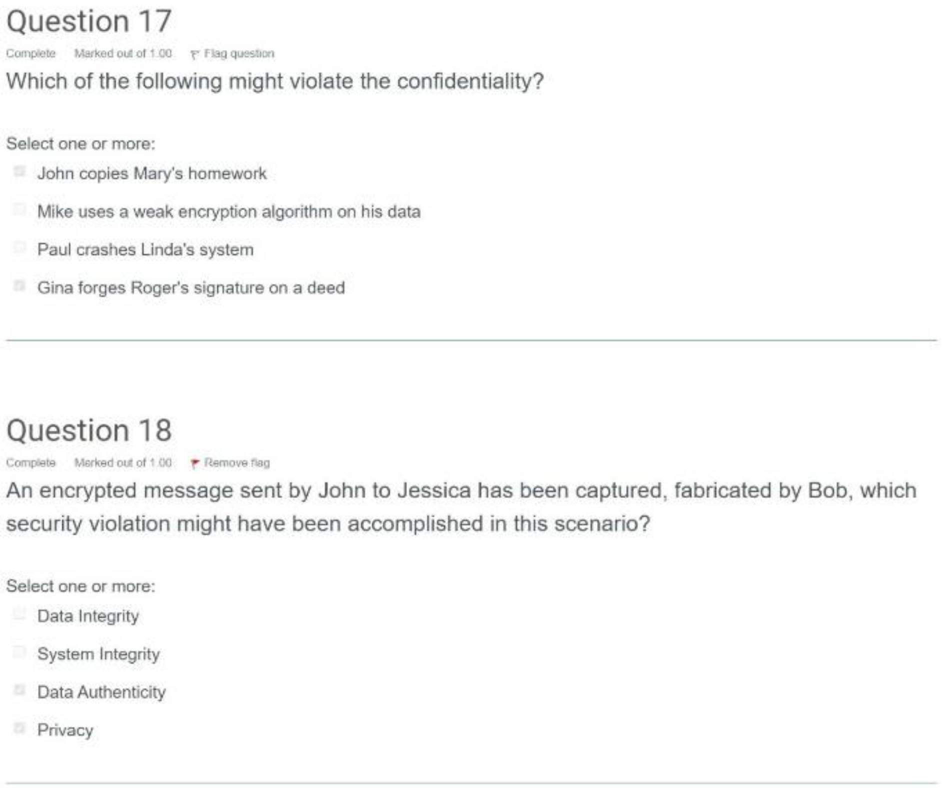
Select one:

○ AES-64

○ SHA-64

○ AES

● DES



Question 17

Complete Marked out of 1.00 Flag question

Which of the following might violate the confidentiality?

Select one or more:

☑ John copies Mary's homework

□ Mike uses a weak encryption algorithm on his data

□ Paul crashes Linda's system

☑ Gina forges Roger's signature on a deed

Question 18

Complete Marked out of 1.00 Remove flag

An encrypted message sent by John to Jessica has been captured, fabricated by Bob, which security violation might have been accomplished in this scenario?

Select one or more:

□ Data Integrity

□ System Integrity

☑ Data Authenticity

☑ Privacy

Question 19

Complete Marked out of 1.00 Flag question

A user-defined network protocol is implemented:

Firstly, the data is encrypted with an encryption algorithm, then the checksum field for the encrypted data is generated.

Which security features are involved in this protocol?

Select one or more:

☑ Confidentiality

☑ Integrity

□ Accountability

□ availablity

Question 20

Complete Marked out of 1.00 Flag question

Which of the following might violate the integrity?

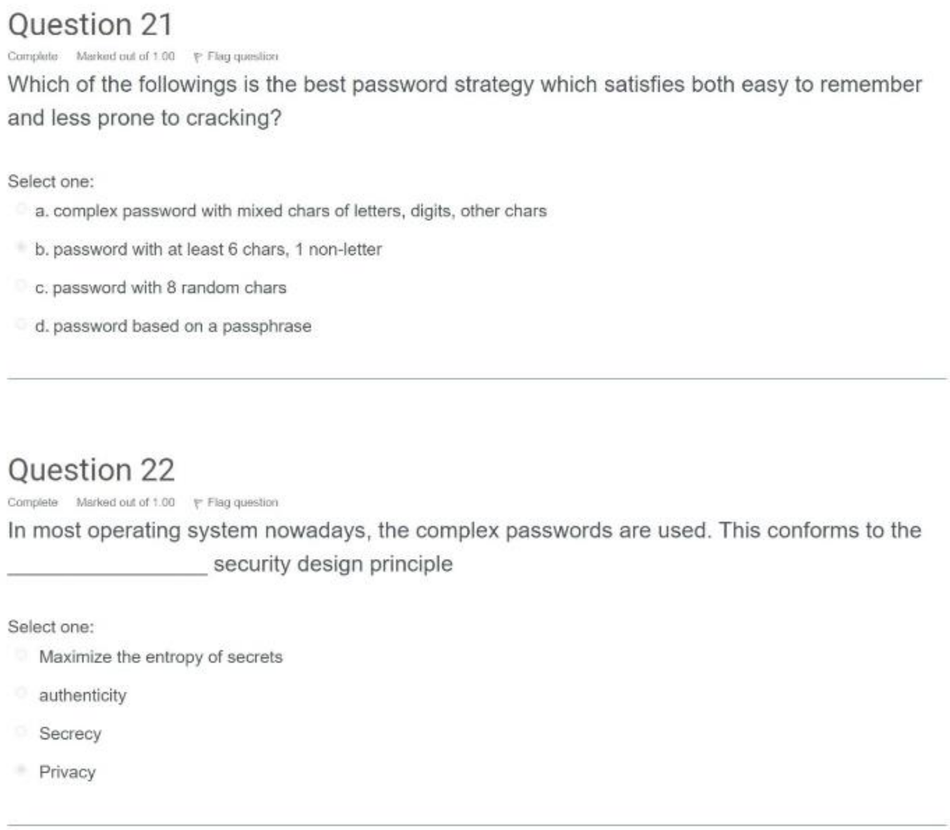
Select one or more:

□ John copies Mary's homework

□ Paul crashes Linda's system

☑ The total transferred amount of the check has been modified from $100 to $1000.

□ Some vulnerabilities have been found during the pentest (penetration test) but the system has not been fixed yet.



Question 21

Which of the followings is the best password strategy which satisfies both easy to remember and less prone to cracking?

Select one:

○ a. complex password with mixed chars of letters, digits, other chars

● b. password with at least 6 chars, 1 non-letter

○ c. password with 8 random chars

○ d. password based on a passphrase

Question 22

In most operating system nowadays, the complex passwords are used. This conforms to the ________________ security design principle

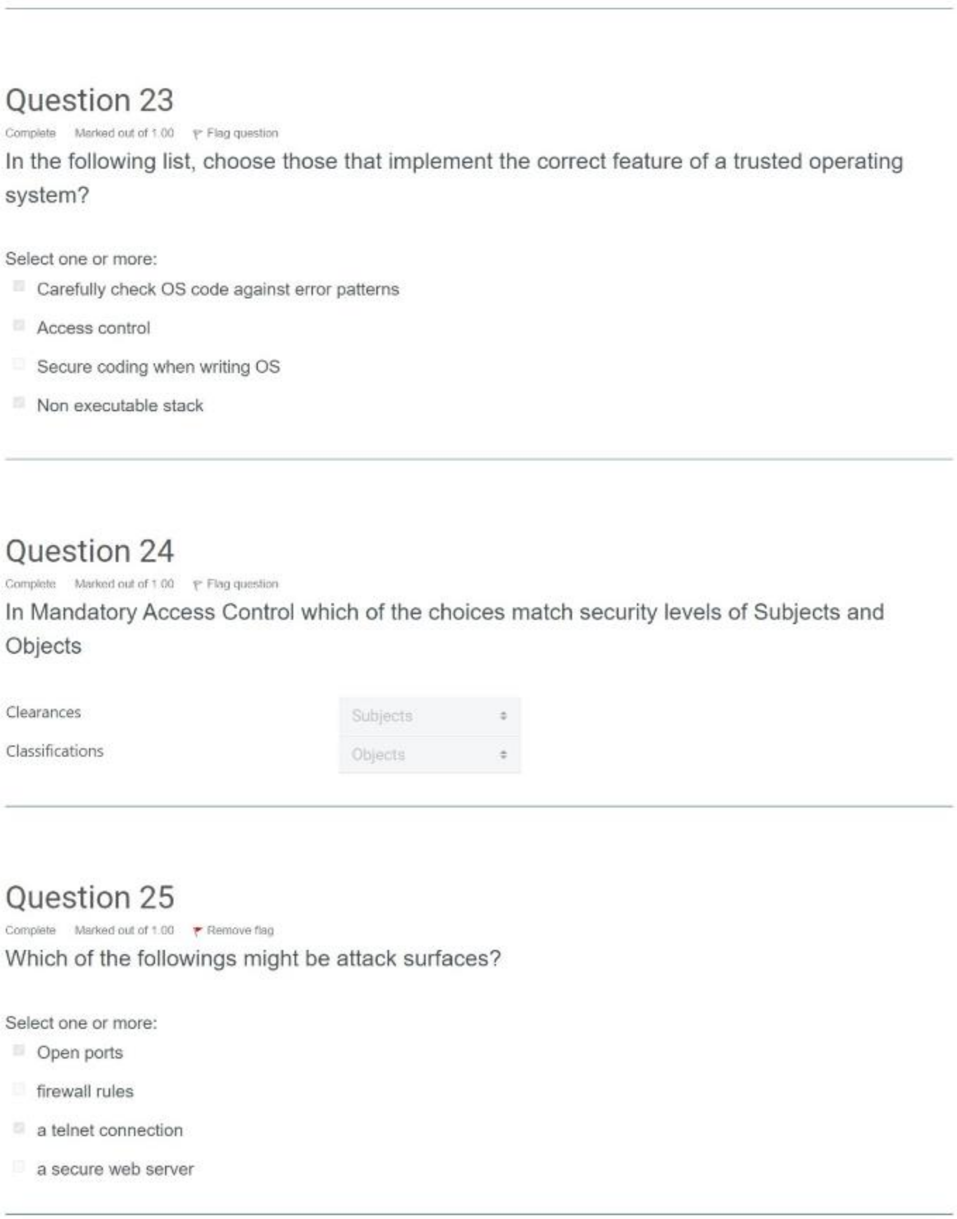
Select one:

○ Maximize the entropy of secrets

○ authenticity

○ Secrecy

● Privacy



Question 23

Complete Marked out of 1.00 Flag question

In the following list, choose those that implement the correct feature of a trusted operating system?

Select one or more:

- ☑ Carefully check OS code against error patterns
- ☑ Access control
- □ Secure coding when writing OS
- ☑ Non executable stack

Question 24

Complete Marked out of 1.00 Flag question

In Mandatory Access Control which of the choices match security levels of Subjects and Objects

Clearances	Subjects ⇕
Classifications	Objects ⇕

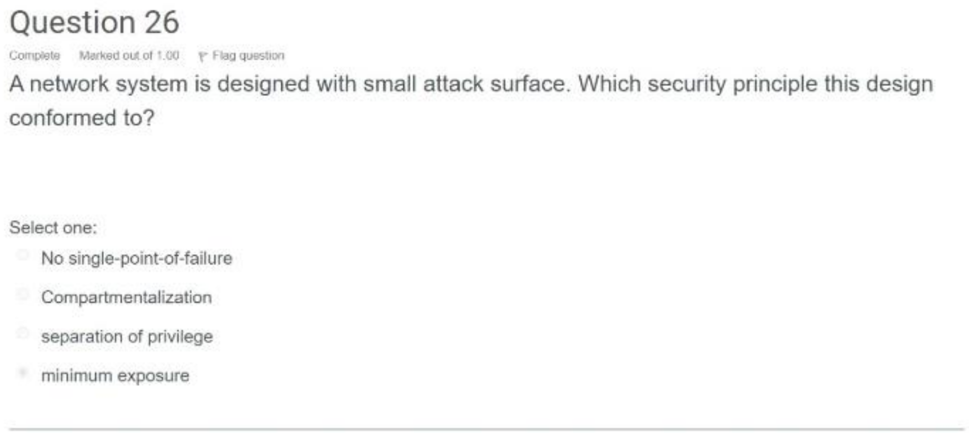
Question 25

Complete Marked out of 1.00 Remove flag

Which of the followings might be attack surfaces?

Select one or more:

- ☑ Open ports
- □ firewall rules
- ☑ a telnet connection
- □ a secure web server



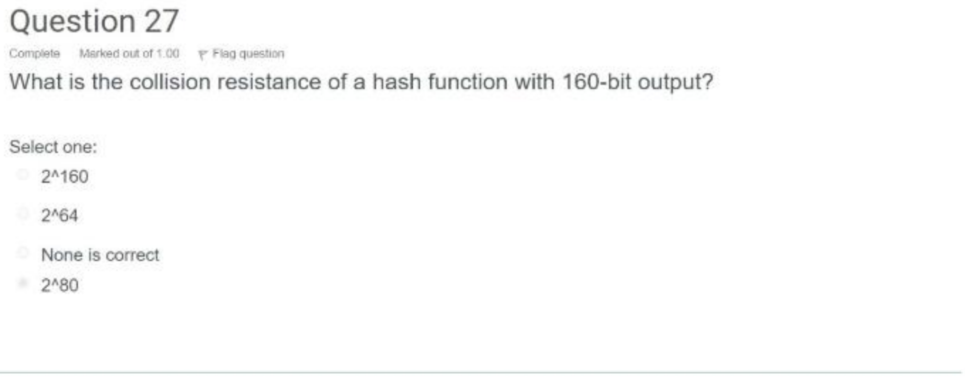
Question 26

Complete Marked out of 1.00 Flag question

A network system is designed with small attack surface. Which security principle this design conformed to?

Select one:

- ○ No single-point-of-failure
- ○ Compartmentalization
- ○ separation of privilege
- ● minimum exposure



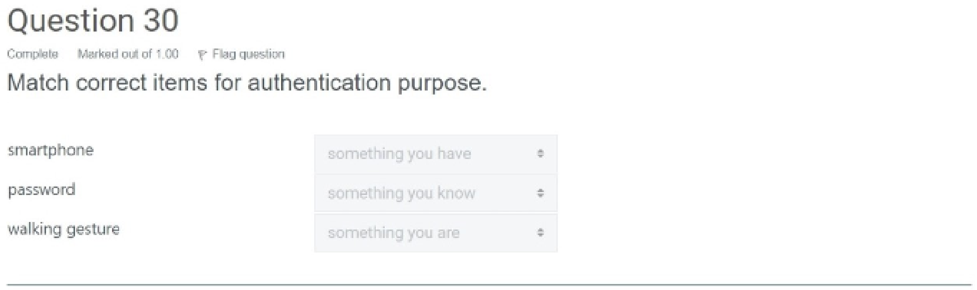
Question 27

Complete Marked out of 1.00 Flag question

What is the collision resistance of a hash function with 160-bit output?

Select one:

- ○ 2^160
- ○ 2^64
- ○ None is correct
- ● 2^80

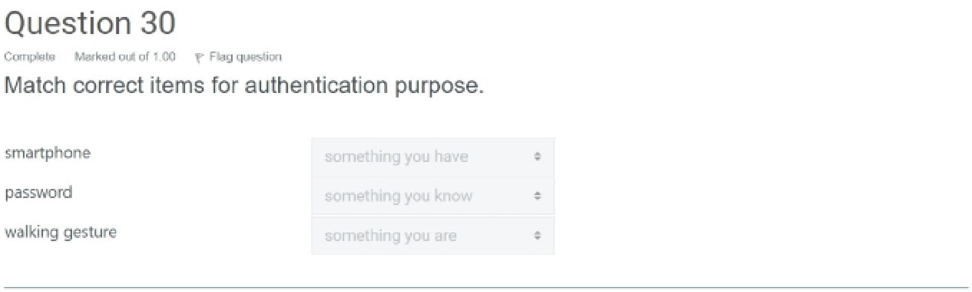


Question 30

Complete Marked out of 1.00 Flag question

Match correct items for authentication purpose.

smartphone	something you have
password	something you know
walking gesture	something you are

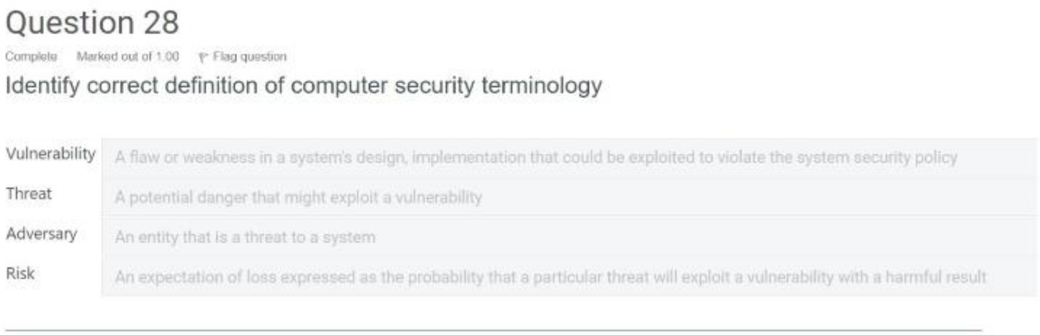


Question 30

Complete Marked out of 1.00 Flag question

Match correct items for authentication purpose.

smartphone	something you have
password	something you know
walking gesture	something you are

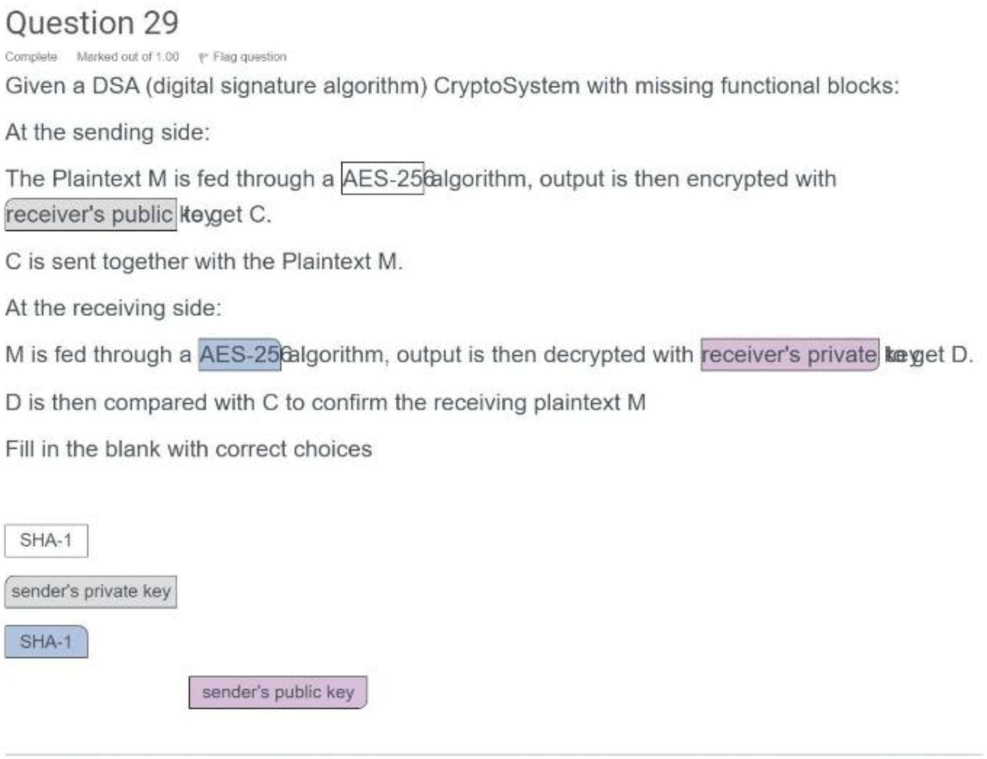


Question 28

Complete Marked out of 1.00 Flag question

Identify correct definition of computer security terminology

Vulnerability	A flaw or weakness in a system's design, implementation that could be exploited to violate the system security policy
Threat	A potential danger that might exploit a vulnerability
Adversary	An entity that is a threat to a system
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a vulnerability with a harmful result



Question 29

Complete Marked out of 1.00 Flag question

Given a DSA (digital signature algorithm) CryptoSystem with missing functional blocks:

At the sending side:

The Plaintext M is fed through a AES-256 algorithm, output is then encrypted with receiver's public key to get C.

C is sent together with the Plaintext M.

At the receiving side:

M is fed through a AES-256 algorithm, output is then decrypted with receiver's private key to get D.

D is then compared with C to confirm the receiving plaintext M

Fill in the blank with correct choices

SHA-1

sender's private key

SHA-1

sender's public key

Question 30

Complete Marked out of 1.00 Flag question

Match correct items for authentication purpose.

smartphone	something you have
password	something you know
walking gesture	something you are

Question 31

Complete Marked out of 1.00 Remove flag

Given a simple Packet-Filtering Firewall network layout:

Internal Network -----| Firewall |----- External Network

(172.16.1.0/24) (192.168.3.0/24)

The rules defined on firewall are given in the following table

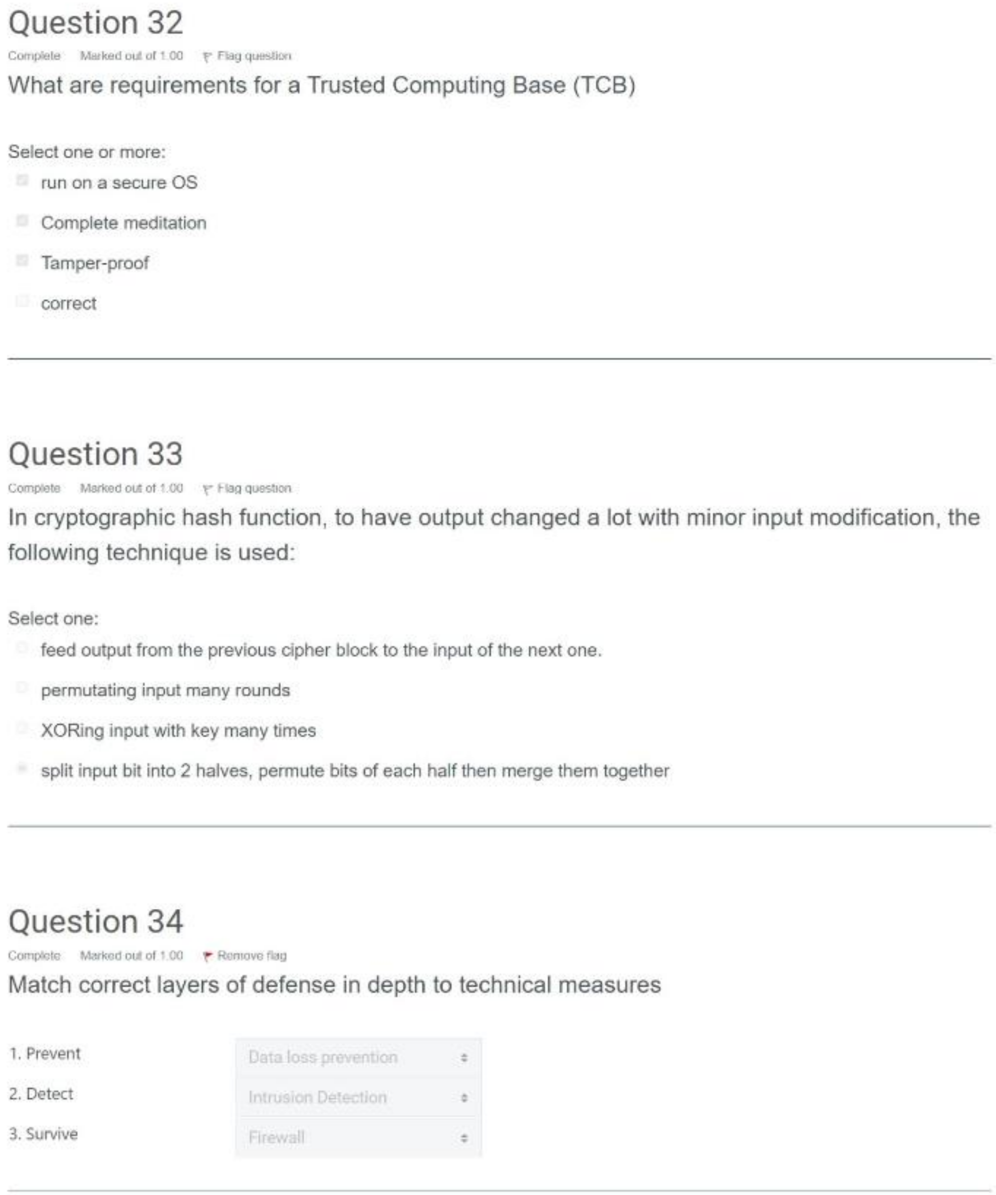
Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

An client (IP=192.168.3.4) opens a connection from port 5150 on his end to the proxy web server on port 8080 of the machine on the Internal network (IP=172.16.1.1). The rules for this communication can be described as:

Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port
5	In	192.168.3.4	172.16.1.1	TCP	8080
6	Out	172.16.1.1	192.168.3.4	TCP	5150

Select the actions of firewall for these packets and which rule of the firewall these actions are matched:

Rule	FW rule	FW Action
5	D	Permit
6	B	Permit



Question 32

Complete Marked out of 1.00 Flag question

What are requirements for a Trusted Computing Base (TCB)

Select one or more:

☑ run on a secure OS

☑ Complete meditation

☑ Tamper-proof

□ correct

Question 33

Complete Marked out of 1.00 Flag question

In cryptographic hash function, to have output changed a lot with minor input modification, the following technique is used:

Select one:

○ feed output from the previous cipher block to the input of the next one.

○ permutating input many rounds

○ XORing input with key many times

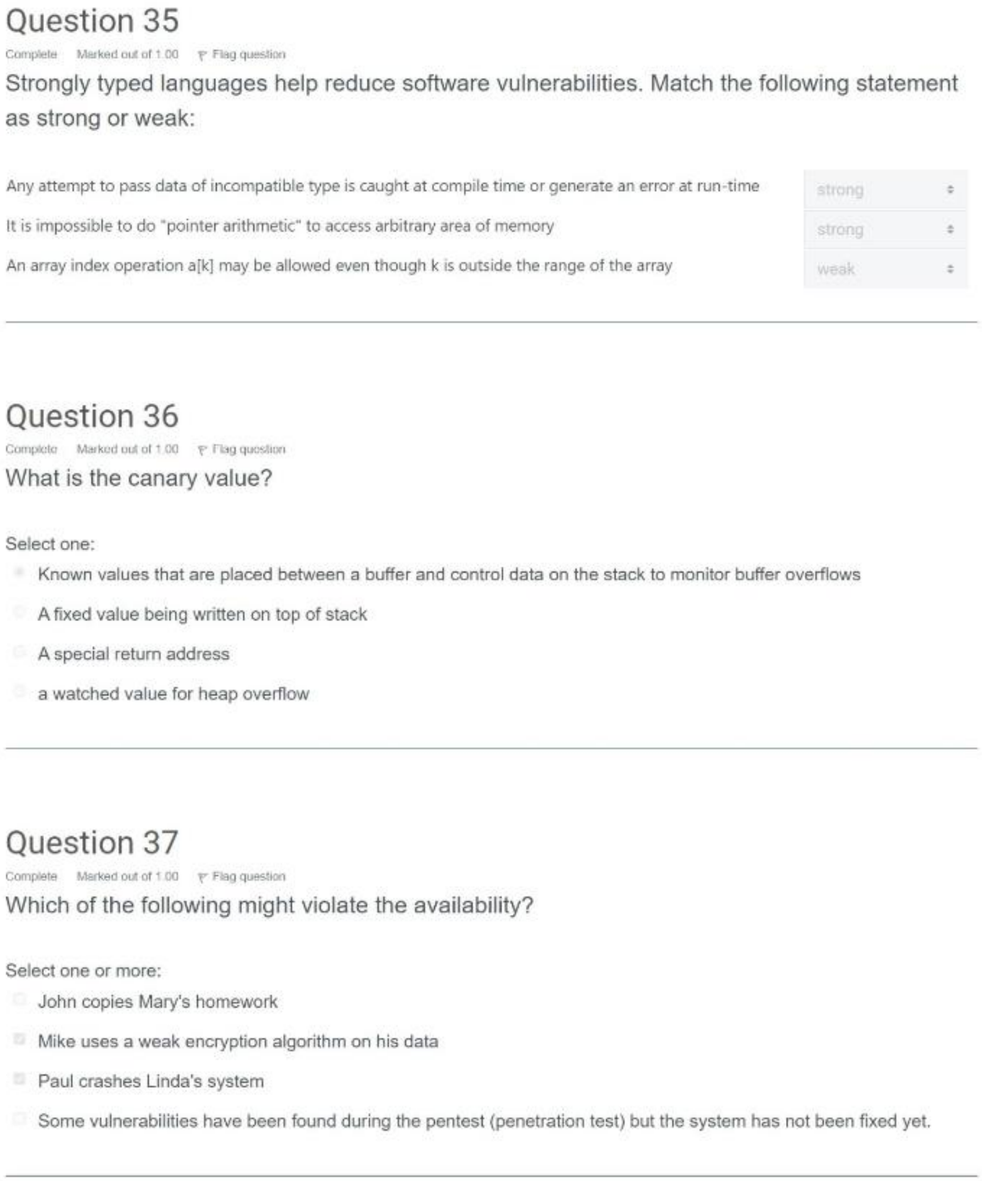
● split input bit into 2 halves, permute bits of each half then merge them together

Question 34

Complete Marked out of 1.00 Remove flag

Match correct layers of defense in depth to technical measures

1. Prevent	Data loss prevention ⬍
2. Detect	Intrusion Detection ⬍
3. Survive	Firewall ⬍



Question 35

Complete Marked out of 1.00 Flag question

Strongly typed languages help reduce software vulnerabilities. Match the following statement as strong or weak:

Any attempt to pass data of incompatible type is caught at compile time or generate an error at run-time	strong ⇕
It is impossible to do "pointer arithmetic" to access arbitrary area of memory	strong ⇕
An array index operation a[k] may be allowed even though k is outside the range of the array	weak ⇕

Question 36

Complete Marked out of 1.00 Flag question

What is the canary value?

Select one:

- ● Known values that are placed between a buffer and control data on the stack to monitor buffer overflows
- ○ A fixed value being written on top of stack
- ○ A special return address
- ○ a watched value for heap overflow

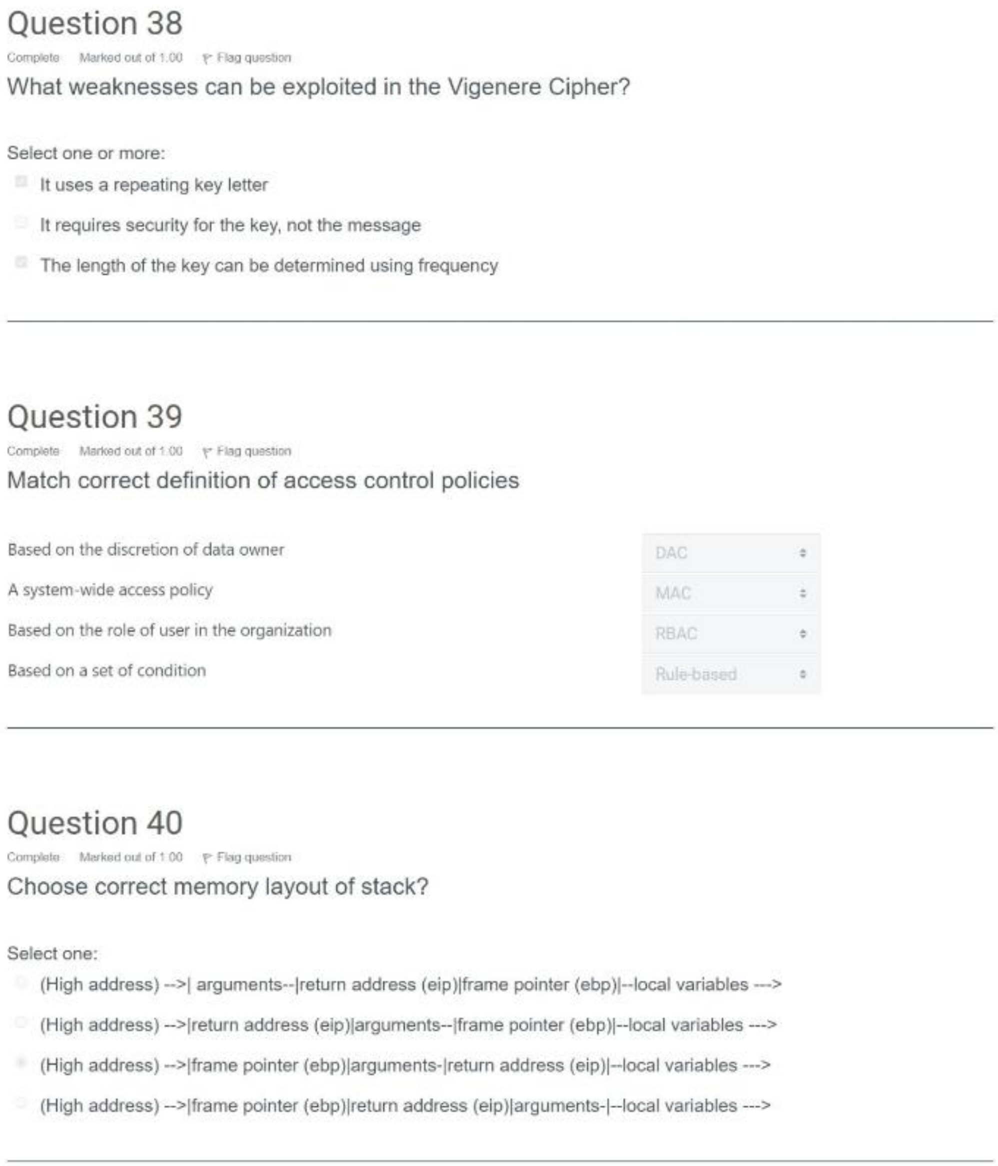
Question 37

Complete Marked out of 1.00 Flag question

Which of the following might violate the availability?

Select one or more:

- ☐ John copies Mary's homework
- ☑ Mike uses a weak encryption algorithm on his data
- ☑ Paul crashes Linda's system
- ☐ Some vulnerabilities have been found during the pentest (penetration test) but the system has not been fixed yet.



Question 38

Complete Marked out of 1.00 Flag question

What weaknesses can be exploited in the Vigenere Cipher?

Select one or more:

- ☑ It uses a repeating key letter
- ☐ It requires security for the key, not the message
- ☑ The length of the key can be determined using frequency

Question 39

Complete Marked out of 1.00 Flag question

Match correct definition of access control policies

Based on the discretion of data owner	DAC ⇕
A system-wide access policy	MAC ⇕
Based on the role of user in the organization	RBAC ⇕
Based on a set of condition	Rule-based ⇕

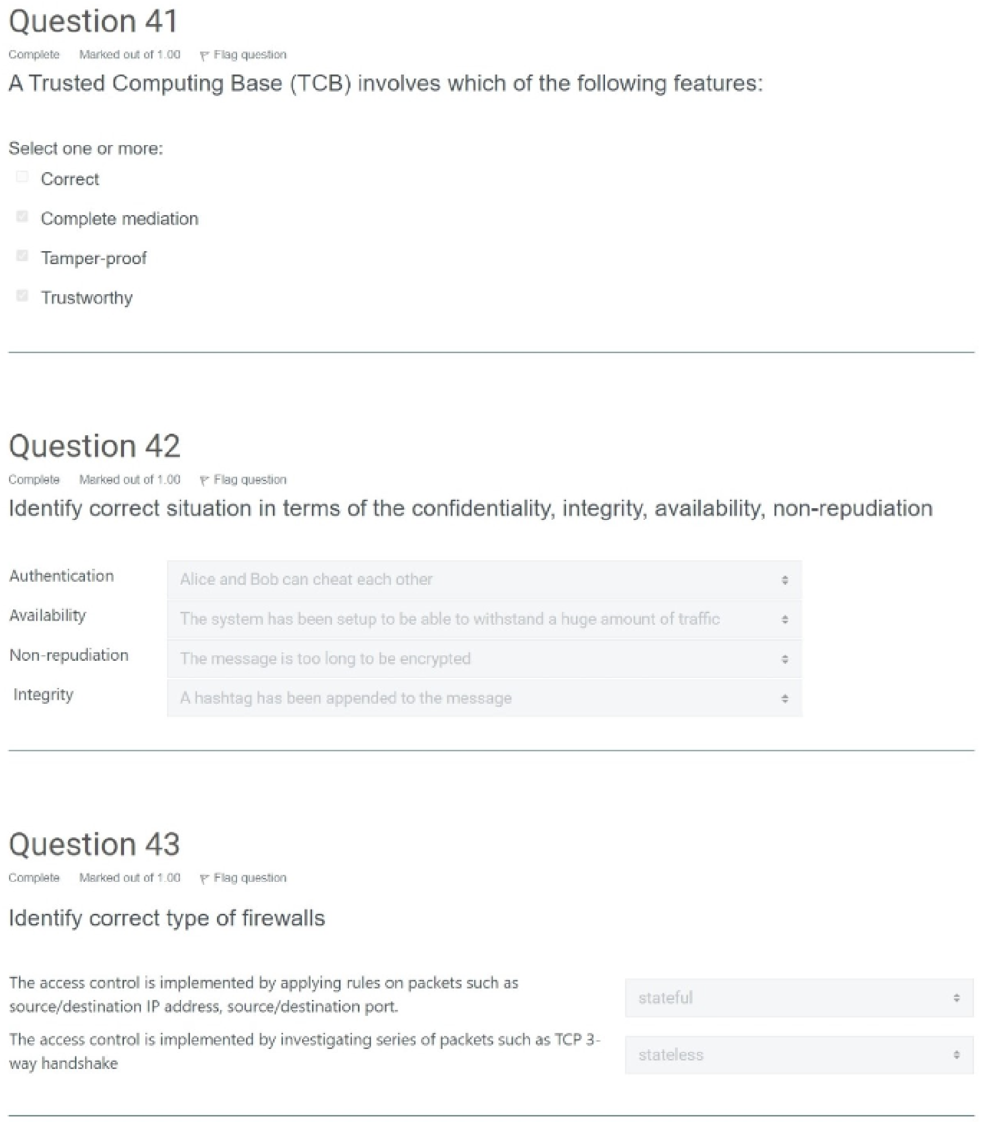
Question 40

Complete Marked out of 1.00 Flag question

Choose correct memory layout of stack?

Select one:

- ○ (High address) -->| arguments--|return address (eip)|frame pointer (ebp)|--local variables --->
- ○ (High address) -->|return address (eip)|arguments--|frame pointer (ebp)|--local variables --->
- ● (High address) -->|frame pointer (ebp)|arguments-|return address (eip)|--local variables --->
- ○ (High address) -->|frame pointer (ebp)|return address (eip)|arguments-|--local variables --->



Question 41

Complete Marked out of 1.00 ⚐ Flag question

A Trusted Computing Base (TCB) involves which of the following features:

Select one or more:

- □ Correct
- ☑ Complete mediation
- ☑ Tamper-proof
- ☑ Trustworthy

Question 42

Complete Marked out of 1.00 ⚐ Flag question

Identify correct situation in terms of the confidentiality, integrity, availability, non-repudiation

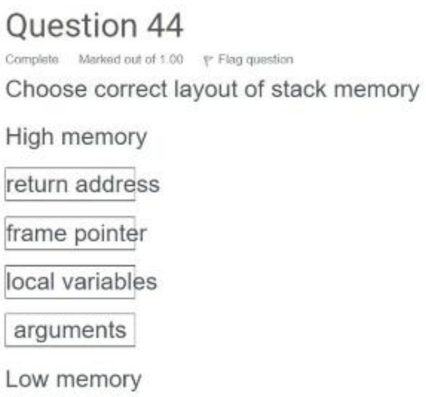
Authentication	Alice and Bob can cheat each other
Availability	The system has been setup to be able to withstand a huge amount of traffic
Non-repudiation	The message is too long to be encrypted
Integrity	A hashtag has been appended to the message

Question 43

Complete Marked out of 1.00 ⚐ Flag question

Identify correct type of firewalls

The access control is implemented by applying rules on packets such as source/destination IP address, source/destination port.	stateful
The access control is implemented by investigating series of packets such as TCP 3-way handshake	stateless



Question 44

Complete Marked out of 1.00 Flag question

Choose correct layout of stack memory

High memory

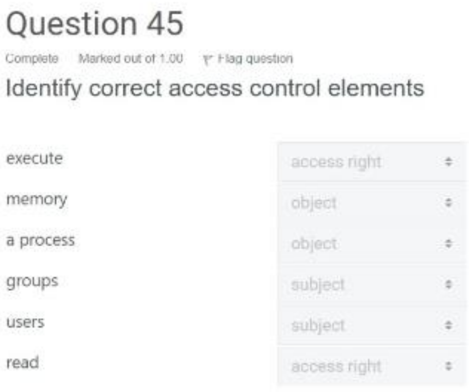
return address

frame pointer

local variables

arguments

Low memory

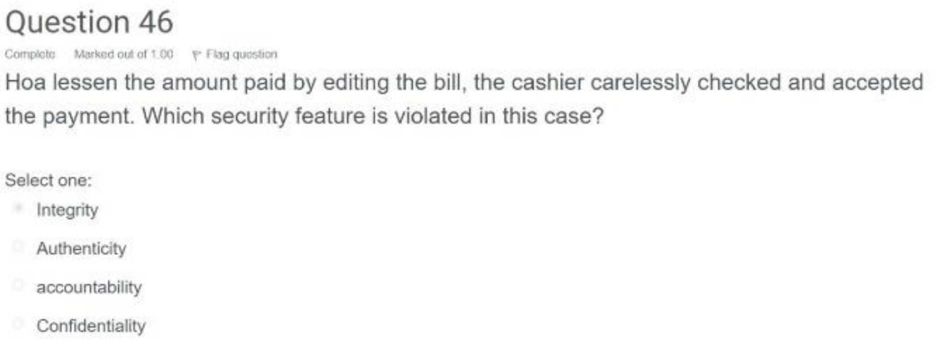


Question 45

Complete Marked out of 1.00 Flag question

Identify correct access control elements

execute	access right ⇕
memory	object ⇕
a process	object ⇕
groups	subject ⇕
users	subject ⇕
read	access right ⇕



Question 46

Complete Marked out of 1.00 Flag question

Hoa lessen the amount paid by editing the bill, the cashier carelessly checked and accepted the payment. Which security feature is violated in this case?

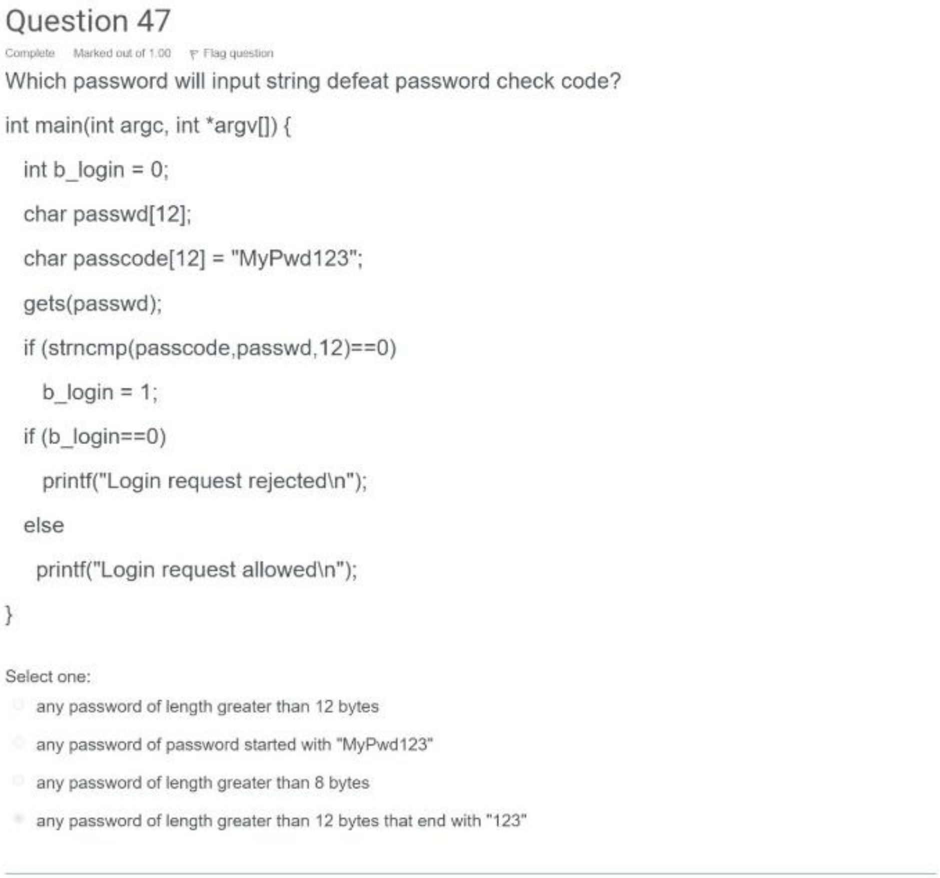
Select one:

● Integrity

○ Authenticity

○ accountability

○ Confidentiality



Question 47

Which password will input string defeat password check code?

```
int main(int argc, int *argv[]) {
  int b_login = 0;
  char passwd[12];
  char passcode[12] = "MyPwd123";
  gets(passwd);
  if (strncmp(passcode,passwd,12)==0)
    b_login = 1;
  if (b_login==0)
    printf("Login request rejected\n");
  else
   printf("Login request allowed\n");
}
```

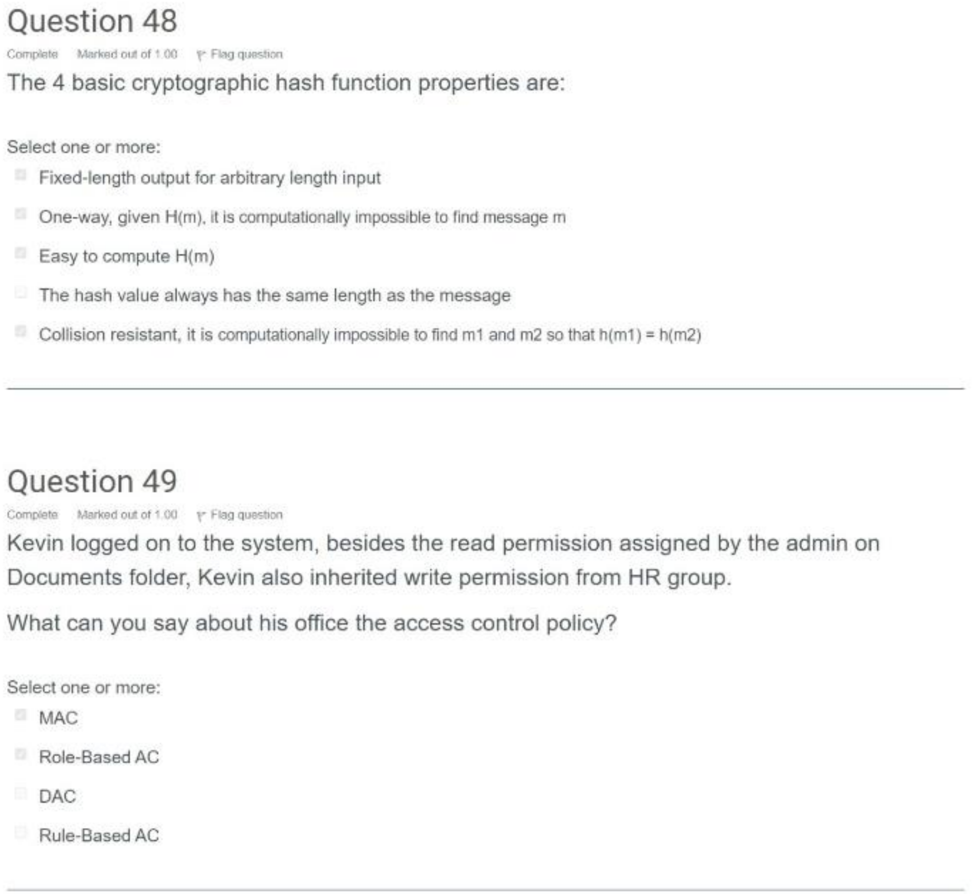
Select one:

○ any password of length greater than 12 bytes

○ any password of password started with "MyPwd123"

○ any password of length greater than 8 bytes

● any password of length greater than 12 bytes that end with "123"



Question 48

Complete Marked out of 1.00 Flag question

The 4 basic cryptographic hash function properties are:

Select one or more:

☑ Fixed-length output for arbitrary length input

☑ One-way, given H(m), it is computationally impossible to find message m

☑ Easy to compute H(m)

□ The hash value always has the same length as the message

☑ Collision resistant, it is computationally impossible to find m1 and m2 so that h(m1) = h(m2)

Question 49

Complete Marked out of 1.00 Flag question

Kevin logged on to the system, besides the read permission assigned by the admin on Documents folder, Kevin also inherited write permission from HR group.

What can you say about his office the access control policy?

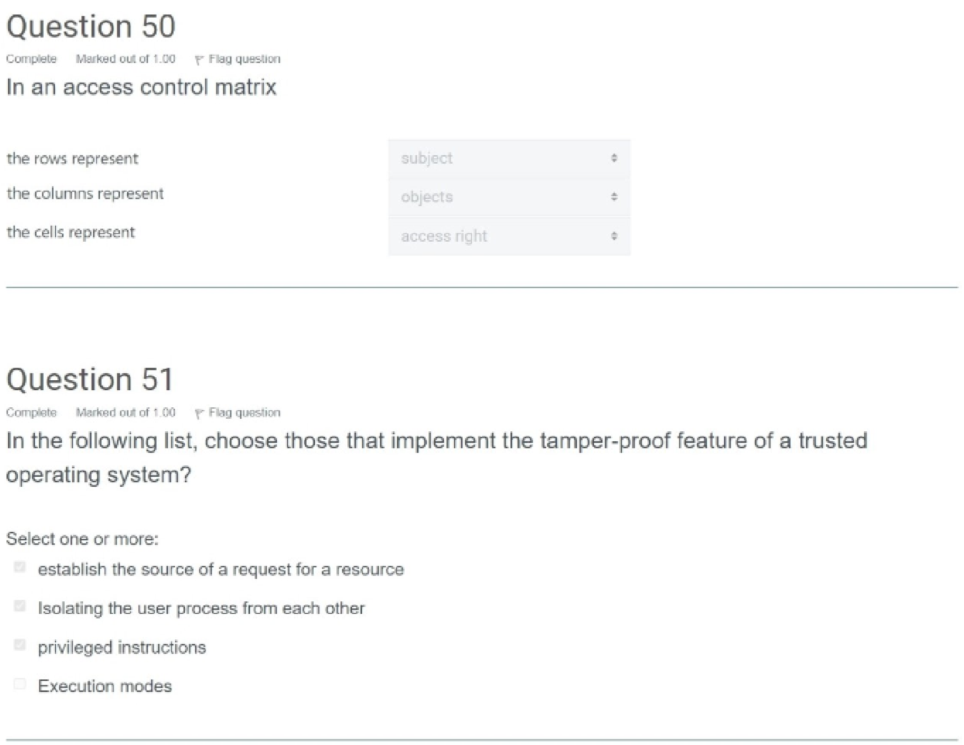
Select one or more:

☑ MAC

☑ Role-Based AC

□ DAC

□ Rule-Based AC



Question 50

Complete Marked out of 1.00 Flag question

In an access control matrix

the rows represent	subject ⬍
the columns represent	objects ⬍
the cells represent	access right ⬍

Question 51

Complete Marked out of 1.00 Flag question

In the following list, choose those that implement the tamper-proof feature of a trusted operating system?

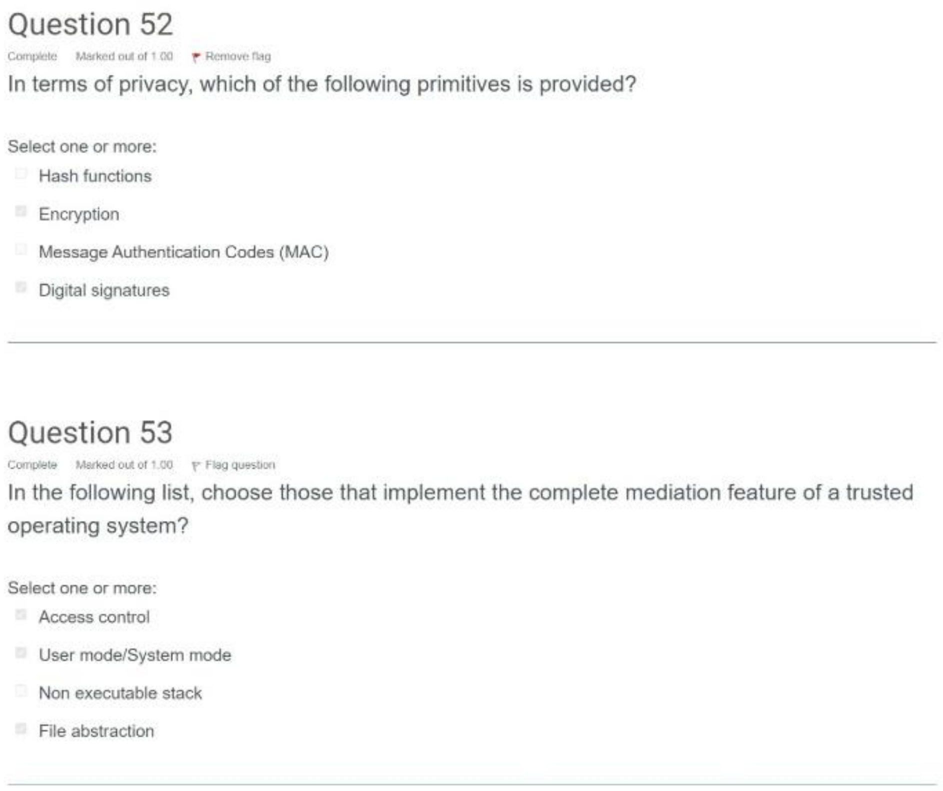
Select one or more:

☑ establish the source of a request for a resource

☑ Isolating the user process from each other

☑ privileged instructions

□ Execution modes



Question 52

Complete Marked out of 1.00 Remove flag

In terms of privacy, which of the following primitives is provided?

Select one or more:

□ Hash functions

☑ Encryption

□ Message Authentication Codes (MAC)

☑ Digital signatures

Question 53

Complete Marked out of 1.00 Flag question

In the following list, choose those that implement the complete mediation feature of a trusted operating system?

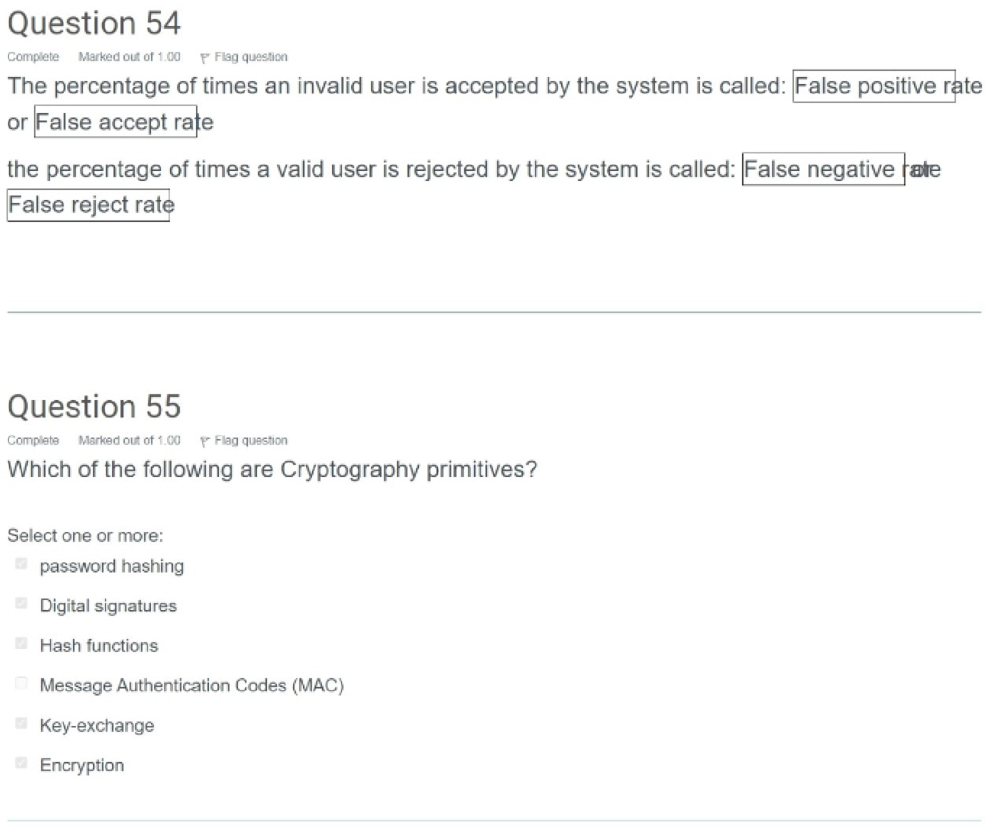
Select one or more:

☑ Access control

☑ User mode/System mode

□ Non executable stack

☑ File abstraction



Question 54

Complete Marked out of 1.00 Flag question

The percentage of times an invalid user is accepted by the system is called: False positive rate or False accept rate

the percentage of times a valid user is rejected by the system is called: False negative rate or False reject rate

Question 55

Complete Marked out of 1.00 Flag question

Which of the following are Cryptography primitives?

Select one or more:

- ☑ password hashing
- ☑ Digital signatures
- ☑ Hash functions
- □ Message Authentication Codes (MAC)
- ☑ Key-exchange
- ☑ Encryption