

My sites / 21W-COMSCI136-1 / Week 6 / Midterm exam

Winter 2021 - Week 9



Winter 2021 - COM SCI126-1 - DEILED

Winter 2021 - COM SCI136-1 - REIHER		
Started on	Tuesday, 9 February 2021, 7:57 AM PST	
State	Finished	
Completed on	Tuesday, 9 February 2021, 9:06 AM PST	
Time taken	1 hour 8 mins	
Grade	88.00 out of 100.00	
Question 1		
Incorrect		
0.00 points out of 4.00		

Let P be the set of all states of a system, R be the set of states a particular security mechanism allows the system enter, and Q be the set of all secure states in the system as defined by the system's security policy. If there is a state r that is a member of P and R, and r is not a member of Q, which of the following describes the security mechanism?

- a. The security mechanism is secure
- b. The security mechanism matches the security policy
- o. The security mechanism is narrow

od. The security mechanism is broad

o e. The security mechanism is precise

Your answer is incorrect.

The correct answer is:

The security mechanism is broad



Ω

What is the purpose of a shadow password file?

- a. To prevent non-privileged users from accessing some password-related information
- b. To allow the use of salting in password storage
- oc. To allow the system to send users plaintext versions of passwords they have forgotten
- d. To permit storage of passwords in encrypted forms
- e. To deceive attackers into trying to crack fake passwords

Your answer is correct.

The correct answer is:

To prevent non-privileged users from accessing some password-related information

Question ${f 3}$

Correct

4.00 points out of 4.00

Which of the following is an example of a covert channel?

- a. Sending data between two machines encrypted with the receiver's public key
- o b. A tamper-resistant hardware link between two computers that is only usable by the computers' trusted processes
- oc. Sending data between two machines encrypted with the sender's private key
- od. Diffie-Hellman key exchange
- o e. Sending information between two processes by adjusting the time slice behavior of the sender

Your answer is correct.

The correct answer is:

Sending information between two processes by adjusting the time slice behavior of the sender





For a commercial system trying to provide separation of function, which of the following is likely to be true?

- a. Different security mechanisms will be used in each part of the system
 b. The system will use the Bell-LaPadula security model
 c. Strong barriers will be placed between users working for different clients who are competitors
- d. Critical security functions will require at least two different users to take action
- e. New software will not be developed on production systems

Your answer is correct.

The correct answer is:

New software will not be developed on production systems

Question 5

Correct

4.00 points out of 4.00

Which of the following is the best example of transitive trust?

- a. Using cipher block chaining to protect a data transmission containing multiple packets
- o b. Using virtual memory techniques to prevent a process from accessing another process' memory
- c. TPM used by the OS to sign the validity of a particular version of an application
- d. The Biba integrity security model
- e. Using nonces to defeat a replay attack

Your answer is correct.

The correct answer is:

TPM used by the OS to sign the validity of a particular version of an application



Which of the following is the best example of a phishing attack?

- a. Using a buffer overflow to take over a web server
- o b. A forged email saying that you need use a particular web site to reset your password
- o. Leaving a flash drive infected with malware lying in a parking lot
- od. Performing a man-in-the-middle attack on Internet commerce
- o e. An email message trying to sell you a product you don't want

Your answer is correct.

The correct answer is:

A forged email saying that you need use a particular web site to reset your password

Question 7

Correct

4.00 points out of 4.00

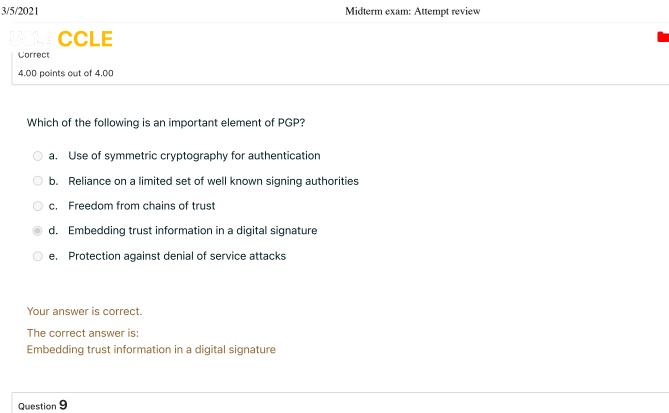
Which of the following is the best example of fail safe design?

- a. A reverse firewall that only permits outgoing packets to a set of trusted IP addresses
- b. Data execution prevention
- oc. Exclusively using open source libraries in one's software products
- d. Using timestamps in a cryptographic protocol
- e. SYN cookies

Your answer is correct.

The correct answer is:

A reverse firewall that only permits outgoing packets to a set of trusted IP addresses



Which of the following approaches would be helpful in detecting that a piece of ciphertext was encrypted using only permutation techniques?

- a. Attacking the random number generator used to create the key
- b. The Kasiski method

Correct

4.00 points out of 4.00

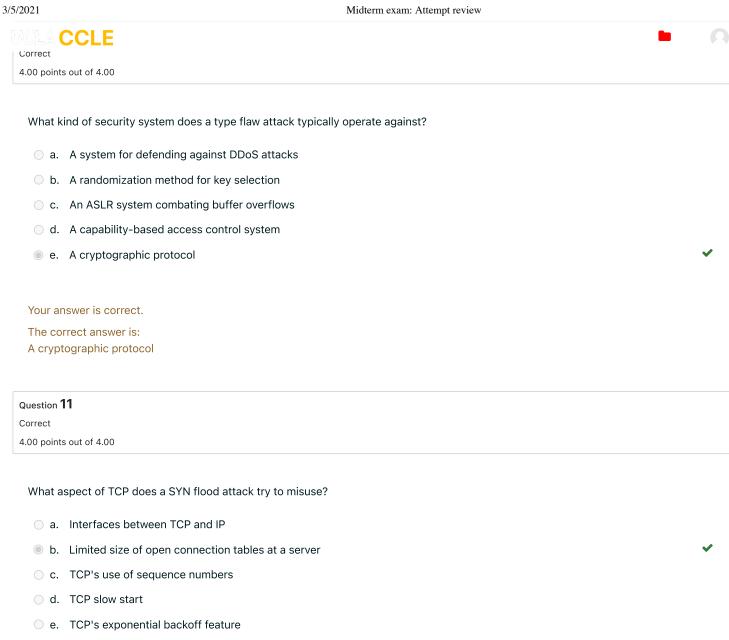
- oc. The Index of coincidence method
- d. Finding repeated patterns of symbols in the cipher text
- e. Examining the frequency distributions of the encrypted data

Permutation ciphers do not change the frequency distribution of the plaintext symbols

Your answer is correct.

The correct answer is:

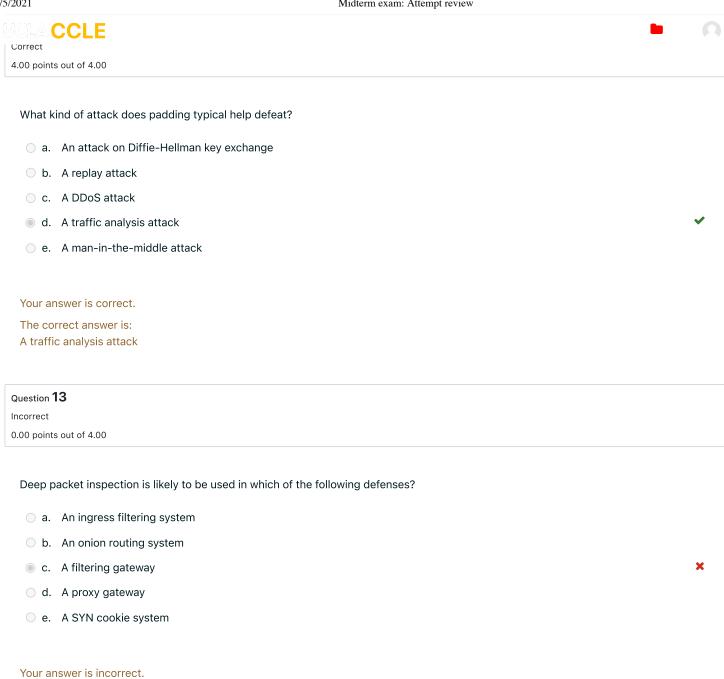
Examining the frequency distributions of the encrypted data



Your answer is correct.

The correct answer is:

Limited size of open connection tables at a server



https://ccle.ucla.edu/mod/quiz/review.php?attempt=5022385&cmid=3638037

The correct answer is: A proxy gateway



Ω

Which of the following approaches helps a security protocol avoid the suppress-replay attack when timestamps are used in the protocol?

- a. Including multiple timestamps in all messages
- b. Using asymmetric cryptography in the protocol
- o. Using symmetric cryptography in the protocol
- od. Ensuring all parties in the protocol are authenticated
- e. Always using timestamps from a single clock

Your answer is correct.

The correct answer is:

Always using timestamps from a single clock

Question 15

Correct

4.00 points out of 4.00

Why have modern GPUs caused problems with the use of passwords for authentication?

- a. They make dictionary attacks easier
- b. They make password salting impossible
- o. GPUs cannot authenticate users via passwords
- od. They can intercept and divulge passwords when they are created
- o e. They limit possible choices of passwords

Your answer is correct.

The correct answer is:

They make dictionary attacks easier





Node A is sending a large quantity of data to node B over the n	etwork. They are encrypting the data with AES, using ECB mode. A
network error flips one bit in the encrypted version of block N.	Which blocks will be improperly deciphered at B due to the bit flip?

- a. Block N-1, block N, and block N+1
- b. All blocks in the same packet as block N
- o. Block N and block N+1
- od. Block N and all subsequent blocks
- e. Block N

Your answer is correct.

The correct answer is:

Block N

Question 17

Correct

4.00 points out of 4.00

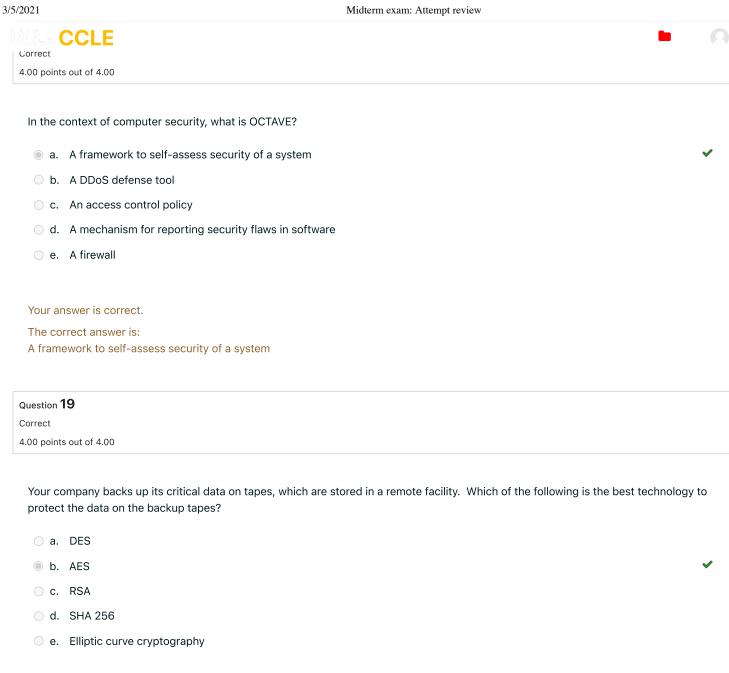
Which of the following changes to the basic Chinese Wall policy does the aggressive Chinese Wall policy add?

- a. Adding integrity controls to confidentiality controls
- b. Ability to apply the model in a distributed environment
- c. A generalization of the conflict of interest classes
- od. More precise inspection of operations on objects controlled by the policy
- Applicability to system objects, in addition to user level objects

Your answer is correct.

The correct answer is:

A generalization of the conflict of interest classes



Your answer is correct.

The correct answer is:

AES





Which of the following is an advantage polyalphabetic substitution ciphers have over monoalphabetic substitution ciphers?

- a. Polyalphabetic ciphers make frequency analysis harder
- b. Polyalphabetic ciphers offer better diffusion properties
- c. Polyalphabetic ciphers are safe against use of index of coincidence cryptanalytic methods
- d. Polyalphabetic ciphers offer better perfect forward secrecy
- o e. Polyalphabetic ciphers use simpler key creation methods

Your answer is correct.

The correct answer is:

Polyalphabetic ciphers make frequency analysis harder

Question 21

Correct

4.00 points out of 4.00

In the context of use of cryptography, what is meant by a round?

- a. The period after which a new key must be established
- b. The period over which feedback is applied in use of a cryptographic mode
- oc. One of several repeated operations as part of a cipher
- od. An exchange of messages in a cryptographic protocol
- The steps in negotiating the cipher and other properties of an encrypted session

Your answer is correct.

The correct answer is:

One of several repeated operations as part of a cipher



Ω

In the context of computer security, what is the difference between a weakness and a vulnerability?

- igcirc a. A weakness is a more serious security problem than a vulnerability
- D. There is no meaningful difference between these terms
- o. A weakness is a system flaw with no security implications, while a vulnerability is a flaw with security implications
- \bigcirc d. A weakness is a vulnerability that can be exploited
- A vulnerability is a weakness that can be exploited

Your answer is correct.

The correct answer is:

A vulnerability is a weakness that can be exploited

Question 23

Incorrect

0.00 points out of 4.00

Which of the following is true of identity-based encryption?

a. The only secrets required by such a system are the secret keys

Another secret is used to derive the keys

- b. It uses symmetric cryptography
- o. It does not require trusted third parties
- d. It can provide key escrow services
- e. It can be based on RSA

Your answer is incorrect.

The correct answer is:

It can provide key escrow services





Which of the following operations is easy to perform in a capability-based access control system?

- Determining the entire set of subjects that can access an object
- $\ \, \bigcirc$ b. Taking access permissions away from a user in a distributed system
- Determining the entire set of objects that a subject can access

- Just examine the subject's capabilities
- Od. Ensuring proper access control when subjects and objects are located in different nodes of a network
- o e. Changing a remote user's ability to access a local resource

Your answer is correct.

The correct answer is:

Determining the entire set of objects that a subject can access

Question 25

Correct

4.00 points out of 4.00

Which of the following is true of IPSec?

- a. It includes procedures for key distribution
- b. It can only be used to provide message confidentiality
- C. It only works with IPv4
- Its transport mode encrypts only the payload of an IP packet
- e. It can be used to provide availability

Your answer is correct.

The correct answer is:

Its transport mode encrypts only the payload of an IP packet

■ Sample midterm exam answer ...

Jump to...

Lecture 11: Intrusion ... ▶











