Quiz 5

Due Feb 2 at 11:59pm **Points** 15 **Questions** 11
Available Feb 1 at 12pm - Feb 2 at 11:59pm **Time Limit** 30 Minutes

Instructions

This quiz covers the following module objectives:

- MO 1. Identify the advantages and disadvantages of symmetric encryption algorithms (CO 4)
- MO 2. Identify the advantages and disadvantages of asymmetric encryption algorithms (CO 4)
- MO 4. Identify transposition cipher, substitution cipher, and one-time pad (CO 4)
- MO 5. Perform encryption and decryption using the Cæsar Cipher (CO 4)
- MO 6. Perform encryption and decryption using the RSA algorithm (CO 4)
- MO 7. Identify the expected properties of a good hash function (CO 4)

This quiz is no longer available as the course has been concluded.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	14 minutes	15 out of 15

Correct answers are hidden.

Score for this quiz: **15** out of 15
Submitted Feb 1 at 12:48pm
This attempt took 14 minutes.

Question 1

1 / 1 pts

One disadvantage of symmetric encryption is:

○ It consumes computer resources

● The need to keep the key secret

○ It is slow

○ It is more prone to attacks

Question 2

1 / 1 pts

Suppose Alice encrypted a message using Bob's public key and sent it to Bob. If an attacker was able to intercept Alice-Bob message, which of the following can be compromised:

○ Confidentiality

● Integrity

○ Both confidentiality and integrity

○ Neither confidentiality nor integrity can be compromised

Question 3

1 / 1 pts

(True/False): One-way hash function means that for a given code h, it is computationally feasible to find x such that H(x)= h.

○ True

● False

Question 4

2 / 2 pts

The word "CAT" is encrypted using Caesar cipher. The resulted ciphertext is:

● FDW

○ FDX

○ GEX

○ GEW

Question 5

2 / 2 pts

(True/False): In Asymmetric key encryption, the private key cannot be derived from the public key

● True

○ False

Question 6

1 / 1 pts

-55 mod 12 = ??

○ 8

○ 7

○ -5

○ -7

● 5

Question 7

1 / 1 pts

Which one is the one way cryptographic hash function?

○ DES

○ AES

● MD5

○ RSA

Question 8

2 / 2 pts

Suppose in RSA algorithm we choose p = 5, q = 13, n = 65, and e = 5, if the plaintext M is 3, what is the ciphertext C?

○ 81

● 48

○ 64

○ 243

Question 9

1 / 1 pts

Suppose that there are 10000 people in a network and Everyone try to communicate with each other using encrypted message. How many keys are needed in total to perform the communication if they use symmetric crypto-system? Here $\binom{n}{m}$ means combination of n things taken m items at a time without repetition.

● $\binom{10000}{2}$

$\binom{n}{m}$ means combination of n things taken m items at a time without repetition.

○ $\binom{10000}{1}$

○ $\frac{10000*10001}{3}$

○ $\frac{9999*10001}{2}$

Question 10

2 / 2 pts

Suppose that there are 10000 people in a network and everyone tries to communicate with each other using encrypted message. How many keys are needed in total to perform the communication if they use asymmetric crypto-system (public key crypto-system)?

● 20000

○ 9999

○ 20003

○ 1

○ 10002

Question 11

1 / 1 pts

Alice wants to communicate with her friends in an esoteric language in encrypted way. In order to do this, they define a new language with 500 letters. Now if they use substitution cipher, what is the possible number of substitution ciphers? Here, n**!** means n factorial.

○ 26**!**

○ 503**!**

○ 501**!**

● 500**!**

Here, n**!** means n factorial.

Quiz Score: **15** out of 15