ⓘ **This quiz has been regraded; your score was affected.**

Quiz 4: Asymmetric Cryptography

Due Feb 15 at 11am **Points** 12 **Questions** 8 **Available** Feb 8 at 3pm - Feb 15 at 11am
Time Limit None

This quiz was locked Feb 15 at 11am.

Attempt History

	Attempt	Time	Score	Regraded
LATEST	Attempt 1	10,136 minutes	9 out of 12	10 out of 12

Score for this quiz: **10** out of 12
Submitted Feb 15 at 4:06pm
This attempt took 10,136 minutes.

Question 1

0 / 1 pts

Which of the followings are true about asymmetric cryptography? Check all that apply.

You Answered
☑ Asymmetric cryptography is also called private-key cryptography.

Correct!
☑ Key distribution and management should be addressed when using asymmetric cryptography.

□ Asymmetric cryptography supersedes and generalizes symmetric cryptography.

□ Given the same key length, asymmetric cryptographic scheme is more secure than symmetric cryptographic scheme.

Question 2

Original Score: 0 / 1 pts **Regraded Score: 1 / 1 pts**

ⓘ **This question has been regraded.**

Suppose f is a trapdoor one-way function designed to be used with the key, k. Which of the followings are computationally easy? Check all that apply.

Correct!
☑ Computing f if the input to f and k are known.

Correct!
☑ Computing f^{-1} if the input to f^{-1} and k are known.

□ Computing f^{-1} if the input to f^{-1} is known.

□ Determining k if the input and the corresponding output of f are known.

Question 3

1 / 1 pts

Which of the followings does the RSA algorithm support? Check all that apply.

Correct! ☑ Digital signature

Correct! ☑ Encryption/decryption

Correct! ☑ Key exchange

Question 4

0 / 1 pts

Which of the followings does the Diffie-Hellman Key Exchange support? Check all that apply.

□ Digital signature

You Answered ☑ Encryption/decryption

Correct! ☑ Key exchange

Question 5

1 / 1 pts

Consider using RSA with the following two primes: p=5, q=11. Which of the following values can work for the public key e? Check all that apply.

□ 2

□ 5

Correct! ☑ 7

□ 8

Correct! ☑ 9

□ 15

Correct! ☑ 21

co-prime with p*q and %2!=0

Question 6

1 / 1 pts

Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive element. Party A chooses 2 and party B chooses 4 as their respective secrets. Which is their Diffie-Hellman Key?

Correct! 2

powerMod(3,2x4,7)

Correct Answer 2

Question 7

3 / 3 pts

This question requires the use of SageMath (or other math software). Consider the RSA cipher with the following public key:

N = 38485385893612647530529565399136160386558570363459

e = 12036041725135809493242715057143070093942766266573

A message of English letters is first converted into a number as follows: First, convert each letter into its numeric equivalent in two digits (i.e., A = 01, B = 02, …, Z = 26). Next, those two-digit numbers are concatenated to form a number (e.g. AXE = 012405, which corresponds to the number 12,405). This number is then encrypted by RSA using the given public key.

Since N is not very large, factorizing it does not take too long. Decrypt the ciphertext shown below and translate the result into letters of the alphabet to discover the message. (Note that when you enter your answer, all letters must be in upper case, e.g. HOPE rather than Hope or hope.)

38339997921296992667439824744705054840732860561898

(In SageMath, the function inverse_mod(x,y) gives the multiplicative inverse of *x* modulo *y*, and the function power_mod(x,y,z) returns $x^y \bmod z$.)

Correct!

PELE

Correct Answers

PELE

Question 8

3 / 3 pts

Use Polland’s p-1 method to factorize the following number into a product of two primes:

201557389900540095613559219541299540522405259329399736824858252876376521311053006710577

What is the value of the larger prime? (Use SageMath or other platforms.)

Correct!

26935068487360434215864599912291896955872647053313

Correct Answers

26935068487360434215864599912291896955872647053313

Quiz Score: **10** out of 12