exam test take 1

Due No due date **Points** 9 **Questions** 9 **Available** after Jun 8 at 4pm
Time Limit 30 Minutes **Allowed Attempts** 2

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	5 minutes	9 out of 9

ⓘ Correct answers are hidden.

Score for this attempt: **9** out of 9
Submitted Jun 8 at 4:30pm
This attempt took 5 minutes.

Question 1

1 / 1 pts

How large is the key space in case of a classical substitution cipher (English alphabet)?

- (●) 26! (26 factorial)
- ( ) 26
- ( ) 2^26 (2 to the 26)
- ( ) 25

Question 2

1 / 1 pts

How large is the key space in the case of the classical shift cipher (English alphabet)?

- ( ) 13

- 2^26 (2 to the 26)
- 3
- 26

Question 3

1 / 1 pts

What makes perfect schemes unpractical?

- The fact that identical messages will always be encrypted in the same way.
- The fact that the encryption algorithm has exponential running time.
- They are hard to implement on computers
- The fact that the key needs to be as long as the message.

Question 4

1 / 1 pts

Out of the triple (Gen, Enc, Dec) which one needs to be deterministic in all cases?

- Dec
- Enc and Dec
- None of them
- All of

Question 5

1 / 1 pts

What do we mean when we speak about the correctness of a scheme?

- That the distribution is indistinguishable from random output.
- That the encryption algorithm is randomized.
- That an attacker can win the eavesdropping experiment with negligible probability only.
- Decryption of the ciphertext gives back the original plaintext.

Question 6

1 / 1 pts

What is a true difference between a perfectly secure and a computationally secure scheme?

- In a perfect scheme, the distinguisher always has limited power
- In a computationally secure scheme, the distinguisher never wins with probability larger than 1/2
- In a perfect scheme, the distinguisher wins with probability below 1/3
- In a computationally secure scheme, the distinguisher may win with probability larger than 1/2

Question 7

1 / 1 pts

Which of the following functions is negligible (as n goes to infinity)?

- 1/(log(n)

- log(n)
- 1/n^100
- exp(-n)

Question 8

1 / 1 pts

Which scheme's security requires the assumption on the difficulty of factoring?

- One-time pad
- AES
- Diffie-Hellman key exchange
- RSA

Question 9

1 / 1 pts

Which of the following modes of operation has the flaw that identical plaintexts get encrypted identically?

- ECB
- CBC
- OFB
- Counter

Quiz Score: **9** out of 9