Feedback — Week 1 Quiz

Help Center

You submitted this quiz on **Fri 23 Oct 2015 12:25 AM IST**. You got a score of **8.75** out of **12.00**. You can attempt again, if you'd like.

Question 1

Consider the Vigenere cipher over the lowercase English alphabet, where the key length can be anything from 8 to 12 characters. What is the size of the key space for this scheme?

Your Answer		Score	Explanation
○ 4 * 26^12			
◉ 26^8 + 26^9 + 26^10 + 26^11 + 26^12	✔	1.00	
○ 26!			
○ 26^12			
Total		1.00 / 1.00	

Question 2

Consider the Vigenere cipher over the lowercase English alphabet, where the key has length 8. For which of the following message spaces will this scheme be perfectly secret? (Check all that apply.)

Your Answer		Score	Explanation
☑ The set of all strings of lowercase English letters containing at most 8 characters.	✖	0.00	
☐ The set of all 9-character strings of lowercase English letters.	✔	0.25	
☐ The set of all 7-character strings of lowercase English letters.	✖	0.00	
☐ The set of all 8-character strings of lowercase English letters.	✖	0.00	
Total		0.25 / 1.00	

Question 3

What is the result of encrypting the ASCII plaintext "cool!" using the variant Vigenere cipher (where encryption is done using byte-wise XOR) and key 0x01 3F?

Your Answer		Score	Explanation
(•) 0x62 50 6E 53 20	✔	1.00	
( ) 0x26 05 E6 35 02			
( ) 0x63 6F 6F 6C 21			
( ) 0x62 50 6F 6C 21			
Total		1.00 / 1.00	

Question 4

Say we have a scheme with a claimed proof of security with respect to some definition, based on some assumption. The scheme was successfully attacked when used in the real world. What are possible reasons for this? (Check all that apply.)

Your Answer		Score	Explanation
☐ The attacker did not read the proof of security.	✔	0.25	
☑ The definition of security may not correctly capture the real-world threat model.	✔	0.25	
☑ The assumption may be false.	✔	0.25	
☑ The proof might be incorrect.	✔	0.25	
Total		1.00 / 1.00	

Question 5

In the definition of perfect secrecy, what threat model is assumed?

Your Answer		Score	Explanation
○ The attacker can eavesdrop on as many ciphertexts as it likes.			
○ The attacker can eavesdrop on a single ciphertext.			
○ The attacker is able to interfere with the communication channel between the two honest parties.			
◉ The attacker can carry out a chosen-plaintext attack.	✖	0.00	
Total		0.00 / 1.00	

Question 6

Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[C='bb']? Express your answer to 4 decimal places with a leading 0, i.e., if your answer was 1/2 then you would enter 0.5000 (without a trailing period).

You entered:

0.0084

Your Answer		Score	Explanation
0.0084	✔	2.00	
Total		2.00 / 2.00	

Question 7

Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[M='aa' | C='bb']? Express your answer to 4 decimal places with a leading 0, i.e., if your answer was 1/2 then you would enter 0.5000 (without a trailing period). Note: carry out the calculation exactly (i.e., do not use the truncated result that you entered as your

answer in the previous question) before truncating your answer to 4 decimal places.

You entered:

0.9473

Your Answer		Score	Explanation
0.9473	✔	2.00	
Total		2.00 / 2.00	

Question 8

Which of the following are true for obtaining perfect secrecy using the one-time pad, assuming the message space contains messages all of some fixed length? (Check all that apply.)

Your Answer		Score	Explanation
☐ The all-0 key must be avoided, since when the all-0 key is used the ciphertext is equal to the message being encrypted.	✔	0.25	
☑ The key must be as least as long as the messages in the message space.	✔	0.25	
☐ The key should be chosen uniformly.	✖	0.00	
☑ The key should be shared between the two communicating parties, and kept secret from any potential attacker.	✔	0.25	
Total		0.75 / 1.00	

Question 9

Consider the one-time pad over the message space of 5-bit strings, where Pr[M=00100] = 0.1 and Pr[M=11011] = 0.9. What is Pr[C=00000]? Express your answer to 5 decimal places with a leading 0. I.e., if your answer was 1/2, then you would enter 0.50000 (without a trailing period).

You entered:

.3125

Your Answer		Score	Explanation
.3125	✖	0.00	
Total		0.00 / 1.00	

Question 10

Which of the following are true about the Vigenere cipher? (Check all that apply.)

Your Answer		Score	Explanation
☑ The Vigenere cipher is computationally infeasible to break if the key has length 100, even if 1000s of characters of plaintext are encrypted.	✖	0.00	
☑ The Vigenere cipher is perfectly secret if the length of the key is equal to the length of the messages in the message space.	✔	0.25	
☐ The Vigenere cipher can always be broken, regardless of the length of the key and regardless of the length of plaintext being encrypted.	✔	0.25	
☐ A Vigenere cipher with key of length 100 can be broken (in a reasonable amount of time) using exhaustive search of the key space.	✔	0.25	
Total		0.75 / 1.00	