Homework 1
Kaitlynn (Katie) Prescott
I pledge my honor that I have abided by the Stevens Honor System.
September 28, 2018

Problem 2:

1. Two security properties to be considered:
   Authentication: Because Mallory can do more than just eavesdropping, it is important to know that you are communicating with the correct person.
   Integrity: For the same reason as above, you also want to ensure the messages are not being changed by Mallory, or anyone else, while in transit.
2. Alice and Bob's protocol does not ensure that another person hasn't discovered the key and changed the message, or any future messages.

Problem 3:

1. Vigenère cipher:
   a. t = 1: Ciphertext of p1 will be (x, x+1, x+2, x+3), ciphertext of p2 will be (x, x+3, x+2, x+5). The password can be determined (this becomes Caesar's shift cipher).
   b. t = 2: Ciphertext of both p1 and p2 will be (x, y, x+2, y+2) for some x and y. The attacker cannot determine the password because the ciphertexts are the same.
   c. t = 3: Ciphertext of p1 will be (x, y, z, x+3), ciphertext of p2 will be (x, y, z, x+5). The password can be determined.
   d. t = 4: Ciphertext of both p1 and p2 will be (x, y, z, w). The attacker cannot determine the password, because the ciphertexts are the same.
2. For the mono-alphabetic substitution cipher, if you have a plaintext character p and a ciphertext character c, then k(p) = c, where k is the permutation that determines the key. If you ask for an encryption of a plaintext that contains 25 distinct letters of the alphabet, then you can determine the key. You could use the plaintext "A quick brown fox jumps over the lazy dog." If a keyspace is chosen randomly, and is sufficiently large, and the plaintext is sufficiently small (i.e. 26! size keyspace, and 1 character plaintext).

Problem 4:

1.

testing testing can you read this
yep I can read you perfectly fine
awesome one time pad is working m
yay we can make fun of Nikos nowm
I hope no student can read this m
that would be quite embarrassingm
luckily OTP is perfectly secure m
didnt Nikos say there was a catch
maybe but I didnt pay attention m

we should really listen to Nikosm

yah we are doing fine without him

Key: **00**6f75666f756e64**00**68656b**00**7921636f6e67726174756c6174696f6e73**00**216c

** **Bold red** characters could not be deciphered for the key, but you can infer what character it is meant to be based on the rest of the message

Manually finding missing key values:

1. 59
2. 74
3. 65
4. 21

Final Key:
596f75666f756e64**74**68656b**65**7921636f6e67726174756c6174696f6e73**21**216c

My strategy was to xor 2 ciphertexts, and to check if there was a space in the plaintexts. If there was, I would save that location, and then xor the ciphertext with all spaces. Then at each index where there is a space, you can decode what the plaintext character is, and add it to the key at the correct location. Finally, I encoded the key in hex, and looped through to find where there are still None values (the initial value of the key), and default the value to '00'. Then, I xored the target ciphertext with the key. If the key wasn't known at a certain index, that character would become a '*', to make it more readable and inferable. Then I printed they plaintext and the key.

2\.
Keys:

9/12: 44 34 7d a5 8b 0d 3c f4 38 97 fc 46 14 67 84 f9 8e 46 7c df b2 fb 7b 6d 33 34 62 24 3f fc d0 94 21

9/13: 6d f7 f9 1e 0f b2 c5 eb 68 0f b5 ad 27 20 a6 53 48 5e 3f 0c 35 ee f5 26 17 48 d0 1c f1 7e dd e0 21

9/14: 3f 73 33 20 56 9d 0a 13 24 31 ae 78 31 17 29 01 9e 20 66 b2 c4 81 5c d8 d9 fc 32 f2 3c 55 bb ef 21

9/15: a5 2a 93 d3 2c c2 9e 62 a5 e6 4d b0 6d 9f 04 c7 91 ac fc 0c 11 ca 36 4c a2 12 a0 80 a8 14 38 64 21

9/16: fe ea a4 0d 1c 8c d9 33 c8 38 4d 22 ff 46 05 49 79 2b 32 2c 0a 89 11 d3 ee 45 a0 82 b2 77 00 5f 21

9/17: e2 5f a7 d8 ff c5 7e 10 9f ad 58 c4 38 37 0a 77 cb 2d e0 53 0f c5 5a 8c 1a 5d 7d ac 17 74 7c 3e 21

9/18: c0 86 c4 bb 31 db d7 56 1b 7c 0d c1 87 9f 62 65 be 63 da 35 83 0a 17 cc b9 48 f6 84 60 aa 70 d1 21

9/19: 85 08 58 9e b4 50 73 86 dd 37 5c d9 2f e7 d7 69 c8 41 a8 95 09 0f 3b 4e 87 28 66 aa 37 44 b8 c2 21

9/20: f9 a2 ac fc b9 ca ab 35 74 24 51 7d af 68 b3 4a 7d 45 b0 42 ae db 1c d3 cc 8b 08 c5 4a 33 d0 20 21

9/21: 59 41 dd 71 91 e2 c9 ae 6f 89 f0 c9 26 f3 0c c1 36 61 65 0e 54 b7 df d7 55 9b 8b c5 8f f6 68 3f 21

9/22: 42 48 c8 5c b0 a4 27 5c e7 8a de bd 1f 3d 9b a2 df 56 23 66 45 b1 6d 03 ef f1 7d d5 83 80 3d c7 21

9/23: ba f6 57 d4 0c 05 31 94 de ad c6 9d 40 dd e9 fd 84 bd 79 e1 95 28 fa c1 0c 09 5d 34 31 1c 2f 3c 21

9/24: 99 f4 73 37 4a 7a 2e 8d bd b4 2d da 15 e2 28 82 81 b0 03 28 7e e8 d3 d2 32 60 0c c3 98 ab 4a 30 21

Key on September 25th:

77 c4 c1 7a 25 6c 12 28 c1 d7 ef 7c 9c 13 dc bc 44 53 93 57 10 15 bd c6 98 c8 49 10 85 4b 6a c2 21