Jessica Noel

Homework 1

"I pledge my honor that I have abided by the Stevens Honor System."

Problem 1

1) The two basic security properties that should be considered are confidentiality and integrity. Confidentiality is important because they are communicated over an insecure channel - this would allow the key to be leaked. Integrity is important because this property ensures that the only two people who are able to access the messages are Alice and Bob, this is essential in secure message transferring.

2) Confidentiality as well as integrity are not satisfied in the above protocol. This is because if an attacker is to Obtain Ka all steps after become meaningless. The attacker can do exactly what Bob does. This causes Alice and Bob's messages to not be just between them.

Problem 2

1) The attacker can determine the password Of the user without much time and effort by using a brute force attack for $t=1$. Because P_1's password is simply the first 3 letters succeeding "a", he can easily see the pattern. When $t=2$, the attacker only has to choose between P_1 and P_2. Since the shift is Obvious, the password is still insecure. When $t=3$ the two patterns Eve can see are $x, y, z, x+3$ and $x, y, 2, x+5$. Given that there are only two possible options it still remains insecure. When $t=4$

Eve can still simply choose between P_1 and P_2. Since P_1 and P_2 are 4 characters long it does not differ much from as if t were equal to 2.

2.) A mono-alphabetic substitution cipher is trivial to break when the attacker launches a chosen plaintext attack because the attacker has the ability to create their own plaintext and encrypt it. By doing this it is easy for the attacker to know find the key length. There are also only 25 letters one would have to figure out, the last letter can be assumed.

Problem 3

The process I used to decipher the ciphertexts was crib-dragging. Essentially, if you XOR something against itself you get 0. If you XOR something against 0, you get itself. So if you XOR two things together and then XOR the result against one of them you will get the other. With crib-dragging you are "dragging" a common set of characters across the cipher text, by doing this you can get part of the original message/key. From this plaintext, cipher text pair you XOR to get the key. The key is you foundthekey! congratulations!!!

The texts are:

- Testing testing can you read this
- Yep I can read you perfectly fine
- Awesome one time pad is working
- Yay we can make fun of Ninos now
- I hope no Students can read this

- That would be quite embarrasing
- Luckily OTP is perfectly Secure
- Didnt Nikos say there was a catch
- Maybe but I didnt pay attention
- We should really listen to Nikos
- Nah we are doing fine without them