Julia Nelson
Homework 1
Cs306
“I pledge my honor that I have abided by the Stevens Honor System” - jnelson6

(2.1) The two basic security properties that Alice and Bob need to consider are **confidentiality** and **integrity**. Confidentiality, because they must protect themselves from unauthorized parties viewing through the unsecured network. Integrity, ignorer to protect their asset from being modified by unauthorized parties.

(2.3) In this protocol only part 2 and 4 satisfy the security properties integrity and confidentiality, while 1 and 3 do not.

(3.1) Possible: Plaintext(P1) = abcd
Plaintext(P2) = bedg
encrypts by Vigenere cipher. The attacker knows the cipher text as well.

If the attacker takes Plaintext(P1) and cipher text, the key can be determined. However, a vigenere cipher uses a repetitive key and key length.
If t = 1, we divide the Plaintext(P1) with key of length 1.
If t = 2, we divide the Plaintext(P1) with key of length 2.
If t = 3, we divide the Plaintext(P1) with key of length 3.
If t = 4, we divide the Plaintext(P1) with key of length 4.
The cipher is poly-alphabetic and depends not only on the key value but as well as the distance, making it impossible to determine the password when t = 1,2,3,4.

(3.2) In mono-alphabetic substitution cipher, it is simple to map an alphabet with the other alphabet without care about position in the plaintext. If we have a chosen plaintext we observe the alphabet value is converted and in which one so we can break it. This observation allows us to find the key value of the mono alphabetic cipher.
There are multiple possible plaintexts.
A mono-alphabetic substitution cipher can be secure (against only cipher text) is if we use random a random string of keys

(4.1)
1. testing testing can you read this
2. yep I can read you perfectly fine
3. awesome one time pad is working
4. yay we can make fun of Nikos now
5. i hope no student can read this
6. that would be quite embarrassing
7. luckily OTP is perfectly secure
8. didnt Nikos say there was a catch
9. maybe but I didnt pay attention
10. we should really listen to Nikos
11. nah we are doing fine without him

(4.2) c68b710955f8e0b1c137dc3077d80e6cc04864f32b2ae8f91ef2bfebe4b75fae21