COSC435 - Homework 2

Kevin Jang (kj460)

Part One: Written questions [25 points]

1. **[10 points]** A cryptosystem that offers *perfect secrecy (Links to an external site.)Links to an external site.* prevents an eavesdropper who observes an encrypted transmission from learning anything about the plaintext, other than its size.

Show with a counterexample that the Substitution Cipher doesn't provide perfect secrecy.

2. **[10 points]** Consider the following modification to one-time pad (OTP) encryption. Rather than share a single one-time pad, Alice and Bob have shared knowledge of two pads, $P1$ and $P2$.

Given a plaintext M, Alice creates the ciphertext $C=M\oplus P1\oplus P2$, where $\oplus$ denotes xor and $|M|=|P1|=|P2|$ (i.e., the size of the message and the two pads are all equal).

To decrypt, Bob takes the ciphertext and xors it with P1 and P2; i.e., $D(C)=C\oplus P1\oplus P2$.

Argue that if a one-time pad offers perfect secrecy, then the above scheme must also be perfectly secure.

3. **[5 points]** Prof. Pedantic, the esteemed Ineptitude Professor of Computer Science and Quackery at Wikipedia University, is developing a new terminal program (and associated service) to log into the servers in his lab. Although he is aware of ssh, he refuses to use it. Instead, he decides to construct his own novel protocol.
Like telnet and ssh, his remote console/terminal program should allow a remote user to type commands and execute them on a remote machine. Since Prof. Pedantic doesn't trust anyone — particularly the students in his introduction to network security class — he decides that all communication should be encrypted.

Prof. Pedantic decides to use the AES encryption algorithm in ECB mode. Is this a good choice? Give two reasons why or why not.

Answers:

1. Substitution Cipher doesn’t provide perfect secrecy, because this method can be broken by frequency analysis (look for frequencies of characters) and pattern analysis (as an example, double Qs could be double Ds, Es, Ls, etc.).
   When a long message gets encrypted with Substitution Cipher method, vowel characters (a, e, i, o, u), especially the English alphabet letter ‘e’ tends to appear significantly more frequent than other alphabet letters. Therefore, an adversary can use frequency analysis to make a valid guess that the most frequently appeared character on the cipher text is ‘e’.

2. If use of a single one-time pad offers perfect secrecy, we can know that an adversary doesn't have a knowledge on what this pad is. Therefore, although an adversary has a knowledge on a second pad and a cipher text, a plain text cannot be computed. Since as its name indicates, one-time pad uses each pad once and if pad is randomly generated, it also guarantees the independence between different pads. Also, one-time pad offers a perfect secrecy.

3. No, because ECB uses a Block Ciphers where blocks of plain text are individually encrypted and concatenated together. Therefore, it has the following issues: first, identical plaintext blocks produce identical ciphertext blocks, second, encrypted blocks can be shuffled (out-of-order) without detection. Due to the above reasons, the messages sent between remote user and machine can be discovered by an adversary.