Crypto Homework 1: Blocks and Streams

Tailang Cao u1480633

Q1:

A known-plaintext attack is an attack when the attacker knows the plaintext and the cyphertext or when the attacker knows what certain pieces of plaintext encrypt to. A ciphertext encrypted with an 8-bit block size block cipher means there are only 256 possible values. Knowing the plaint text and the cipher text, the attacker can easily create an algorithm to decrypt the key and get the rest of the messages.

For me, there are two methods that may apply. First is to try out all the possibilities. As there are only 256 options for each block, the process wouldn't take much effort. Second is to create a cryptogram or table with the already known ciphertext and build it up using common words, letters, etc.

Q2:

Part A: As the message is encrypted by the same key, the same plaintext will be encrypted to be the same cyphertext. The eavesdropper would then discern that Alice sent the same message if she did so, this would be dangerous if the message sent is a Boolean message. Also, as Alice is using the same block cipher, the eavesdropper will be able to know the size of the message and the key based on the cyphertext.

Part B: The attacker can change the message received by sending blocks of data that are of the same size as the cyphertext with bad data. They can also change the order of the data or delete them. All of above would result in failure of the communication.

Part C: We can use a cipher block chaining where an XOR is applied between the output of the previous block and the plaintext of the next block. Also, it uses an initialization vector which is used to help with randomization. This is less prone to attacks because it hides patterns that are possible to detect when just using ECB. We can also add a signature to each message that can be read with a public key to certify the identity of the sender.