Basics of Cryptography

Reading

- Section 8.4

Practice Problems

8.4 2, 3

Notes

Cryptography is centered around the following ideas:

Alice and Bob Typically there are two parties that are trying to communicate, and one is trying to send a message to the other. We typically call them Alice and Bob.

cypher This is the term for the specific cryptographic scheme that the two parties are going to employ.

plaintext This is the text message we want to send. It is typically converted to a series of numbers via some letter-number correspondence.

encryption We "encrypt" the plaintext via some algorithm that tells us how to convert each number in the plaintext into a new number.

cyphertext This is the result of the encryption process. It is the text we send across to the other party. It would typically look like meaningless jumble. In a good cryptographic system, knowing the cyphertext should not be giving you any information about the plaintext it came from.

decryption The other part will "decrypt" the cyphertext using an algorithm analogous to the encryption algorithm.

secret key Usually the encryption and decryption algorithms are based on some secret key that is somehow shared between the two parties. Only someone would knows the correct key would be able to correctly decrypt the cyphertext.

A very simple cypher could be developed using modular arithmetic. We start by assigning each letter to a number, starting with A being 1, B being 2 and so on, till Z which is 26.

For instance the word NUMBER would become the sequence of numbers "14 21 13 2 5 18".

Next we decide on a "secret key", which is a number between 0 and 26. We will choose 3. Now we shift all numbers up by 3, modulo 26. So a 24 would have become 1. In our example above, this would be "17 24 16 5 8 21".

Lastly we convert this back to letters: "QXPEHU". This is our cyphertext.

To decrypt this at the receiving end, we need to know that it was shifted up by 3. All we would have to do to decrypt then would be to shift left by 3, to revert the above process.

For practice, decrypt this: “DZHVRPH”

This cypher is of course quite vulnerable to a brute force attack: There are only 26 different possibilities, we could just try all possible shifts till we find one that makes sense.