Joshua Brown

9 Algorithms Chapter 4

September 13, 2018

Public key cryptography has become the main solution for sending secret messages across dangerous paths. Cryptography uses a simple yet affective strategy to protect a message someone would like to keep secret. An algorithm such as the shared message trick, block ciphers, and the paint mixing trick has allowed public key cryptography to be the main source to send and receive secret messages.

The shared message trick starts with two people who know the same number(key). From there one of you must communicate to the other adding up the key with another random number. The second person then receives the sum of both numbers and then subtracts the key number by the total you gave him. By doing this he will get the same number the first person chose to add. There are two problems with the shared trick and they are that it is too simple, as well as someone could analyze your messages statistically and find out what your secret numbers are. Block ciphers put an end to this weakness by adding more steps into the encryption process. First, long messages are broken into small block sized pieces that are usually 10-15 characters long. Now instead of adding a block and the key together, each block is mixed up by a set of rules. These rules can include adding the key to the block or subtract the second half of the key from the last part of the block. While this is a very good method to resist statistical attacks, it can still be reversed if somebody knows the key. The paint mixing trick is a very simple yet affective encryption method that cannot be statistically broken or reversed even if someone knows the key. Paint mixing is done by two people having a private number and announcing a public number for everyone to hear. Once you have those two number you multiply them together. The other person does the same thing with their private and public number. Next, we share our number that were multiplied out and multiply those with our original private number. Once both people have done that they will have the same number which is their shared secret number. The advantage of this paint mixing trick is that there is only a one-way path. There is no way for somebody to work backwards to get the decrypted message. The reason this method works so well is because you both didn’t get the same message with the same exact steps. Yes, they included the same numbers, but they were multiplied differently.

The most interesting part about the algorithm is how useful it is in the real world. Companies like the NSA and other security agencies consistently use algorithms like these. While some of it may be used to spy on Americans it is stull useful. These ideas are important to know for classes I am going to take next semester and even in my future job searches.