A Brief Insight into Cryptography

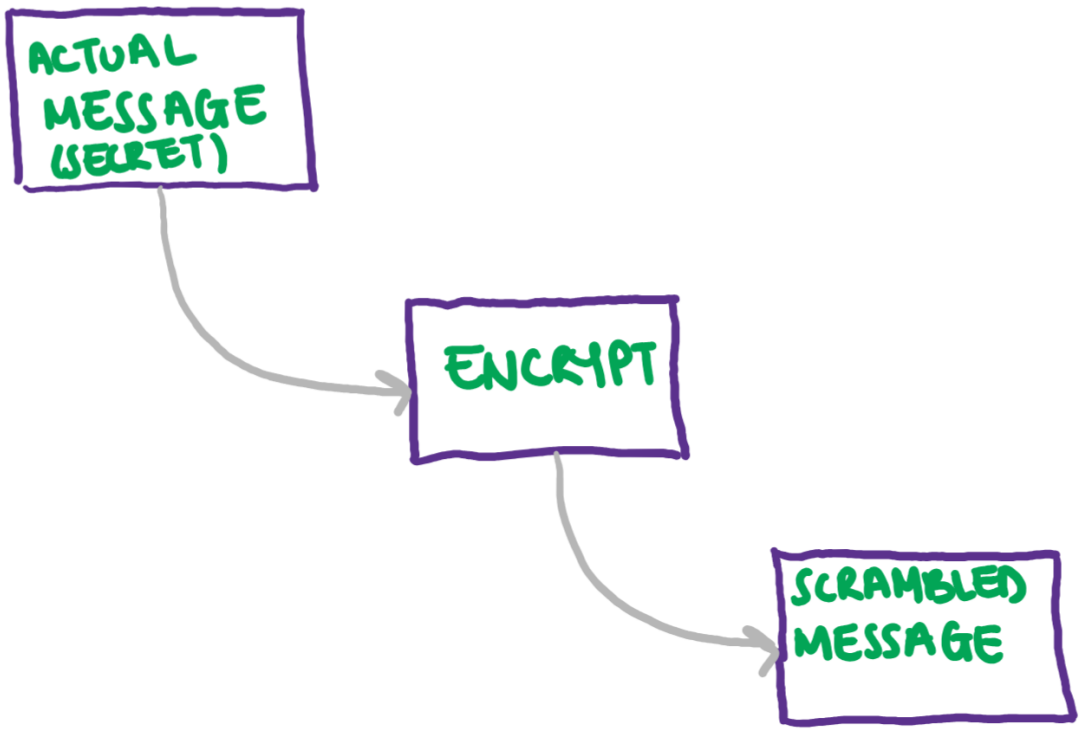
Have you ever wanted to send a message or some information that you wanted to keep secret between you and the receiver? If yes, then you're certainly not the first.

Throughout human history, there has always been a need to communicate secretly, whether this is official secrets, such as between generals at war, or just between two school friends.

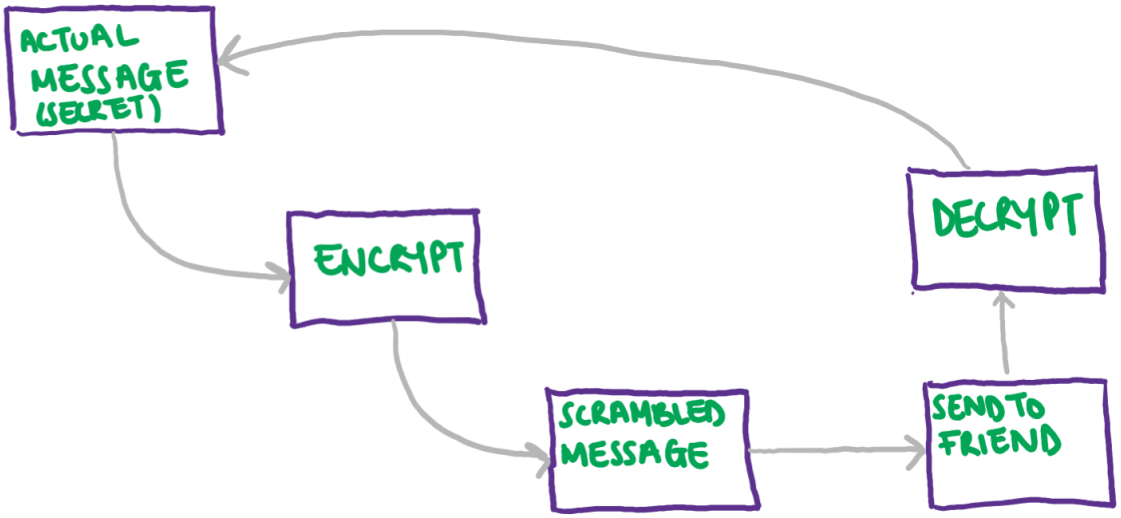
As a result, we have centuries and centuries worth of developing and enhanced 'Cryptography'.

The standard definition of the word 'cryptography' is: 'The art of writing or solving codes'. And most commonly, this involves scrambling the message to be sent, so that it becomes unreadable unless you have the correct key.

This process is widely known as encryption.



If we want to turn the scrambled message back to the actual message, then we need to DECRYPT the scrambled message. This means the whole chain looks like this:



The technical term for ‘actual message’ is called the ‘plain text’ and the technical term for ‘encoded message’ is called the ‘cipher text’. If you do a lot of research into cryptography, then you will most likely see these terms a lot.

So what actually is encryption?

Consider the encryption process as a series of steps that are needed to jumble up the text. And the decryption process as the reverse of these steps.

These instructions could involve replacing letters with symbols or moving sentences about in a specific pattern or even just writing everything backwards. All these would be considered ‘encryption’.

Furthermore, the more complex your instructions the more difficult it will be to decrypt the message (without the instructions). Hence, having complex instructions is the safest option (for really top secret messages!).

As mentioned, throughout history, many different types of encryption have been used constantly. However, nowadays you may not notice because a lot of encryption is done for us, via the messaging facilities that we use on our devices.

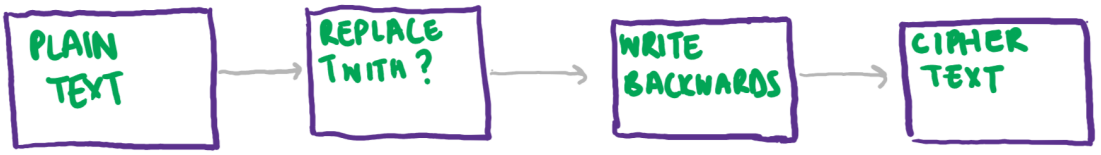
//symmetric and asymmetric?

Example

To show the very basics of encryption, here is a made up encryption process:

Replace all letter ‘t’s with a ‘?’ and write the message backwards:

Therefore, if we had the message: HELLO THIS IS MY SECRET MESSAGE, to encrypt. Then we would encrypt it, as follows.



Hence, with HELLO THIS IS MY SECRET MESSAGE, after the first instruction we have: HELLO ?HIS IS MY SECRE? MESSAGE.

And after the second instruction (our final cipher text), we have: EGASSEM ?ERCES YM SI SIH?

Of course, this is a rubbish encryption process and would not be keeping many secrets, but very useful to be able to see the process.

Important Note: often you will see the collective name for an encryption process as a ‘cipher’.

Famous Ciphers

As mentioned, cryptography has been around for hundreds of years, which means it’s a given that there are many encryption processes (or ciphers) that have gained fame, and are now used to form the basis of many more complex ciphers.

Examples of these are: Caesar cipher, Substitution cipher and Transposition cipher.

In other resources, there is much more detail about what these ciphers are and how you can use them.

Linking to Computer Science

Whilst at first the connection between Cryptography and Computer Science may not be that big, only that it’s needed so that we can communicate over the internet, the connection is very deep rooted.

As ciphers get increasingly more complicated, decrypting a message by hand can become very difficult. Therefore, being able to code your own solutions is almost necessary. Whilst a lot of online decryption tools exist for famous ciphers, these are rendered useless when a complex or modified cipher is used.

In my own experience at using programming to decrypt messages, having a visual representation is the most useful. This makes JavaScript such a useful language to use for cryptography, as we can create very visual tools.

Furthermore, Alan Turing provides a great link between Cryptography and Computer Scientists. Turing was a part of the code breaking team at Bletchley Park during WW2, where his role was to help figure out how to decipher the Enigma Code.

The Enigma code was a very complex cipher used by the Germans to send messages during the war.

Turing was also widely known for his work in developing the first computer and developing the basis for Artificial Intelligence (through the Turing Test), hence he is one of the most influential figures in Computer Science.

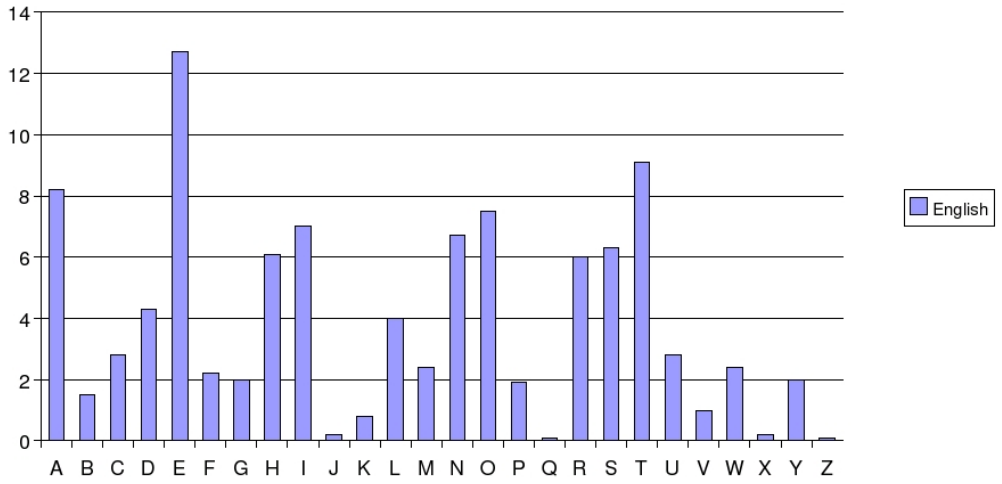
Important Decrypting Techniques

Whilst using programming to help decrypt messages is very important, unless the key is known, this cannot be the only technique used.

For example, if you had a scrambled up message with no clue where to start or what cipher to use, then you would be left with the option to try every cipher to ever exist, which would take quite some time.

However, there is a very simple technique that can make finding the type of cipher much easier: ANALYSING LETTER FREQUENCIES.

In the English language, in any text (that is of suitable length) the expected proportion of letters appearing are shown in this graph:



As you can see, the letter E, T, A and O are the most frequent, and the letters J, Q, X and Z are the least frequent.

Each of the resources, for every cipher, will contain explanations of how you can spot the cipher using letter frequencies. For now, it is just important to note that the frequency of letters in a text is vital.

The second vital tool to decryption are CRIBS.

Simply, a crib is a word or phrase that you know will appear in the plain text.

For example, if you had intercepted an encoded letter from Alice to Bob, you may infer that the letter will begin ‘Dear Bob’ or something similar.

In fact this is partially how the Enigma code was broken in WW2. The decrypters inferred that every message the Germans sent would end in ‘HEIL HITLER’.

Conclusion

Hopefully now you have a taste for what cryptography is, and are ready to move on and start writing and cracking some ciphers using your knowledge and programming skills!