# Cryptography Assignment - CS4182

[Github](https://github.com/TomC17/CS4182-Project-2020)

Benjamin Setterfield 19247125

Ian Rowland 19190589

Ruadhrí Ryan 14196115

Tom Carey 19192363

### Introduction - (Placeholder by Tom for now)

Cryptography in its earliest incarnations dates back to the very first time that man attempted to write, he would make scribbles which had meaning to no one but him unless given the “key”, in this case being the ability to read. Cryptography and the written word grew alongside each other as humans progressed, needing more and more complex information to be expressed to others or hidden from sight. Today Cryptography is used in everyday life just out of sight in message apps, account password protection, cloud storage and other online services in the form of Encryption. All of this was made possible by great minds throughout history making great strides in this field, from Polybius to Alan Turing and many more.

### Origins of Cryptography - Tom Carey 19192363

Cryptography sprouted from ”the need to conceal messages” (*Damico 2009, para 3*). Cryptography itself is rooted in the earliest civilisations we know from history, Greece and Egypt being notable mentions. The very word “Cryptography” comes from the Greek “Kryptos” and “Graphein” which mean “Hidden Writing”. The Egyptians however are responsible for the very first Cryptographic techniques that we know of dating back 4000 years.. Their Hieroglyphic writings were incomprehensible to all but the royal scribes who would transfer messages from kings (*Origin of Cryptography 2020*). Actual cryptographic efforts have been found “carved into the wall of a tomb from the Old Kingdom of Egypt circa 1900 BC” but these don’t appear to have been serious, rather they seem to be for the amusement of others, though this is not certain (*History of cryptography 2018*).

Scholars would eventually shift their cryptographic techniques to something closer to what would be recognised by many as Cryptography today, albeit quite simply. This technique was a “simple mono-alphabetic substitution cipher”, to use this cipher they replaced the alphabet of the message the message was written in with another alphabet according to a rule or key. (*Origin of Cryptography 2020 para 3*) A modern example of this kind of cipher would be to take the Alphabet and assign each letter a number at random and take a note of which letters are assigned what number, then write a message in english and rewrite it with the numbers you’ve chosen, from there you are left with a simple secret message in the form of a long string of numbers, the note with the letters and their corresponding numbers is the rule or key. Another early form of cipher is the famous “Caesar Shift Cipher” or simply “Caesar Cipher”. This method involved shifting the alphabet by a set number. For example if you offset the Alphabet by 5 then A would be F, B would be G, Z would be E etc. This was a simple cipher but was rather popular and easy to create, in this case the key would be the number you’ve chosen to offset by.

The Simple Substitution Cipher is an improvement upon the Caesar Cipher. Instead of shifting letters along the Alphabet according to a number, the letters are swapped around and the way each letter is swapped is the key for the cipher. Any letter combination is viable A-L, B-F, F-K, etc. The sheer amount of possible variations (4x1026) makes this an incredible improvement on the Caesar Cipher, even today a brute force of this cipher takes time. The human element in this cipher is its biggest flaw, obvious combinations make it much easier to break. (*Traditional Ciphers 2020)*

Steganography, while not directly a form of Cryptography is an important part of its development and history. Steganography focuses more on concealing the message entirely rather than just its contents and as a result is used in Cryptography as an added layer of security or it can be used on its own. Steganographic techniques are said to date back to the Ancient Greeks and Spartans. Spartans used the scytale transposition cipher but it is not known if it was used for encryption specifically. The ancient Greeks used simple steganographic techniques such as writing messages under tables, tattoos under hair or under wax on tablets. While none of these are Cryptographic techniques they and other Steganographic techniques can be used to enhance the security of an encrypted message. (*History of cryptography 2018, para 4*)

The Polybius Square was a concept used in telegraphy to encode the alphabet to make it possible to send messages via light signals, such as the number of torches in an area that are lit or unlit. The system was developed in the 2nd century BC by Polybius, a greek historian(*Polybius* 2020). While there is no evidence that such a system was actually used then the system is noteworthy as it is now used in Cryptography and Steganography. The Polybius Square is a 5x5 grid with each letter in the alphabet stored in it with the one notable difference being “I” and “J” are stored in the same square. The outside of the square has the number one to 5 along the top and left of the square. Using this system with torches would have been a great advancement from previous torch signals which were rather simple before this. (*Telegraphy* 2020)

Simple encryption techniques such as these set the basis for more and more complex encryption types to be developed as information grew more and more crucial to keep from prying eyes. This is seen in how decryption techniques have grown alongside encryption techniques. This conflict between the need to keep information private and the need to make it public is seen repeatedly in the past as a massive turning point in wars such as World War II and the famed Alan Turing and Enigma Machine. These will be looked at in more detail in later sections.

### History of Cryptography in Computer Science - Ruadhrí Ryan 14196115

### Important Figures in Cryptography - Benjamin Setterfield 19247125

### Modern Applications of Cryptography - Ian Rowland 19190859

### Summary

### References and Citation list - (Tom Section)

Damico, T. (2009) "A Brief History of Cryptography", *Inquiries Journal*, 1(11), p. Available at: <http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography> (Accessed: 28 April 2020).

*Origin of Cryptography - Tutorialspoint* (2020). Available at: <https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm> (Accessed: 28 April 2020).

*Traditional Ciphers - Tutorialspoint* (2020). Available at: <https://www.tutorialspoint.com/cryptography/traditional_ciphers.htm> (Accessed: 28 April 2020).

*History of cryptography* (2018). Available at: <https://en.wikipedia.org/wiki/History_of_cryptography> (Accessed: 28 April 2020).

*Telegraphy* (2020). Available at: <https://en.wikipedia.org/wiki/Telegraphy> (Accessed: 28 April 2020).

*Polybius* (2020). Available at: <https://en.wikipedia.org/wiki/Polybius#Cryptography> (Accessed: 28 April 2020).