# Cryptography Assignment - CS4182

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

Benjamin Setterfield 19247125

Ian Rowland 19190589

Ruadhrí Ryan 14196115

Tom Carey 19192363

### Origins of Cryptography - Tom Carey 19192363

Cryptography of a kind dates back to the very first time that man attempted to write, he would know what the scribbles meant but no one else would unless given the “key”, in this case being the ability to read. 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.

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*)

### References and list of Citations

#### 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).

#### *History of cryptography* (2018). Available at: https://en.wikipedia.org/wiki/History\_of\_cryptography (Accessed: 28 April 2020).