# Cryptography Assignment - CS4182

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

Benjamin Setterfield 19247125

Ian Rowland 19190589

Ruadhrí Ryan 14196115

Tom Carey 19192363

### Modern Applications of Cryptography - Ian Rowland 19190859

Cryptography plays an extremely important role in the use of technology in the modern day, as without it, devices and connections would not be secure, and users would not have any privacy in personal communications, or security from their information being accessed by outside sources, such as hackers. It is because of this, that cryptography is important for its use in password storage, data and cloud storage, and secure communications by means of end-to-end encryption.

Password storage,is perhaps, one of the most obvious uses of cryptography in modern devices, as it prevents people who don’t have the proper credentials to access information from doing so, if passwords are secured properly. Secure password storage is typically achieved through a method called ‘Hashing’. Hashing is a process where an input value of an arbitrary length is converted to an output of a fixed length by being put through a hash function(Kamal, 2017). Hash functions are, very importantly, known as one-way functions, which means “there is no way of deducing the input value by reverting from the output hash value ”(Kamal, 2017). Hashing is useful because of the fact that it is a one-way function, as it allows the relevant access credentials to be made available to a system in a secure manner, without being directly stored on that system.(Kamal, 2017).

Hashing is not without its vulnerabilities, however, as there are a few ways for attackers to circumvent it to gain access to a system. Among these are Exhaustive attacks, dictionary attacks, and Rainbow table attacks. With Exhaustive attacks, every possible combination of characters within a character set are used, until the correct password is obtained. As a result, it essentially has a success rate of 100% (Kamal, 2017).

Dictionary attacks involve hackers trying a series of phrases and words that are typically commonly used. Dictionary attacks have the potential to be either highly successful or unsuccessful, based on whether or not slight modifications are made to the aforementioned common phrases.(Kamal, 2017).

“*Rainbow table Attacks involve looking up the precomputed hash tables and the corresponding key value to find any matching hash*.”(Kamal, 2017). This type of attack can take less time to decrypt passwords than either exhaustive or dictionary attacks.

End to End encryption is another important application of cryptography. It refers to a method of transferring information between users, whereby only the users involved in the transmission have access to its information(Galushka, 2018).This means that even the service providers of a relevant communication system cannot access information sent between intended users(Isobe and Minematsu, 2018). End to end encryption is very useful for maintaining security and privacy between users, as well as maintaining the privacy of confidential information. It is mainly known to be used in messaging apps such as WhatsApp. An important note, however, is that end to end encryption essentially *“eliminates government surveillance and its ability to keep the country safe by intercepting terrorist communications.”*(Endelay, 2018). As a result, governments have sought to gain a ‘backdoor’ to such systems, like whatsapp, in the interest of national security. This, however, has been met with resistance, as it would result in a loss of privacy for users, which is the main benefit of end to end encryption, but it would also give hackers the means to access such systems for malignant purposes, which would ultimately defeat the purpose of end to end encryption(Endelay, 2018).