# 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, cloud data 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, 2019). 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, 2019). 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, 2019).

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, 2019).

Exhaustive attacks can exist in one of two ways: Known-plaintext only attacks, and Ciphertext-only attacks. With Known-plaintext only attacks, knows both the plaintext and the ciphertext, and may then attempt to figure out the key that is used to encrypt the plaintext(Kamal, 2019). With ciphertext-only attacks, a potential attacker will know the ciphertext, and will attempt to discern the appropriate plaintext, or the cryptographic key used, by attempting every possible combination of keys used.

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, 2019).

“*Rainbow table Attacks involve looking up the precomputed hash tables and the corresponding key value to find any matching hash*.”(Kamal, 2019). 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).

Another use of cryptography can be found in the encryption of e-mails. E-mails can be encrypted by means of Public Key Cryptography. This is a method of encryption that allows information sent through e-mail to be seen only by the sender and their intended recipients, and can be applied to the aforementioned End to End encryption, as any means of private online communication can make use of public key cryptography (Gurshaney, 2016). Public Key Cryptography can also be referred to as asymmetric encryption. This means that the appropriate cryptographic algorithm requires two separate, complementary cryptographic keys. The first key, used by the sender, is used to encrypt the information, while the recipient uses the second key to decrypt the information. This ensures that only the users involved in the transfer of information can actually view such information (Gurshaney, 2016).

Cloud data storage is another area in which cryptography has an important application. Cloud storage can be defined as a system where data is stored and maintained remotely, and is typically accessed through the internet(Stephen, 2014). It can also be used to back up data that is not exclusively stored remotely, such as photos on a phone, for restoration at a later point if that data were to be lost. Encryption is needed for cloud storage so as to ensure the security of stored data, so that only the person or people for the stored data is intended will be able to view it. (Stephen, 2014). Because encrypting all of the data that would be stored via cloud storage would be very expensive, data is often protected by means of access credentials such as passwords and identification/account numbers (Stephen, 2014). If data is very sensitive or confidential, however, actual encryption of the data itself may be used, and the data will be converted into ciphertext, which would contain the same information as the unencrypted data, “*but is not in a format readable by a human or computer without the proper mechanism to decrypt it”(Stephen, 2014).*

### References & Citations List:

Stephen, O .(2014). “*The Study of the Application of Data Encryption Techniques in Cloud Storage to Ensure Stored Data Integrity and Availability”*

Available at: <http://www.ijsrp.org/research-paper-1014/ijsrp-p3443.pdf> Accessed on: 28th April 2020

Gusharney, K. (2016) “ Email Encryption with Public Key Cryptography”

Available at: <http://sites.psu.edu/kaylagursahaneyportfolio/wp-content/uploads/sites/46465/2016/04/Technical-Definition.pdf> Accessed on 5th May 2020.

Isobe, T, and Minematsu, K (2018) “*Breaking message integrity of an end-to-end encryption scheme of line” Available at:* [*https://eprint.iacr.org/2018/668.pdf*](https://eprint.iacr.org/2018/668.pdf) *Accessed on : 28th April 2020.*

Endelay, R.E (2018) “*End-to-End Encryption in Messaging*

*Services and National Security—Case of*

*WhatsApp Messenger.”*

Available at: <https://doi.org/10.4236/jis.2018.91008> Accessed on: 28th April 2020.

Galushka, V. V. *et al* (2018) “*System of end-to-end symmetric database encryption*”

Available at: doi :10.1088/1742-6596/1015/4/042003 and <https://iopscience.iop.org/article/10.1088/1742-6596/1015/4/042003/pdf>

Accessed on 28th April 2020.

Kamal, P. (2019) “*Security of Password Hashing in Cloud”*

Available at: <https://doi.org/10.4236/jis.2019.102003> Accessed on: 28th April 2020.