Bogenberger, O., Cleary E., Crowley, T., Kocik, D., McMorrow, R. (2020) Report on Cryptography, University of Limerick, unpublished

**Abstract:**

**Introduction**

**Early History**

Caesar Cypher first actual use of cryptography to hide messages.

"Caesar used it in order to   
if there was occasion for secrecy, he wrote in cyphers; that is, he used the alphabet in such a manner, that not a single word could be made out. The way to decipher those epistles was to substitute the fourth for the first letter, as d for a, and so for the other letters respectively." The Twelve Caesars 56.Gaius Suetonius Tranquillus. Translator:Alexander Thomson

Due to the Power and enemies he had aquired in Rome Caesar needed a good way to keep his messages secret.The Caesar is of course a simple form of cryptography but as it was close to the first use of cryptography it didnt need to be too complex, and the caesar cypher was also suprisingly used in modern computing in the ROT13 method as a low security way of hiding information. this method was used more to protect the viewer from potentially offensive language or information.Another interesting adaption of the Caesar Cypehr in history was the Vigenère cipher.

Vignere cipher first use of encryption key

**Cryptography and early computing**

Hebern rotor machine.

Enigma.and Bombe machine.

**Early modern history**

Ibm crypto group and Lucifer(D.E.S. Data Encryption Standard)

1997 NIST encryption (Advanced Encryption standard).

**Cryptography and modern computing**

//also discuss key terms, mention cryptography and encryption were synonymous

//Terms to mention: key(randomness),

**Symmetric cryptography (Secret key?)**

The formal definition of symmetric encryption is “an algorithmic tool that allows a pair of parties to communicate secret information over open communication media that are accessible to eavesdroppers.” (Theory of Cryptography Conference Corporate 2010) This is a classic model of encryption, where the both parties share a secret key. The key is assumed to be random, single-purpose and not dependant on the message. The security is ensured by the fact that encryption and decryption happen in safe environments and the adversary cannot intercept the key.

**Introduction(explanation)**

**Stream cipher**

**Common attacks**

**Public key cryptography**

**Introduction**

**RSA**

**Common attacks**

**Hash functions**

**Introduction**

**Message Authentication**

**SHA1,2,3,**

**MD5**

**Common attacks**

**Crypto cracking**

**Other technologies that rely on cryptography**

**Blockchain**

**VPN**

A VPN or Virtual Private Network.

**Short note on future of cryptography(quantum)**

**Conclusion**

**List of references**

**Bibliography**

Canetti R., Tauman Kalai, Y., Varia, M., and Wich, D. (<https://link-springer-com.proxy.lib.ul.ie/book/10.1007%2F978-3-642-11799-2>)

Theory of Cryptography Conference Corporate, A. (2010) *Theory of Cryptography 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, Proceedings*,1st ed. 2010. ed., Berlin, Heidelberg:Springer Berlin Heidelberg.