Bogenberger, O., Cleary E., Crowley, T., Kocik, D., McMorrow, R. (2020) Report on Cryptography, University of Limerick, unpublished

Contents

**Abstract:**

**Introduction**

**Early History**

Caesar Cypher first actual use of cryptography to hide messages.

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).

**Symmetric cryptography (Secret key?)**

**Introduction(explanation)**

**Block cipher**

**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**

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

**Conclusion**

**List of references**

**Bibliography**