Bogenberger, O., Cleary E., Crowley, T., Kocik, D., McMorrow, R. (2020) Report on Cryptography, University of Limerick, unpublished

Contents

[Introduction 2](#_Toc39325053)

[Early History 2](#_Toc39325054)

[Cryptography and early computing 2](#_Toc39325055)

[Early modern history 2](#_Toc39325056)

[Cryptography and modern computing 2](#_Toc39325057)

[Symmetric cryptography (Secret key?) 2](#_Toc39325058)

[Introduction(explanation) 2](#_Toc39325059)

[Stream cipher 2](#_Toc39325060)

[Common attacks 2](#_Toc39325061)

[Public key cryptography 3](#_Toc39325062)

[Introduction 3](#_Toc39325063)

[RSA 3](#_Toc39325064)

[Common attacks 3](#_Toc39325065)

[Hash functions 3](#_Toc39325066)

[Introduction 3](#_Toc39325067)

[Message Authentication 3](#_Toc39325068)

[SHA1,2,3, 3](#_Toc39325069)

[MD5 3](#_Toc39325070)

[Common attacks 3](#_Toc39325071)

[Crypto cracking 3](#_Toc39325072)

[Other technologies that rely on cryptography 3](#_Toc39325073)

[Blockchain 3](#_Toc39325074)

[VPN 3](#_Toc39325075)

[Short note on future of cryptography(quantum) 3](#_Toc39325076)

[Conclusion 3](#_Toc39325077)

[List of references 3](#_Toc39325078)

[Bibliography 3](#_Toc39325079)

**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).

# 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

# 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.