Bogenberger, O., Cleary E., Crowley, T., Kocik, D., McMorrow, R. (2020) Report on Cryptography, University of Limerick, unpublished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

# Symmetric cryptography

## Introduction

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.

According to (Buchanan 2017, p.55), there are two main types of symmetric (a.k.a. “secret key”) encryption: stream cipher and block cipher. Buchanan also mentions that symmetric key decryption is faster than the asymmetric one with two keys, and so it is more suitable to use where data has to be transmitted in real-time e.g. secure voice communication online.

## Stream cipher

Stream encryption works on the basis of operating on a continuous data stream, where “the message is broken into successive bits or characters and then the string of characters is encrypted using a key stream” (Nandi *et al.* 1994). In order to create a ciphertext, a pseudorandom, pseudo-infinite key must be generated in binary form. This key is then XOR-ed with the plaintext (here the data stream) in binary form. (Buchanan 2017, p.58)

According to (Paar 2010) traditionally, modulo-2 addition performed by the XOR gates was used for stream encryption, since the key used by this form of encryption is random. This is because after XOR operation the resulting bit has 50% chances of being 1 and 50% chances of being 0, unlike if we were to use other gates (e.g. AND gate).

A popular example of a stream cipher encryption algorithm is RC4.

## 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(Paar 2010)

# 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)

Buchanan, W.J. (2017) *Cryptography*, Gistrup, Denmark ;:River Publishers.

Nandi, S., Kar, B.K. and Pal Chaudhuri, P. (1994) 'Theory and applications of cellular automata in cryptography', *IEEE Transactions on Computers*, 43(12), 1346-1357, available: <http://dx.doi.org/10.1109/12.338094>.

Paar, C. (2010) *Understanding Cryptography: A Textbook for Students and Practitioners*.

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.