Rachel Lowe 1301408

Is the future of cyptogarphy more secure?

Contents

[1 Introduction 1](#_Toc440116061)

[2 What is cryptography 2](#_Toc440116062)

[3 History 3](#_Toc440116063)

[3.1 Symmetric cryptography 3](#_Toc440116064)

[3.2 Public key cryptography. 4](#_Toc440116065)

[4 Quantum computers and quantum cryptography. 5](#_Toc440116066)

[4.1 Quantum cryptography 6](#_Toc440116067)

[5 Cryptography in cloud computing 6](#_Toc440116068)

[6 Future proposals of cryptography 6](#_Toc440116069)

[6.1 Multi-level cryptography 6](#_Toc440116070)

[6.2 Robust symmetric cryptography 7](#_Toc440116071)

[6.3 Overview of future proposals 8](#_Toc440116072)

[7 Conclusion 9](#_Toc440116073)

[8 Recommendations 9](#_Toc440116074)

# Introduction

This report is being written to give an informative view of cryptography and the security of its future.

Over the years cryptography has become very important in securing data, however what does the future mean for cryptography, will possible future inventions be dangerous for current cryptography and will future proposals.

This report will investigate the History of cryptography to develop an understanding of how secure it has been in the past which needs to be gained in order. Furthermore symmetric cryptography and Public Key Cryptography will be discussed as these are the start of cryptography in the computing world.

Quantum computers will be discussed as it is said that the they have a high computing speed which means they could be dangerous for Cryptography. Therefore, it would be appropriate to research any possible alternatives to the Cryptography existing presently.

This report aims to come to a conclusion as to whether cryptography is becoming more powerful and if there are dangers to cryptography in the future. In preparation to achieve this, the report will look at a brief history of cryptography, discussing how it has developed over the years. The report will be discussing how the future of cryptography is developing. It will mainly cover a type of cryptography called encryption. The report will discuss future proposals, what they are and how they can if and how they help the security of cryptography. The report is aimed at anyone who is interested in cryptography and would like to find out more about its future.

# What is cryptography

Cryptography is changing plan-text into what is called cipher text this is text that is not readable to the human eye this is because the data is scrambled the cryptography that this report will mainly focus on is called encryption, for the data to be read it would need to be decrypted.

Encryption is where data is changed into text that is unreadable to the human eye Icipertext () using a special code known as a key. Decryption is changing data back into plain text that is readable to the human eye using a type(type of key) and this means that the data was this proposed and this means allot of things and this means

# History

I

According to A-valid and Savala (2011) in the very early years cryptography was used only for confidentially of messages, the beginning of cryptography used pen and paper rather than using computers. Enigina was used by the Germans in the second would war and this was broken by the first enigma machine made by Allan turning. Now we have computers, cryptography is more concerned with the security of data, as attack against it can cause a lot of trouble,

## Symmetric cryptography

Symmetric cryptography was the first type of encryption known by the public(Al-Vahed , Sahhavi. (2011), this is where the sender and receiver both have the same key in order to encrypt and decrypt the file.

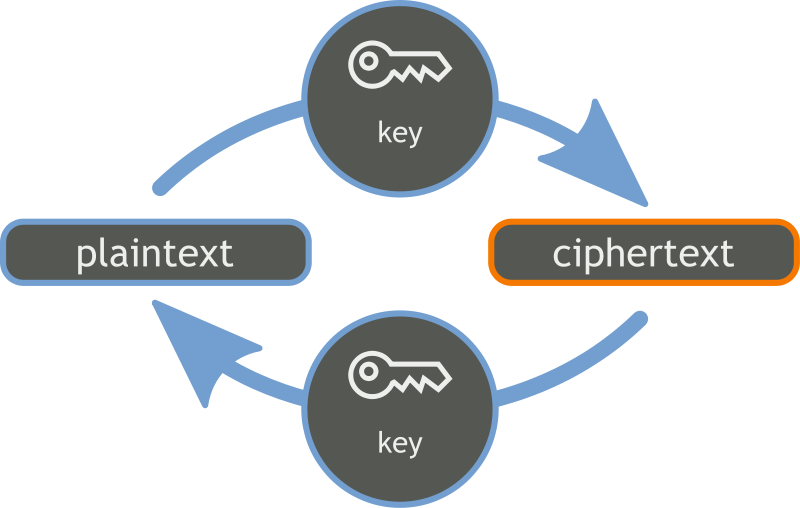


Figure 1 (Wikimedia author unknown )

As mentioned above figure one shows the plaintext is being encrypted with cyber key and then shows the plan text being encrypted that is shared between the two users involved sending the data and one reviver and then then the encrypted cipher-text and it being decrypted back into plain text by the key that is shared by two users.

## Public key cryptography.

After symmetric cryptography public key cryptography became invented, this is also called asymmetric cryptography. According to Whitfield(1998) this was invented because there were two problems found with symmetric cryptography. The first being that if people who had not met each other before needed to communicate they would need to agree on a secret key before this time. This does not seem possible with symmetric cryptography. The other problem, was that there needed to be a way a of knowing whether the message was in fact from the other person. With this type or cryptography there are two keys a private key and a public key these are both related. The public key is used to encrypt the data and the private key is used to decrypt the data changing it back into plain text. Anyone can access the public key and the private key is secret so only the person the data was intended for can access the file. The public key being available to anyone seems to solve the issue of two people who had not met each other needing to communicate without having agreeing on a secret key in advance as anyone would be able to encrypt the data. However from the information gathered the way it solves the issue of their needing to be a way of identifying whether the message was in fact from the other person is unclear.

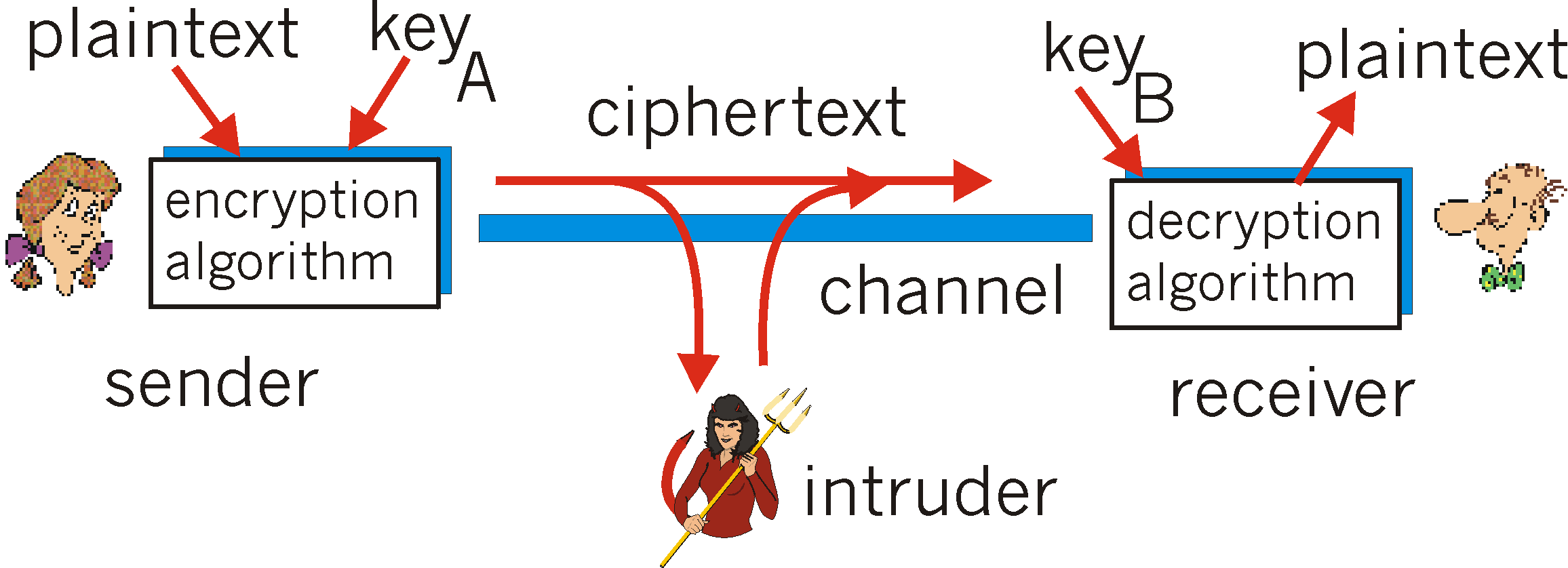


Figure 2 (<http://userpages.umbc.edu/> author unkown)

As mentioned above the figure 2 shows the person who sends the data with the plan text and the key which is privative and this says this reports and this is report has this means this plan text involves this means then the cipher text being sent to the receiver and then sent to the receiver and then being sent to the receiver then the receiver and this decrypting the cipher text , another thing encryption methods.

# Quantum computers and quantum cryptography.

Quantum computers have been talked about for many years, according to Zinger(2015) a few have been built however, the ones so far are quite small. Quantum computers could become dangerous to cryptography because of a high computer speed they can process big numbers in seconds meaning that they may be able to break the secret keys used in cryptography. This is a problem these days the reason for this is that a lot of personal information is being transferred over the internet therefore, if quantum computers ever become wide speed hackers would be able to access personal information considerably easier than they would with using this days computers. If this were to happen then a new method of cryptography would need to found, thus quantum cryptography is discussed below. And it seem

## Quantum cryptography

According to Besand(2005) The idea for quantum cryptography, using cryptography in Quantum computing started in the 1960’s. This was not actually proposed until 1984. However, this seems yet to exist, with this the sender creates a lot of random numbers and splits them up into bits and then transfers them to the receiver who lets the sender know the time they received these bits. According to lee(2015) quantum cryptography could be able to stop credit card hacks, this would suggest that this type of cryptography is more powerful than previous types of cryptography

# Cryptography in cloud computing

Cloud Computing has become increasingly popular over the years, this means that it needs to be made secure, according to. Naha and Ganesan (2014) this can be done with elective curve cryptography which is cryptography done with elective curves which are a set of points that make up an equation. Moreover, there is something called define key exchange, this is another type of public key cryptography. Naha and Ganesan (2014) propose improve the security of cloud computing, when a user wants to get data from a server the request is made into a file, and that file is then encrypted and sent to the server, the sever then decrypts the data and processes the information the user requires, that information is then encrypted again and sent back to the user.

This seems a good approach to improve the security of cloud computing for the information seems as it is uncertain to what is done with the information uploaded to cloud at the moment and this uncertainty can lead people wondering how secure the data that they upload to the cloud actually is.

# Future proposals of cryptography

## Multi-level cryptography

Following on from the earlier discussion of cryptography of in cloud computing a multi-level cryptography has been proposed, Dinesha and Agrawal (2014) proposed. This is three levels and three corresponding methods to secure data in this system. These three levels are called chief data officer, cryptography officer and data designer. The three ways that accompany these levels are data lock, data encryption and metadata. The roles of these levels are explained below:

* Chief data officer with data lock: this locks the data with appropriate information
* Cryptography officer and data encryption: the cryptography officer is in charge of data encryption and can chose the preferred encryption method available
* Data designer and metadata: the data designer is in control of data storage and ensures the data pattern of sensitive data is preserved.

In the first level the data designer turns the data into metadata. This data will then be processed and encrypted by the cryptography officer in the second level. In the third and final level the chief data officer locks data (Dinesha and Agrawal, 2014).

Decryption with this system is as follows, the data designer unlocks the data, this is then decrypted by the cryptography officer, finally the data designers converts the metadata back into its an original file.

This appears to be a more secure technique of cryptography than current methods as there are multiple levels making it more difficult for an attacker to intercept and cause harm, as they would need to go through more than one level to receive all the data. Additionally, it seems from this information that only three people are authorised to handle the encrypted data this gives the impression that it is more difficult for an attacker to gain access to the secret information.

## Robust symmetric cryptography

According to Chaudhuri et al (2015) with current encryption methods if a hacker gets hold of a key to decrypt the data then they have access to all data immediately. Therefore, Chaudhuri et al (2015) proposed a scheme where the encryption key will change in every session.

This schemeis started with a private key which is decided between the sender and the receiver along with the plain text, which is to be turned into one cipher text and one byte for the plain-text. The size of the text is categorised into in four bytes and sixty four bytes are created by the private key with this one hundred and twenty eight bits are created which is called session key1. This is then used by a block cipher technique known as Advanced Encryption Standard (AES) which is the most appropriate technique to use for this method. The session key1 is a version of the plain text itself (Chaudhuri et al, 2015).

During the second level another key is created which is called session key2**,** which is a form of cipher text. First, the session key1 is looked at as a group of sixteen bytes, each bite is counted in the session key1. Some bites might be zero, therefore some normalisation is used to escape an outcome of zero. In the next step what is found in session key1 is changed into ciphered text to form what is called session key2 (Chaudhuri et al, 2015).

A block cipher is an encryption method that turns input into groups of bytes that are fixed in size usually 16 bits (PC Mag, 2016). According to Search Security (2014) AES is a block cipher technique that is used by the US government. This standard identifies the Rhijnda algorithm which is a block chipper processes blocks of data that are one hundred and twenty eight bits using keys with sizes of one hundred and twenty eight, one hundred and ninety two, and two hundred and filthy six bits. (Fedel Information, 2001)

This technique seems to be more secure than present methods of cryptography, the reason for this is that the key is changing every session and will give hackers less chance of gaining access to the encrypted data.

## Overview of future proposals

It appears from the research that little has been found out about proposals of future types of cryptography as a process to the methods as discussed above. In consideration of the reason for this, it could be because it needs to be kept secret for security, as other methods of cryptography have been in the past. For example, symmetric cryptography and public key cryptography methods discussed in this report, both existed before they were known to the public. Alternatively, the reason may be that the research was not carried out thoroughly enough. Therefore, in this case it would be suitable to expand on research to gain more knowledge for this discussion.

# Conclusion

The aim of this research was to discover whether cryptography is more secure in the future than it has been in the past and is presently. A definitive answer has not a been achieved. While the multilevel cryptography and the robust symmetric cryptography suggest that cryptography could be more secure in the future, the high spend of quantum computing being able to break long integers could mean that the future of cryptography is in danger, although there is quantum cryptography appears to improve this situation it is uncertain of whether this has been released.

# Recommendations

Having thought over the research gathered in this investigation the following recommendations have be made:

* Introduce more types of cryptography
* Release quantum cryptography if this has not been archived.

**8.** Bibliography

Al-Vahed A, Sahhavi. H (2011). *An overview of Morden cryptography .* Available: [http://waprogramming.com/papers/50ae461463f880.93134133.pdf. Last accessed 21/11/2015](http://waprogramming.com/papers/50ae461463f880.93134133.pdf.%20Last%20accessed%2021/11/2015).

Bennart, C. H., & Brassard, G. (2014). Theoretical Computer science. (university  of montreal, Ed.) Montreal,, QC, Canada. accessed on 15/10/15  available from <http://ac.els-cdn.com/S0304397514004241/1-s2.0-S0304397514004241-main.pdf?_tid=61e44a0>

Chaudhuri et al . (2015). *Robust symmetric cryptography using plain-text variant session key .* Available: [http://www.inderscienceonline.com/doi/pdf/10.1504/IJESDF.2015.067990. Last accessed 09/01/2016](http://www.inderscienceonline.com/doi/pdf/10.1504/IJESDF.2015.067990.%20Last%20accessed%2009/01/2016).

Deral Information . (2001). *Announcing the ADVANCED ENCRYPTION STANDARD (AES.* Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Last accessed 9/01/16.

Dinesha H A and 2 Agrawal V K. (2014). *Multilevel Cryptography with Metadata and Lock Approach for Storing Data in Cloud.* Available: [http://scholarpublishing.org/index.php/TNC/article/view/591/403. Last accessed 09/01/2016](http://scholarpublishing.org/index.php/TNC/article/view/591/403.%20Last%20accessed%2009/01/2016).

Federal Information . (2001). *Announcing the ADVANCED ENCRYPTION STANDARD (AES.* Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Last accessed 09/01/2016.

Gilles Brassard. (2005). *Brief History of Quantum Cryptography: A Personal Perspective.* Available: http://arxiv.org/pdf/quant-ph/0604072.pdf Gilles Brassard. Last accessed 11/01/2016.

ImperialViolet . (2010). *Elliptic curves and their implementation.*Available: https://www.imperialviolet.org/2010/12/04/ecc.html. Last accessed 18/11/2015.

Neha t , Ganesan R. (2014). *Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography.* Available: https://eprint.iacr.org/2014/049.pdf. Last accessed 09/01/2016.

PC mag. (2016). *Definition of: block cipher.* Available: http://www.pcmag.com/encyclopedia/term/38763/block-cipher. Last accessed 09/01/2016.

searchsecurity. (2014). *Advanced Encryption Standard (AES) definition.*Available: http://www.neilstoolbox.com/bibliography-creator/reference-website.htm#. Last accessed 09/01/2016.

tech times . (2015). *Quantum Cryptography May Make Future Credit Cards Hack-Proof.* Available: [http://www.techtimes.com/articles/22352/20141218/quantum-cryptography-may-make-future-credit-cards-hack-proof.htm. Last accessed 09/01/2016](http://www.techtimes.com/articles/22352/20141218/quantum-cryptography-may-make-future-credit-cards-hack-proof.htm.%20Last%20accessed%2009/01/2016).

Whitfield D . (1988). *The First Ten Years of Public-Key Cryptography .*Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4442. Last accessed 11/01/2016.

Ziegler L. (2015). *Online security, cryptography, and quantum computing.* Available: http://digitalcommons.csbsju.edu/cgi/viewcontent.cgi?article=1118&context=forum\_lectures. Last accessed 18/11/2015.