

Sri Lanka Institute of Information Technology

**Cryptography**

**Individual Assignment**

IE2022 - Introduction to Cyber Security

Submitted by:

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT19991290 | 1. D. Jaliya |

Date of submission

**Table of Contents**

[Abstract 4](#_Toc38443029)

[1. Introduction 5](#_Toc38443030)

[2. Evolution of the topic 6](#_Toc38443031)

[3. Future developments in the area 7](#_Toc38443032)

[4. Conclusion 8](#_Toc38443033)

[5. References 9](#_Toc38443034)

# Abstract

The science of hiding information and data in plain sight, in order to conceal it from unauthorized access is the cryptography. It is a technique of transmitting data in a particular form so that only those whom it is intended can read and processed it.

Confidentiality, integrity, authentication, and irrevocability are the four main objectives of the cryptography. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information, storage, or transit. But nowadays cryptography is most often associated with scrambling plaintext, into ciphertext, then back again. Attackers can bypass cryptography and hack into computers that are responsible for data encryption and data decryption, and exploit deep implementations such as the use of default keys. Cryptographers should make it harder for attackers to access information protected by encryption algorithms.

Cryptographic techniques have been used for secure communication for thousands of years. Military communication has had the greatest influence on encryption throughout history. With the beginning of the information age, the need for secure private and commercial communication has been led with the invention of the world wide web, this new method of information exchange has caused a tremendous need for information security. The knowledge about cryptography and encryption will help people develop better ways to protect valuable information as technology becomes more efficient and faster.

Based on the needs, various cryptographic methods such as public-key cryptography, or symmetric key cryptography can be used during the storage and transmission of data. Biotechnology, financial services, health care, and media companies are the major sectors that widely using cryptography.

Cryptography is a solution to many of the security challenges that are present on the internet. This technology helps to solve most of the problems. Cryptography also can be used to harm society. Governments are concerned that encryption will make law enforcement global security goals more difficult to achieve. For example, terrorists could communicate information over the internet using encryption that law enforcement agencies could not decrypt.

# Introduction

When transferring data over a network or storing data in storage devices we must consider about security of data. Especially in data transit that data can be disclosed to unauthorized individuals or data can be modified by unauthorized users. To prevent that, most secure communication protocol use cryptography as part of its implementation to encrypt the message and send, only the authorized receiver can decrypt it. The word cryptography is originated from the ancient Greek word kryptos, which means “secret or hidden,” and graphein which means “to write.”

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

In the past cryptography was effectively synonymous with encryption. But in modern days cryptography is mainly based on mathematical theory and the practice of computer science. In modern-day computer science, cryptography alludes to secure information and correspondence methods got from numerical ideas and a lot of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. Cryptographic key generation, web browsing on the internet, verification to protect data privacy, digital signing, and confidential communications such as credit card transactions and email are the use of these algorithms.

Cryptography is mainly used for the implementation of technical security controls of digital devices that we use, and the protection of data transmitted over the network and stored in storage devices. Most of the secure communication protocol depends on the cryptographic mechanism to provide security services like confidentiality, integrity, authenticity, and non-repudiation.

Integrity is used to make sure that nobody in between the sender and receiver. Only the sender, an intended receiver should understand the shared content. Therefore a hash is calculated and added. By using hashing algorithms such as MD5, SHA(1,2), etc. HMACs are used to prevent unauthorized modification. This stands for the hashed message authentication code.

Confidentiality is used to make sure that nobody between the sender and receiver is able to read what data or information is sent between the sites. There are two types of algorithms are used to achieve encryption. Symmetric algorithms and asymmetric algorithms. Symmetric encryption algorithms use the same key to encrypt and decrypt. Asymmetric algorithms use two kinds of keys called a private key and public key. A public key is used to encrypt data and those data can only be decrypted with a private key. Symmetric encryption use algorithms like DES, 3DES, or AES.

Authenticity is used to make sure that the message is not a forgery and that makes sure that the message comes from whom it sent. Different kinds of techniques can be used such as configured pre-shared keys from both sides to achieve authenticity.

Encryption and Decryption algorithms are referred to as a cipher. Encryption means hiding some data. The ciphertext is unreadable and when plaintext is encrypted it becomes ciphertext. Cipher is a method o hiding word or text with encryption by replacing original letters with other letters, numbers, and symbols through substitution or transportation. When encrypting and decrypting messages cipher is used as well-defined steps that can be followed as a procedure. Transposition, substitution, and one-time pad are some of the methods of creating cipher.

In transposition ciphers, no letters are replaced and only the plaintext is systematically rearranged into another sequence. Spell plaintext backward is an example of transposition cipher. Mainly depending on the key substituting any character from the given fixed set of characters to some other character from the same set call substitution cipher. Caesar Cipher and Vigenere Cipher are examples of substitution cipher.

The one-time pad was invented in 1917 by Gilbert Vernam who was AT&T Bell labs engineer. It is a subset of vernam cipher and it was implemented using a random set of non-repeating characters as input ciphertext. In a one-time pad, original plain text length must be equal to the length of input ciphertext. Input ciphertext was used only in one time and it is never used again for any other message. Therefore it was called a one-time pad. In a one-time pad, there is a unique private key. And this onetime use private key is used to encrypt the message. Only the receiver who has a private key can decrypt the message and access to the data. Information encrypted with the one-time pad is impossible to break because in a one-time pad the encryption is unique and there is no any relation with other encryptions.

Cracking code is getting access to encrypted information without a key or password. There are various methods to crack codes. The brute-Force method, Ciphertext-Only method, Known-Plaintext method, Chosen-Plaintext method, Chosen-Ciphertext method, Meet-in-the-Middle method are some of them.

Cryptography is the science of hiding data and information in plain sight in order to protect it from unauthorized entry. It is a technique of distributing data in a special form such that it can be read and interpreted only by those it is intended for.

The four primary objectives of cryptography are secrecy, honesty, authentication and irrevocability. Techniques such as microdots, combining words with pictures, and other ways to conceal information, storage or transit are used in cryptography. But now cryptography for a few days is more commonly concerned with plaintext scrambling, in ciphertext, then back again. Attackers can circumvent and exploit authentication on machines responsible for data encryption and decryption of data and take advantage of deep implementations, such as the use of default keys. Cryptographers can make it more difficult for hackers to access data secured by encryption algorithms.

For thousands of years, cryptographic methods have been used for reliable correspondence. Throughout history, military contact has had the greatest effect on cryptography. With the invention of the world wide web, the need for safe private and commercial communication was led with the advent of the information era, this modern way of sharing of information has caused a huge need for information security. As technology becomes more powerful and quicker, understanding of cryptography and encryption can help people learn safer ways to safeguard valuable information.

Different cryptographic techniques may be used during data storage and transfer, such as public key cryptography or symmetric key cryptography, depending on the specifications. The main industries that commonly use cryptography include biotechnology, financial services , health care and media businesses.

# Evolution of the topic

The word cryptography is originated from the Greek Krypto and graphein, which mean hide and writing. The technique of cryptography was born parallel with the art of writing. With the evolution of civilizations, human beings got organized into groups, tribes, and kingdoms. This led to the emergence of ideas such as battles power and supremacy. These thoughts further changed the natural need of people to communicate secretly with the specific recipient which in turn ensured the continuous evolution of cryptography too.

In ancient times, as the majority of people could not read the first type of cryptography was simply writing. Later with the development of knowledge and skills, most of the great civilizations started to use some special kind of cryptography to transfer some important private information.

A big evolution of cryptography has come with the recording of the first cryptographic key in the 1600s. It caused a big shift in the space, moving the importance of hiding the system to hiding the key. In that situation, the information could be public, but one could still not read the information in the message without the key.

‘Hieroglyph’ is the first known evidence of cryptography. Egyptians used this technique in order to communicate with a message written in ‘hieroglyph’. This technique was used by ancient kings to transmit messages. A system of pictorial writing was used in this method. The symbols in the hieroglyph may represent the objects that they depict but usually, stand for particular sounds or groups of sounds. The simple meaning of hieroglyph is” sacred carving”. It is a Greek translation of the Egyptian phrase “the god’s words”, which was used at the time of the early Greek contacts with Egypt to distinguish the older hieroglyph from the handwriting of the day.

A simple monoalphabetic substitution was used from 500 to 600 BC. Replacing the alphabets of a message with other alphabets according to some secret rule is the technique used in This cryptography method. This secret rule is the key to retrieve the message back from the garbled message.

Scytale is a cryptography method used for secret communication between military commanders. There is a tapered bottom, around which was spirally wrapped a strip of parchment or leather on which the message was written with the scytale.

Caesar shift Cipher is the earlier Roman method of cryptography developed around 100BC. This was used by Julius Caesar to send private and secret messages to his generals in the field. Shifting the letters of a message by an agreed number is the technique used in this method. Here the recipient of the message would then shift the letters back by the same number in order to retrieve the original message. This cipher can be easily broken by ciphertext only scenario.

Multiplicative ciphers, Affine ciphers, and Vigenere ciphers are also examples of symmetric encryptions. Vigenere cipher is the most complex cipher as it uses a table of alphabet laid across the top row and the column. The vigenere cipher was created in the 16th century. A special element called “secret key” was found in this cipher. Cipher has the disadvantage of being easily broken by the frequency of letters

Steganography also another method of cryptography used by ancient civilizations. This method added another dimension to cryptography. In this method, the sender wants to protect the secrecy of information by concealing it as well as the sender wants to make sure that any unauthorized person gets no evidence that the information even exists. They used to apply techniques like invisible watermarking for that purpose.

In the 15th century, improved coding systems such as vigenere coding came into existence. Moving letters in the message with a number of variable places instead of moving them the same number 0f places was the technique used in this method.

Jefferson’s Encryption Device was invented by Thomas Jefferson in the year 1790. This machine has comprised of 36 wheels orchestrated around a pivot with an alternate irregular letter set imprinted outwardly of each wheel.Each wheel contains a different substitution alphabet, unlike using the same wheel 36 times. This device is usually called multiplex cipher because the wheels are arranged simultaneously instead of serially. The sender of a cipher message would arrange her disks in the agreed-upon order and then simply spin each disk to spell out the first 36 letters of the message to use this machine. At that point the recipient of the message would mastermind his code wheels as indicated by the recommended 0rder and afterward explain the message across one level line.

The first use of a rotor for encryption was recorded during the 19th century. In the early 20th century the invention of electromechanical and mechanical machines provided more advanced and efficient means of coding information.

Enigma rotor machine is one such example for this kind of machine. It was invented in 2003 by Arthur Scherbius. This machine has an electromechanical rotor instrument that scrambles the 26 letters of the letter set. When using this machine one person enters texts on the keyboard of the machine and another person writes down which of 26 lights above the keyboard lights up at each keypress. Enigma requires a list of daily key settings and auxiliary documents in its use.

Code talker is the name given to American Indians who utilized their own ancestral language to send private and mystery messages. They for the most part utilize this language on front lines. Code talkers were appointed two by two to a military unit. When utilizing this language, one individual would work the compact radio and the subsequent individual would get messages in the local language and make an interpretation of them in to English.

One time pad ciphers is an encryption technique that can not be cracked. The utilization of one-time pre-shared key a similar size as, or longer than, the message being sent is required. This technique was introduced first by the Frank Miller in 1882. This is the optimum cryptosystem with theoretically perfect secrecy.

Cryptography found its way in to commercial applications, with IBM being the first company to develop a crypto-group systematically and what ended up being the first U.S. standard for encryption. This technique also short-lived and it was also broken by a very powerful method called a brute-force attack. This leads to increases in the complexity of the private keys. Both cryptography and cryptanalysis became excessively mathematical during the period of world war II. Then government organizations, military units, and other organizations started adopting the applications of cryptography.

With the development of cryptography, unauthorized users want to decrypt those encrypt data and get access to that secret information that they can not access. Because of that, they develop various cracking code methods to achieve their target. Such as Brute-Force Method, Ciphertext-Only Method, Known-Plaintext Method, Chosen-Plaintext Method, Chosen-Ciphertext Method, Meet-in-the-Middle Method.

In chosen plaintext attacks the cryptanalyst takes the plaintext into the the device and so watches as it happens. It will be encrypted with plaintext.This tactic was used by the Allies in WWII. Sending fake Allied Troop Signals Movements. The attacker would also attempt to feed a scheduled attacker, Series of messages to show the Most of the manner in which the information is used and encryption.

I n known plaintext attack, there is both the ciphertext and the plaintext for the attacker. The attacker acknowledges the algorithm used for encryption. This is complicated since there are so many keys, but the details in plaintext can make it easier to experiment than in the previous case.

Differential power analysis is one of another attack which is attack on smart cards. A DPA attack analyzes the power output from a processor performing an en cryption algorithm in order to get information about the key being used by that algorithm.

# Future developments in the area

Cryptography is an essential part of today’s information systems from e-mail to cellular communication and from secure web access to digital cash. Cryptography helps to provide fairness, confidentiality, accountability, and accuracy. It always prevents fraud in electronic commerce and assures the validity of financial transactions. It can prove your identity and protect your anonymity. It can prevent industrial competitors from reading your confidential documents and it can keep vandals from altering your web page. Because of commerce and communications continue to move to computer networks, cryptography will become more and more vital in the future.

But the cryptography methods in the market do not provide the level of security it advertises. Most systems are designed by engineers who think cryptography is like any other computer technology instead of cryptographers. Cryptographic systems can not develop by security by tacking on cryptography as an afterthought. You have to well aware of what you are doing every step of the way, from conception through installation. In the computer security sections, billions of dollars are spent, and most of it is wasted on insecure products. At the end of the week, cryptography looks the same on the shelf as strong cryptography. Two e-mail encryption products may have almost the same user interface, from these two one is secure while the other permits eavesdropping. A comparison chart may suggest that two programs have the same features, but one has gaping security holes while the other has no such security holes. But an experienced cryptographer can identify the difference.

Some people break cryptographic systems and they do not follow cryptographic rules, they cheat. They attack a system by using techniques the designers never thought of. Art thieves have burgled the homes by cutting through the by using the chain saw. Home security systems are no matter how sophisticated and expensive and will not stand a chance against this attack. Computer thieves are also coming through walls. They bribe insiders, modify software, steal private and personal data, and collude. To prevent such conditions, the defenders have to protect all the data and information against every possible vulnerability, but the attacker only has to find a single security flaw to compromise the whole system.

Nowadays computer security is a house of cards; it may stand for now, but it can’t last. As many insecure products are still in their infancy, they have not been broken. But when these products are widely used, they will convert into targets for criminals. The press will publicize the attacks, by undermining public confidence in these systems. Ultimately, depending on the strength of their security the products will win or lose in the marketplace.

No one can guarantee 100% 0f security. But we can work towards 100% risk acceptance. Fraud exists in current commerce systems: cash can be counterfeited, checks altered and credit card numbers stolen. Yet these systems are still successful because the conveniences and benefits outweigh the losses. A good cryptographic system always strikes the balance between what is possible and what is acceptable.

The good news about cryptography is that we already have the protocols and algorithms we need to secure our systems. The bad news is that was the easy part; it requires considerable expertise in implementing the protocols. The areas of security that interact with people – human/ computer interface security, key management, access control-often defy analysis. And the disciplines of public key infrastructure, tamper-resistant hardware design, software security and computer security, are very poorly understood.

Over the last two decades field of cryptography has seen several trends, including the decryption capabilities to a person’s attributes; efficiency gains in areas such as secure multi-party computation, which allows multiple parties to interact on confidential data sets; new solution for homomorphic encryption using lattice-based cryptography; and, now, threat and promise of quantum computers pushing the field to develop post-quantum cryptographic techniques.

Many industrial labs, researchers, and governments are actively working on developing a quantum computer that can handle large-scale computation, such as the workstation Q. While classical computers, tablets, phones, laptops, servers, and so on store and process information in the form of bits., quantum computers process quantum bits, a two-state quantum-mechanical system, called qubits.

Small scale quantum computers already exist, and already estimate vary as to how many years it will take before engineers and researchers succeed in building a quantum computer that can handle computations involving thousands of qubits. However, when that day does inevitably come, the consequences for the world’s security infrastructure and e-commerce will be enormous.

In 2017, the national institute of standards and technology in the U.S. launched an international-multi-year post-quantum cryptography competition to select the most appropriate cryptographic systems for the future. A post-quantum cryptosystem is one that is not known to be breakable. There are five main proposals for post-quantum systems. they were invented by using hard math problems, each of which has been studied for a decade or more.

Code-based systems based on the difficulty of decoding random linear codes, multivariate cryptosystems based on the difficulty of solving systems of many non-linear equations in many variables, lattice-based systems based on the hardness of finding short vectors in lattices, systems based on Merkle-hash trees supersingular isogeny graph systems that are based on the difficulty of finding paths between two points in a large, seemingly random, graph are those cryptosystems that mentioned earlier.

One of the advantages of lattice-based cryptosystems is that they can build systems that they can build that privately and securely handle computation on encrypted data. Homomorphic encryption may seem esoteric, but it just means encryption which users can compute on. But standard cryptosystems at present do not have this property: if you try to add together two ciphertexts. Encrypted using the advanced encryption standard, then the result will be gibberish. This encryption type differentiates itself by preserving the structure of data. It encodes data in a mathematical object and then encrypts it in a way that does not affect the contained data and information.

Cryptographic structures are also based on the assumption that, computationally, such math problems are very difficult to overcome. Mathematicians have researched many of these questions, such as the factoring of some types of large numbers, from decades to decades. In reality, the predicted protection of such structures is also calculated by mathematicians by plotting the progression of the best-known attacks in 'running time.' This forecasts perform well, but only in the absence of substantial disruptions; new algorithms or innovations are dramatically increasing the attacks' predicted runtime.

Many academics, industrial labs, and governments are currently working on the creation of a quantum computer that can accommodate large-scale computation, such as the work at Station Q. Whereas classical computers store and process data in the form of bits (strings of zeros and ones), quantum computers process quantum bits, a two-state quantum mechanics

A qubit will hold a value of one and zero simultaneously, relative to a 'regular' bit. The theoretical benefit of this is that each qubit will also concurrently execute copious operations, drastically shortening calculation times and allowing considerably more complex processes to be measured.

In 2017, an international multi-year Post-Quantum Cryptography (PQC) competition was initiated by the National Institute of Standards and Technology ( NIST) in the United States to pick future cryptographic systems. A post-quantum cryptosystem is one that is not understood by a full-scale quantum computer to be breakable in polynomial time.

The use of quantum mechanical effects to perform cryptographic tasks or to crack cryptographic structures is represented in Quantum Cryptography. The value of quantum cryptography is that using classical correspondence alone makes the completion of different cryptographic activities that are proved or conjectured to be difficult. Quantum mechanics, for instance, means that the calculation of quantum data disturbs the data. This can be used in quantum key key eavesdropping to detect split. delivery.

Digital signatures can be permanently connected to the substance of the signed message. Then they will not be moved from one text to another, so any effort would be observable. Two of the most common digital signature systems are RSA and DSA. There are two algorithms in digital signature schemes: one for signing, where a hidden key is used to process the message, and one for verification, where the matching public key is used to validate the signature authenticity of the message.

# Conclusion

In this document, we provide a review of the purposes of cryptography, the evolution of the cryptography in the recent past to extent of it today, and the future development of the cryptography. Cryptography started with a list of challenges for protecting data, information, continues with the presentation of the basic cryptographic algorithms and protocols. From a technical point of view, cryptography is the most important solution for many of the security challenges that are present on the internet. So it is clear that the technology of cryptography exists to solve most of the problems. But there are several issues that have obstructed the widespread use of cryptography on the internet. Cryptography faces a difficult problem as a science. Most of the algorithms used in cryptography can not be proven secure. For that reason, there is suspicion around many of the algorithms used in cryptography. The next aspect is related to the intellectual property associated with the cryptographic algorithms. Most of the cryptographic algorithms are patented, and only very few companies and institutes have licensed them for use.

Finally, cryptography can be used as a harmful technique to society. Governments are concerned that encryptions used in cryptography will make law enforcement and national security goals more difficult to achieve. For example, terrorists could communicate data and information over the internet using encryption that law enforcement agencies could not decrypt.

However, the current trend in society indicates that cryptography is gaining importance. In the future, cryptography may be widely used throughout the internet: for electronic mail, for sending electronic mail, for sending documents that are sold over the web, and even perhaps for all network communication between switches and routers on the internet. Modern algorithms in cryptography are very complex to be executed by humans. So those algorithms are executed by computers or specialized hardware. The design of a secure system using techniques of encryption is focused mainly on the protection of keys. Keys can be protected by encrypting them under other keys or by protecting them physically, while the algorithm used to encrypt the data is made public and subjected to intense security. When cryptographers hit on an accurate method of encryption, they can patent it as intellectual property and earn royalties when their method is used in commercial products and by commercial institutes. In the current open environment, many accurate and affective cryptographic algorithms are available in major bookstores, libraries, and the internet, or patent office.

# References

* DATA COMMUNICATIONS AND NETWORKING ,Chapter 30, cryptography by BEHROUZ A. FOROUZAN
* Definition of ‘Cryptography”: The Economic Times. <https://economictimes.indiatimes.com/definition/cryptography>
* StackExchange: <https://security.stackexchange.com/questions/148173/authenticity-confidentiality-integrity-general-questions>
* Tutorialspoint, Trasposition Cipher : <https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_transposition_cipher.htm>
* Cryptography article by AmiMunshi, GeeksforGeeks: <https://www.geeksforgeeks.org/substitution-cipher/>
* Origin of cryptography, Learn Cryptography : [https://www.tutorialspoint.com/cryptography/origin\_of\_cryptography.htm#:~:text=Evolution%20of%20Cryptography,-It%20is%20during&text=Only%20after%20the%2019th,and%20science%20of%20information%20security.&text=During%20the%20period%20of%20World,and%20cryptanalysis%20became%20excessively%20mathematical](https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm" \l ":~:text=Evolution of Cryptography,-It is during&text=Only after the 19th,and science of information security.&text=During the period of World,and cryptanalysis became excessively mathematical)
* The evolution of cryptography by Nikolas Molyndris (3 DEC 2018) : <https://blog.decentriq.ch/evolution-of-cryptography/>
* Summery of cryptography by Rich Aliano : <https://condor.depaul.edu/elliott/513/projects-archive/DS420Winter99/tchaikovsky/conclusion.htm>.
* Cryptography, at a fundamental level, is the science of keeping secrets by Kristin Lauter, 4 September : https://qeprize.org/news/the-future-of-cryptography/