International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 5 Issue 1, January - 2021, Pages: 24-26

Cryptographic Protection of Information

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *The term "cryptography" originally meant "to hide, to conceal a record." It was first mentioned at the time of writing. Today, cryptography refers to the concealment of information in any form, such as numbers stored on disk or in the form of messages transmitted over computer networks. Cryptography can be applied to any information that can be encoded with numbers. Privacy cryptography has a wider range of applications. Specifically, the methods used in cryptography can be used in many processes related to the protection of information. Cryptography protects information from unauthorized access and ensures its confidentiality. For example:*

Keywords: Cryptography, History of cryptography, communication theory, encryption key, symmetric encryption algorithm, asymmetric encryption algorithm.

INTRODUCTION

1. The concept of cryptography.

2. Aims and objectives of cryptography.

3. History of the development of cryptography. Modern cryptography

4. Principles of cryptographic protection of information.

The term "cryptography" originally meant "to hide, to conceal a record." It was first mentioned at the time of writing. Today, cryptography refers to the concealment of information in any form, such as numbers stored on disk or in the form of messages transmitted over computer networks. Cryptography can be applied to any information that can be encoded with numbers. Privacy cryptography has a wider range of applications. Specifically, the methods used in cryptography can be used in many processes related to the protection of information. Cryptography protects information from unauthorized access and ensures its confidentiality. For example, when sending payment slips by e-mail, it can be changed or fake entries can be added. In such cases, it is necessary to ensure the integrity of the information. In general, unauthorized access to a computer network cannot be completely prevented, but it can be detected. This process of verifying the integrity of information is often referred to as ensuring the authenticity of the information. The techniques used in cryptography can ensure the authenticity of information with a small amount of modification.

METHODS

It is important not only to know that the information came from the computer network without distorting its meaning, but also to make sure that it came from the author. There are various ways to verify the authenticity of the transmitters. The most common procedure is to exchange passwords, but this is not a very efficient procedure. Because anyone who has a password can access the information. If precautions are taken, it is possible to increase the efficiency of passwords and protect them with cryptographic methods, but cryptography also provides procedures that allow more powerful passwords to be changed continuously. One of the latest advances in cryptography - digital signatures - is a method of ensuring the integrity of information by filling it with a special property, in which the information is provided by its author.

can only be verified when the public key is known. This method has many advantages over certain methods of integrity checking using a secret key. Let's look at some of the uses of cryptography. Two modifications are used to hide the meaning of the information being transmitted: encoding and encryption. Coding uses books or tables that contain a set of frequently used phrases. Each of these phrases is, in most cases, a randomly selected code word with a set of numbers. A similar book or table is required to encode the information. An encoding book or table is an example of an optional cryptographic change. Information technology

requirements for coding - the ability to convert string data into numeric data and vice versa. Encoding can be done on fast and external storage devices, but such a fast and reliable cryptographic system is not successful. If this book is used without permission, it will be necessary to create a new code book and distribute it to all users. The second type of cryptographic conversion involves encryption - algorithms that convert the original text into a form that cannot be understood. This type of change is compatible with information and communication technologies. Here the protection of the algorithm is important. Using a cryptographic key can reduce the security requirements of the encryption algorithm itself. Now only the key serves as the object of protection. If it is copied from a key, it is called cryptology. The word comes from the Greek words "crypto" - mysterious and "logus" - meaning message. Cryptology is divided into two areas: cryptography and cryptanalysis. The purpose of cryptography is to ensure the confidentiality and authenticity of messages. The task of cryptanalysis is to unlock the protection system developed by cryptographers. Currently, cryptosystems can be divided into two classes: • symmetric single key (secret key); • Asymmetric two-key (open-key). Symmetric systems have two problems: 1) How can participants in the exchange of information pass the secret key to each other? 2) How to determine the authenticity of the message sent? The solution to these problems is found in public key systems. In a public key asymmetric system, two keys are used. One cannot be determined by the other.

The first key is used by the sender to encrypt the information, while the second is used by the recipient to retrieve the information and must be kept confidential.

Figure 5.1. General scheme of data encryption and decryption This method can ensure the confidentiality of information. If the first key is secret, then it can be used as an electronic signature, and in this way it is possible to authenticate the information, that is, to ensure the integrity of the information. In addition to information authentication, the following issues can be addressed: • user authentication, ie identification of the user who wants to access the resources of the computer system: • mutual authentication of network subscribers during the communication process. One of the areas that needs to be protected today is e-commerce through e-payment systems and the Internet. Principles of cryptographic protection of information Cryptography is a set of methods of data modification aimed at solving two main problems of data protection: confidentiality; integrity. While privacy is understood as hiding information from malicious individuals, integrity means that information cannot be altered by malicious individuals.

This cryptographic system can be schematically described as follows:

Figure 5.2. Schematic representation of a symmetric cryptographic system

Here the key is sent through some protected channel (represented by dotted lines in the drawing). In general, this mechanism applies to a symmetrical key system. An asymmetric two-key cryptographic system can be schematically described as follows:

Figure 5.3. Schematic representation of an asymmetric cryptographic system In this case, the public key is sent over the protected channel and the secret key is not sent. If malicious individuals fail to achieve their goals and cryptanalysts cannot recover encrypted information without knowing the key, then the cryptosystem is said to be a cryptographic system. The strength of a cryptosystem is determined by its key, which is one of the basic rules of cryptanalysis. The basic premise of this definition is that a cryptosystem is a well-known system that requires a lot of time and money to change, so it is only necessary to protect the information by changing the key.

RESULTS

• symmetric single key (secret key); • Asymmetric two-key (open-key). Symmetric systems have two problems: 1) How can participants in the exchange of information pass the secret key to each other? 2) How to determine the authenticity of the message sent? The solution to these problems is found in public key systems. In a public key asymmetric system, two keys are used. One cannot be determined by the other.

The first key is used by the sender to encrypt the information, while the second is used by the recipient to retrieve the information and must be kept confidential.

Figure 5.1. General scheme of data encryption and decryption This method can ensure the confidentiality of information. If the first key is secret, then it can be used as an electronic signature, and in this way it is possible to authenticate the information, that is, to ensure the integrity of the information. In addition to information authentication, the following issues can be addressed: • user authentication, ie identification of the user who wants to access the resources of the computer system: • mutual authentication of network subscribers during the communication process. One of the areas that needs to be protected today is e-commerce through e-payment systems and the Internet. Principles of cryptographic protection of information Cryptography is a set of methods of data

modification aimed at solving two main problems of data protection: confidentiality; integrity. While privacy is understood as hiding information from malicious individuals, integrity means that information cannot be altered by malicious individuals.

This cryptographic system can be schematically described as follows:

Figure 5.2. Schematic representation of a symmetric cryptographic system

Here the key is sent through some protected channel (represented by dotted lines in the drawing). In general, this mechanism applies to a symmetrical key system. An asymmetric two-key cryptographic system can be schematically described as follows:

Figure 5.3. Schematic representation of an asymmetric cryptographic system In this case, the public key is sent over the protected channel and the secret key is not sent. If malicious individuals fail to achieve their goals and cryptanalysts cannot recover encrypted information without knowing the key, then the cryptosystem is said to be a cryptographic system. The strength of a cryptosystem is determined by its key, which is one of the basic rules of cryptanalysis. The basic premise of this definition is that a cryptosystem is a well-known system that requires a lot of time and money to change, so it is only necessary to protect the information by changing the key.

DISCUSSION

This method has many advantages over certain methods of integrity checking using a secret key. Let's look at some of the uses of cryptography. Two modifications are used to hide the meaning of the information being transmitted: encoding and encryption. Coding uses books or tables that contain a set of frequently used phrases. Each of these phrases is, in most cases, a randomly selected code word with a set of numbers. A similar book or table is required to encode the information. An encoding book or table is an example of an optional cryptographic change. Information technology requirements for coding - the ability to convert string data into numeric data and vice versa. Encoding can be done on fast and external storage devices, but such a fast and reliable cryptographic system is not successful. If this book is used without permission, it will be necessary to create a new code book and distribute it to all users. The second type of cryptographic conversion involves encryption - algorithms that convert the original text into a form that cannot be understood.

CONCLUSION

. Cryptography protects information from unauthorized access and ensures its confidentiality. For example, when sending payment slips by e-mail, it can be changed or fake entries can be added. In such cases, it is necessary to ensure the integrity of the information. In general, unauthorized access to a computer network cannot be completely prevented, but it can be detected. This process of verifying the integrity of information is often referred to as ensuring the authenticity of the information. The techniques used in cryptography can ensure the authenticity of information with a small amount of modification.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

3 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

4Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

5 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.