IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 1, Ser. II (Jan - Feb 2019), PP 65-68
www.iosrjournals.org

Importance of Cryptography in Information Security

Muharrem Tuncay Gençoğlu
Department of Computer Technology, University of Firat, Elazig, Turkey
Corresponding Author: Muharrem Tuncay Gençoğlu

Abstract: *This investigation argues that cryptography is a very effective technique to protect highly confidential and valuable information from cyber criminals. Information security is becoming one of the hot topics around the world. The need for modern cryptography to provide techniques and keys to protect information is vital. The process of encryption and decryption is essential for the communication of highly sensitive information. This inquiry emphasizes that without cryptography, private information such as credit card details, passwords and identity card numbers will be accessible to cyber criminals. This study also discusses relevant topics such as the definitions of cryptography, history of cryptography, principles and types of cryptography. Even though cryptography is used to convert information into an unreadable format, we cannot be absolutely sure that confidential data would not be accessed by cyber criminals who seem to be getting smarter and smarter by the day. Technological advancements have enabled them to improve their criminal techniques. Hence, it is important that we learn how to outsmart such criminals.*

Keywords: *Cryptography, Algorithms, code, encryption, decryption,*

Date of Submission: 30-01-2019 Date of acceptance:16-02-2019

I. Introduction

In today's rapid growth of digital communication and electronic data exchange, many of us communicate in cyber space without giving a second thought about security. We exchange a lot of our private information and secrets in cyberspace. Whether we like it or not, our digital footprint is in cyberspace. To be precise, whatever we communicate is often unprotected and open to cyber criminals for manipulation. There is hence an urgent need for modern cryptography to find ways to protect sensitive or confidential information. Effective encryption and decryption of data hold the key to security in cyberspace. As such, we need to convert information into an unreadable format so that it can be protected and accessed only those authorized to do so.

Cryptography is a crucial instrument to protect information that is communicated using computers. Cryptography is an artistic transformation of data into an unreadable format so that only the intended recipient can understand and use it. Cryptography is the art and science of hiding important and secret information from being infringed upon by unauthorized persons. Hence, generally speaking, cryptography is all about protecting and safeguarding information from cyber criminals or anyone else other than the intended recipient. Cryptography enables people to communicate on the Internet, transferring crucial and confidential information securely. Therefore, cryptography permits users to use public or private media such as the internet to do online shopping and evade being victims of criminals and password sniffers. This is accomplished by using the latest technological advancements in computer science. Cryptography, also known as cryptology, thus helps users and institutions to cipher and decipher hidden messages into codes, ciphers and numbers so information can be transmitted safely. Cryptography is initiated by encryption and decryption keys. The process of coding and transformation of plain text into the unreadable format is called encryption; while the process of decoding and converting the unreadable text to readable information using a special digital key is called decryption. As discussed earlier, the sole purpose of cryptography is to protect information, email, credit card details and other personal data transmitted across a public network[1-4].

Two major techniques in cryptography are used to convert information into encryption[5-6].

1.1. Symmetrical Cryptography

This technique is related to algorithms. It uses the same digital key for encryption as well as decryption. It is also called secret-key, personal key, private key and shared key. Although the named keys are not exactly identical, they are related to one another. Nevertheless, symmetrical cryptography is a weak technique of protecting information. As it is easily decoded, it is prone to attacks by criminals and can be hacked. Still, if it is planned and carefully executed, the risk of decoding is reduced.

1.2. Asymmetrical Cryptography

This cryptography technique uses different digital keys for the encryption and decryption of information. In asymmetrical cryptography, a pair of digital keys is used by the end user. One digital key is dedicated to encryption while another is assigned for decryption. These digital keys are called public and private keys. Both keys are different from each other. Hence, the general view is that asymmetrical cryptography is reasonably safe and secure. One of the techniques used in asymmetrical cryptography is the assignment of a key to a particular type of data. Another interesting concept in asymmetrical cryptography is the usage of a random digital key assigned by the public key keeper or the sender. It is also called pair digital keys that must be used to encrypt and decrypt the information.

II. Basıc Prıncıples Of Cryptography

The following are some important principles of cryptography:

1. Encryption: Encryption is one of the important principles of cryptography. This principle indicates that a message or information must be encrypted to become unreadable so that the privacy of individuals is protected. This principle also shows that the recipient of information must decrypt the received information by using a special digital key.
2. Authentication: One of the important principles of cryptography is identifying the origin of the information. When the source of information is identified it is easy to communicate securely. Authentication is only possible by providing a special key exchange to be used accordingly by the sender to prove his/her identity.
3. Integrity: Integrity of information sent to the receiver is very important. This principle indicates that cryptography ensures the integrity of data by providing codes and digital keys to ensure that what we receive is genuine and from the intended person. The receiver is assured that the information received has not been modified or compromised during the process of transmission. For example, a cryptographic hash is utilized to ensure the integrity of the information.
4. Non-Repudiation: This principle ensures that the sender of the information cannot deny the fact that he/she never sent the information. This principle uses digital signatures to prevent the sender from denying the origin of the data.

2.1. Types Of Cryptography

Cryptography is divided into three main types[7-10]:

2.1.1. Secret key Cryptography

This type of cryptography utilizes only one covert digital key. The same digital key is used for encryption and decryption. When the sender of the original data sends the information, he uses the same key to encrypt the information into the unreadable format and the recipient also uses the same key to decrypt the data into a readable format. This is a simple type of cryptography with one serious problem. The distribution of a single key may open the door to abuse.

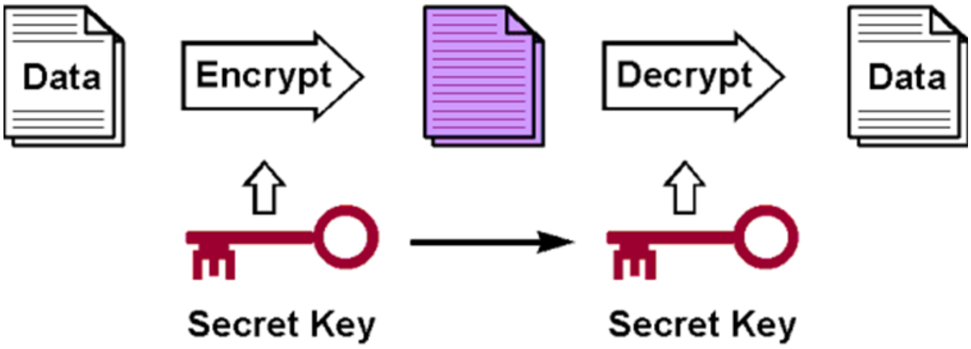

Fig.1. Secret key Cryptography

2.1.2. Public key Cryptography

Unlike the secret digital key cryptography concept, the public digital key utilizes a pair of digital keys. The two-key system enables the parties to communicate more securely. In this type of cryptography, each communicating party has a pair of keys. One key is secret while another is considered public. The public key is shared among them. When sending information, the sender will use the public key to encrypt the information. Once the recipient gets the encrypted information, he uses his secret key to decrypt the information into a readable format.

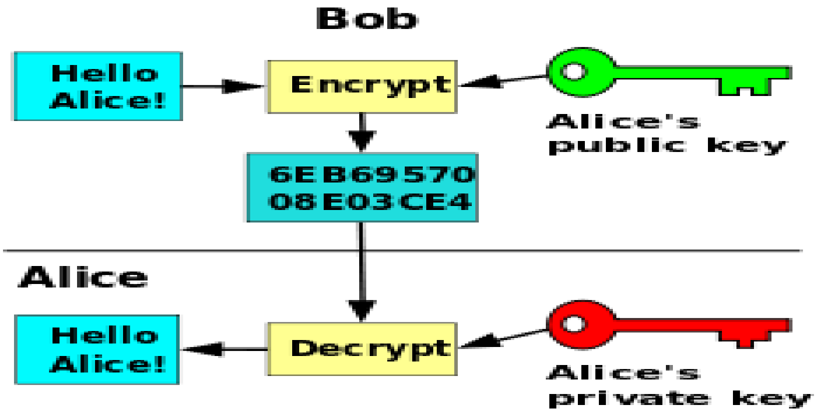

Fig.2. Public key Cryptography

2.1.3. Hash Functions

This type of cryptography does not require any digital key as it utilizes a fixed length hash value encrypted into the plain text. The purpose of the hash key is to make sure that the original information is not tampered with. This is a one-way encryption. It uses algorithms to facilitate communication. The hash key normally provides a digital fingerprint, making sure that the file is not corrupted or infected with a virus. The hash key also helps computer administrators to encrypt passwords.

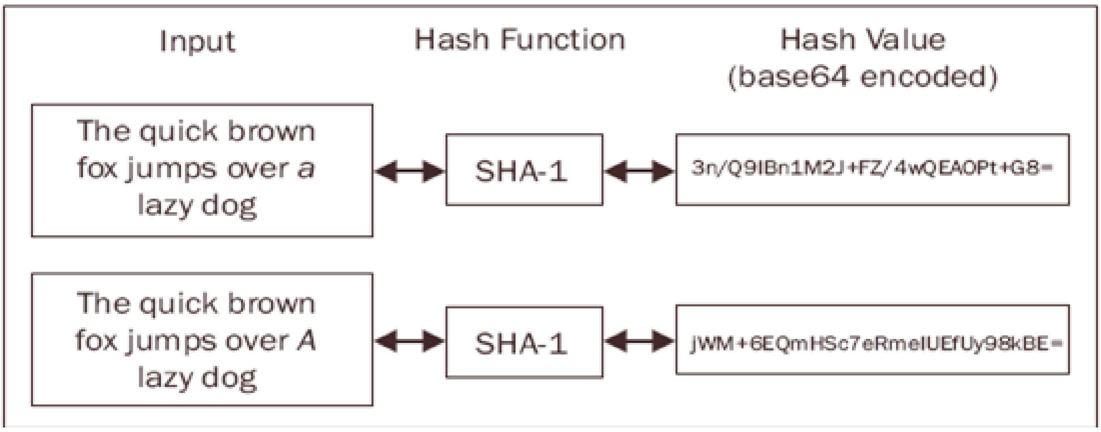
Input
Hash Function
Hash Value (base64 encoded)
The quick brown fox jumps over a lazy dog
SHA-1
3n/Q9IBn1M2J+FZ/4wQEAOPt+G8=
The quick brown fox jumps over A lazy dog
SHA-1
jWM+6EQmHSc7eRmeIUEfUy98kBE=

Fig.3. Hash Function

III. Conclusion

As evident from the above discussion, today most of us communicate or send data in cyberspace at our own risk. We transmit private information and secrets when we use the Internet for various purposes. Whether we like it or not, the information out there in cyberspace may be hacked by cyber criminals. Information security should be a top concern of all computer users around the world. There is a need for modern cryptography to provide protection and digital keys to ensure that information that is transmitted in cyberspace remains intact and secure. Techniques of encryption and decryption must be improved to ensure the highest possible level of security to bona fide internet users. In this digital age, the challenge is to outsmart cyber criminals so that both the sender and intended recipient can enjoy peace of mind. We need to convert our information into unreadable forms so that our data can be protected and will reach its destination safely.

Today, in the age of computerization, we are facing increasing risk of having our intellectual property compromised, and falling victims to cheating, fraud and impersonation. Therefore, we need strong cryptography to protect us from these criminals. Even though we use cryptography to convert our information into an unreadable format, needless to say, we are still not completely safe. The criminals are becoming smarter and smarter by the day. Advancement in technological achievements also makes them more aggressive.

References

[1]. Koç, Ç.K, Cryptographic Engineering, Springer, 2009, PP 125-128.
[2]. Bachman, D. J.; Brown, E. A.; Norton, A.H, Chocolate Key Cryptography, Mathematics Teacher, 104(2),2010, p100-104.
[3]. Martin, K.M, Everyday Cryptography Fundamental Principles and Applications, Oxford University Press,2012.
[4]. Delfs, H.and Knebl, H. Introduction to Cryptography Principles and Applications, Springer,2007.
[5]. Paar, C.and Pelzl, J, Understanding Cryptography, Springer,2010.
[6]. Gençoğlu, M.T, Embedded image coding using laplace transform for Turkish letters, Multimedia Tools and Applications, 67(3),2019,PP 1-14.
[7]. Jung, I. Y.; Yeom, H. Y, Enhanced Security for Online Exams Using Group
[8]. Cryptography, IEEE Transactions on Education,52(3),2009, p340-349.
[9]. Karls, M. A, Codes, Ciphers, and Cryptography-An Honors Colloquium
[10]. PRIMUS, 20 (1),2010, p21-38.
[11]. Kaur, M, Cryptography as a Pedagogical Tool, PRIMUS, 18(2),2008, p198-206
[12]. White, T,Encrypted Objects and Decryption Processes: Problem-Solving with Functions in a Learning Environment Based on Cryptography. Educational Studies in Mathematics,72(1),2009, p17-37.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Muharrem Tuncay Gençoğlu. " Importance of Cryptography in Information Security" IOSR Journal of Computer Engineering (IOSR-JCE) 21.1 (2019): 65-68.