Cryptography

Technical Description

INTRODUCTION

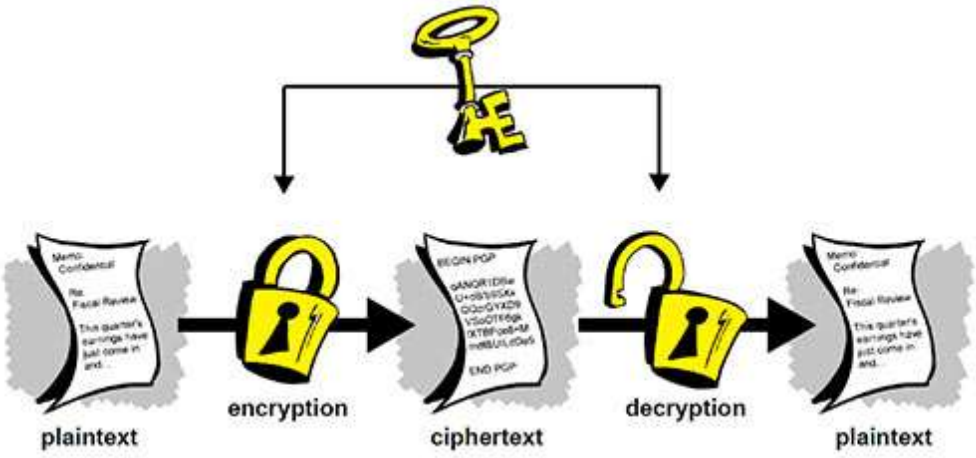
The purpose of this description is to explain the process of the basic structure of cryptography within the field of computer science.

In general, cryptography is a process that ensures the safety of transmitted data. Within the field of computer science, cryptography is a security process that is used with common virtual transactions such as with online payments, e-mails, and databases. Understanding the general structure of cryptography is important, because it provides high levels of security of private information through a transaction, in order to prevent any unwanted interferences.

PROCESS OF CRYPTOGRAPHY

OVERVIEW

The entire process of cryptography is enclosed in the idea of a cryptosystem [1].

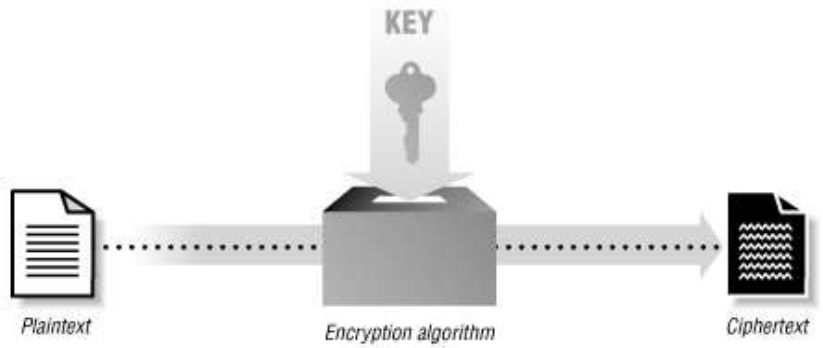


[2]

A cryptosystem consists of two main programs: encryption and decryption. A single set of information is passed through a cryptosystem that undergoes these two programs. It starts off as what is called a plaintext before this set of information is encoded within the system. The plaintext becomes encoded as it goes through the encryption program. Through encryption, the plaintext is transformed into a piece of information that appears to be ambiguous, which is called a ciphertext. This now ciphertext can only be revert back into its plaintext as it goes through the decryption program. In addition, there are algorithms and mathematical formulas creating an encryption key and decryption key that are also used throughout this process of cryptography.

ENCRYPTION PROGRAM

The encryption process is how the plaintext is transformed into a ciphertext in order to be transferred safety through a cryptosystem.



[3]

The basis of encrypting a message involves computed various algorithms and mathematical formulas, which are determined by the programmers themselves.
An encryption key and a decryption key are created through these encryption algorithms.

Imagine: In order to lock a lock, a key is necessary to complete this action.

The generated encryption key is that key. It is needed for a set of transmitted information to be secure. The key insure that all of those logical processes are private and unseen from any unwanted observers as the private information goes through its transaction.

There is one situation where both the encryption key and the decryption key are the same key and another situation where they are different keys.

EQUAL ENCRYTION KEY AND DECRYPTION KEY

When the encryption key and decryption key are equal, they are the same. Being the same key, this key has to be kept private; such as a shared password [1]. This is to make sure that the information being protected is kept safe.

DIFFERENT ENCRYPTION KEY AND DECRYTION KEY

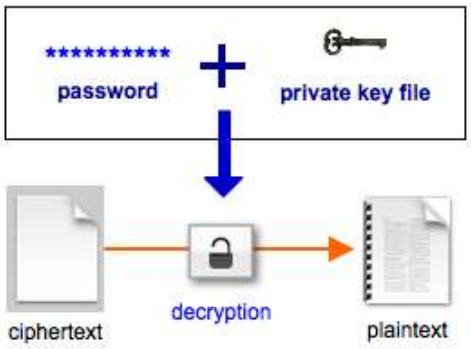
When the encryption key and decryption key are different, usually the encryption key is publically shared and the decryption key is kept private [1]. Such as a personal password used as a decryption key.

Realistically, both situations are used every day in data security [1].

Furthermore, the use of the logical processes transform the private information from its plaintext state to its ciphertext state. Based on appearance, the encryption algorithms convert the understandable plaintext into an ambiguous ciphertext, in order to keep the private information safe from any outside eavesdroppers. Yet through the process of decryption, what appears to be ambiguous nonsense, is then decode back into what is then again understandable information to its viewer.

DECRYPTION PROGRAM

The decryption process reverts the encode information (ciphertext) back into the original information being shared (plaintext).



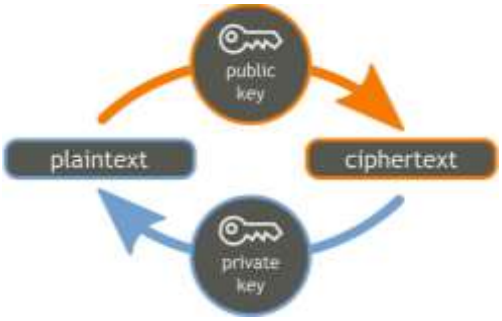
[4]

Imagine: With the correct key, this is the process that unlocks a secured lock.

The decryption key that was created through the encryption program, is now used by the secondary source to convert the ciphertext back into the plaintext. The output generated is the plaintext, unless the ciphertext has been tampered with by unwanted outsider of the cryptosystem. In that case, the output generated would be an error [1]. This added level of caution characterizes the overall process of cryptography a reliable high level form of data security, which is used daily among day-to-day virtual communication.

CONCLUSION

Overall, the aspect of data security is the basis of cryptography. First off, a preliminary source withholds private information that is needed to pass on to a secondary source. Within the idea of a cryptosystem, this transaction can be done securely and efficiently. The plaintext is passed through a program of encryption that contains the creation of an encryption key. The encryption key is created with a series of algorithms and mathematical formulas, which then a decryption key is also created in order to complement and revert the encryption process. Through encryption, the once plaintext is transformed into a ciphertext that can only be read by the secondary source when pass through a program of decryption. With the availability of the decryption key for the ciphered message, will only the original message be revealed. This process can also be done in the reverse, from the secondary source back to the primary source.



[5]

The process of cryptography is used daily in society's common practices such as through internet browsing, company databases, and private messaging. It is important to understand how these essential data is kept secure. Cryptography is a process that takes the value of a private message and keeps it reserved and safe.

This Technical Description Created By:
Rhea Mae Edwards
Technical Writing (WR 327)
Liz Delf

Bibliography
Citation Style: IEEE

[1] P. Cetef, *Cryptography 101 – The Basics*. 2013 [Online]. Available: https://www.youtube.com/watch?v=fNC3jCCGJ0o. [Accessed: 2 May 2016]

[2] *Figure 1-1 : Conventional Encryption*. 2016 [Online]. Available: https://www.pantechsolutions.net/images/stories/virtuemart/product/cryptography.jpg. [Accessed: 28 April 2016]

[3] *Figure 6.1: A simple example of encryption*. [Online]. Available: http://www.diablotin.com/librairie/networking/puis/ch06_02.htm. [Accessed: 3 May 2016]

[4] J. V., *Figure 1*. 2013 [Online]. Available: http://www.jscape.com/blog/bid/97283/Automatically-PGP-Decrypt-Files-Upon-Download-from-FTP-Server. [Accessed: 3 May 2016]

[5] T. DeMichele. 2016 [Online]. Available: http://factmyth.com/factoids/cryptography-is-the-art-of-writing-and-solving-codes/. [Accessed: 3 May 2016]