Cryptography

Technical Description

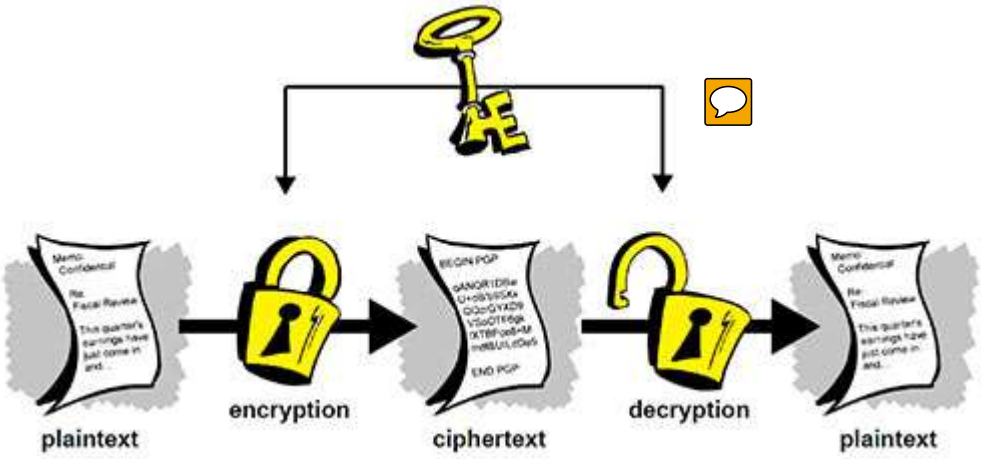
INTRODUCTION

The purpose of this description is to explain the process of the basic structure of cryptography. In general, cryptography is a process that ensures the safety of transmitted data. Cryptography is a security process that is used with common virtual transactions such as with an 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 to prevent any unwanted interferences.

PROCESS OF CRYPTOGRAPHY

OVERVIEW

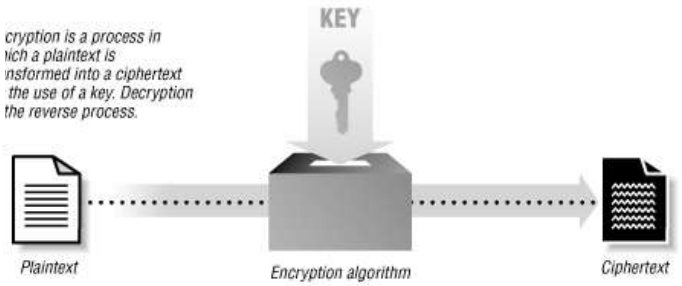
The entire process of cryptography is enclosed in the idea of a cryptosystem. [1]
A cryptosystem consists of two main programs: encryption and decryption. A single set of information is passed through a cryptosystem that undergoes these two programs. It starts off as a plaintext before this piece of data is encoded within the system. The plaintext becomes encode as it goes through the program of encryption. By encrypting this message, this plaintext is transformed into a piece of information that appears to be ambiguous. This now ciphertext can only be revert back into its plaintext as it goes through the process of decryption. In addition, there are algorithms and encryption and decryption keys that are used throughout this process of cryptography.



[2]

ENCRYPTING

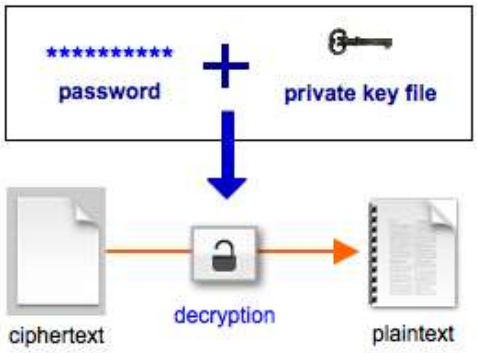
- Figuring out an algorithm to encode the plaintext.
- The algorithm can also be reversed/decoded.
- With the use of a chosen algorithm, an encryption key is created.
- Encrypting is like locking/securing the private information.
- The ciphertext not being understood (ambiguous) to any outside eavesdroppers.



[3]

DECRYPTING

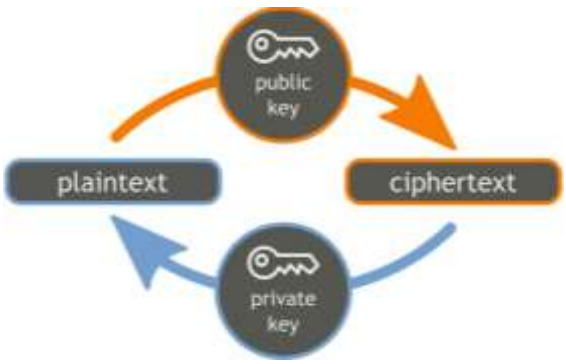
- Unlocking the ciphertext, revealing private information, converting back into plaintext.
- The decryption key, which can be associated with a password of some sort, will decode the ciphertext.



[4]

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 pass through a program of encryption that contains the creation of an encryption key. The encryption key is created with a series of algorithms, which then a decryption key is also created in order to complement the 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. Cryptography is a process that takes the value of a private message and keeps it safe.



[5]

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]