Cryptography in Computer Security

Muthu Dayalan
Senior Software Developer,Chennai, India

Abstract-**One of the major concerns in the use of technology today is the security of information. Organizations invest heavily in information system security to avoid damage and theft of the software, hardware as well as the information contained therein. This process is referred to as computer security or cyber security. It also aims at protecting information from access by unauthorized persons and harm from the internet such as viruses. In this paper, cryptography which is one of the main methods used in information protection is discussed highlighting its originality and the methods used in the early days and in modern days. The three methods of cryptography together with their advantages and disadvantages are also discussed. Additionally, the threats and attacks that the cryptography process secures information from are outlined. A discussion of the life cycles of secret keys and passwords from their generation to their disposal is also included**.

Key words – **cryptography, secret key, password, encryption, decryption .**

I. INTRODUCTION

This is the process in which a plain text is converted into a text that is hard to be interpreted by any other person except the intended. The method converts the message into unintelligible form before being transmitted to the intended user [6]. This process hinders data from being altered, stolen and helps in authentication of the user. The main goal of cryptography is to provide:

a) Confidentiality- through cryptography confidential data is protected from being accessed by strangers or unauthorized individuals [6]. Text form is usually in a way that no one else can understand it other than the targeted receiver.
b) Allows authentication: cryptography allows both the message sender and the receiver to confirm and identify each other. This ensures that the data receiver understands the sender to avoid cases of wrongly sent information or data meant to destroy the information system [6]
c) Maintains Integrity: this information protection method ensures honesty in the data being transferred [6]. In this, the data sender cannot send destructive information especially in a company and they bear the responsibility of the information sent.
d) Prevents repudiation: through cryptography, the main intentions of the information sender cannot be changed later on denied.

This cryptography information security method also:

a) Provide security from attacks such as malware and viruses [12]
b) Prevent cryptanalysis: this is done when information is being transmitted through the communication lines [2]. Attackers get access to the information and retrieve the original information.
c) Prevents use of unauthorized applications: uncertified applications may result in the injection of viruses to the information system hence attack the saved data [11]. Cryptography prevents this by allowing only certified applications.
d) Prevents access of data by unauthorized individuals.

II. CRYPTOGRAPHY AND COMPUTER SECURITY

Cryptography originated from the great need to hide information and allowing only a few people to have access to it [8]. During wars, gathered information about the enemy needed to be kept in secret to avoid linkage. Field commanders, as well as agents, could not get the advantage of their enemies without keeping this information in secret. The best way to achieve this was through hiding the meaning of their information such that only the authorized persons understood it [8]. Some of the methods used in the early days were:

a) Coding
b) Substitution
c) Transposition

In later days, cryptography has still been in use mainly in the protection of documents containing military information and political plans [7]. Improved technology has led to the evolvement of cryptography and computer security such that they have become a necessity in most operating organizations as well as individuals. This has resulted in the emergence of several types of cryptography which include:

III. SYMMETRIC CRYPTOGRAPHY METHOD

In this cryptography method, the secret key is known by both the data sender and the receiver [13]. They have the knowledge of the passwords used to encrypt and decrypt the information in advance. Flow of information in this method is as illustrated in fig .1

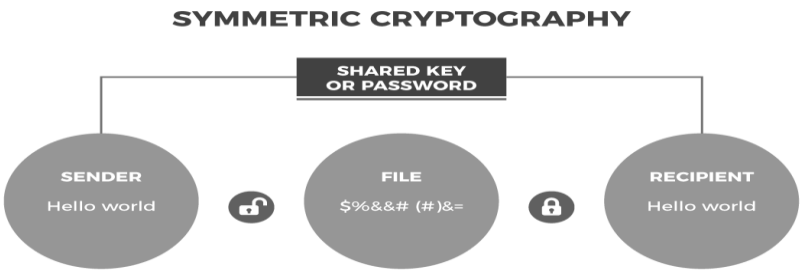

Figure 1 symmetric cryptography

Symmetric method 1

Advantages of Symmetric Cryptography

a) Encrypting and decrypting data is usually easier as the key is already known and does not involve complicated computations [13].
b) It has guaranteed security and can take many years before any one guesses the secret key or the password especially when used with the 256-bit
c) The method uses different secret key where several people are involved this means that when a pair has interfered with their key, the rest continue with communication without any effects [13].

Disadvantages of Using Symmetric Cryptography

a) There has to be a much secure way of sharing the secret key to the other party. This to avoid a case of the key being intercepted and give and the information tampered with [10].
b) It is sometimes unreliable to use: considering that the major goal is to keep the data secured makes this cryptography method unsafe to use due to the vulnerability of the secret key.
c) The use of so many secret keys with the different person that receives the information, it becomes challenging to keep the keys secure [10].
d) Due to the sharing of the secret keys for both the sender and receiver of the data, it may be hard to verify that the particular senders.

IV. ASYMMETRIC CRYPTOGRAPHY

In this method, two different keys are usually used as shown in fig.2 to encrypt the information [15]. One of the secret keys is known to the public while the other is kept secret. The public key can be shared out and is the one used in encryption while the secret key is only known and used by the few that have been given to decrypt the information [15].

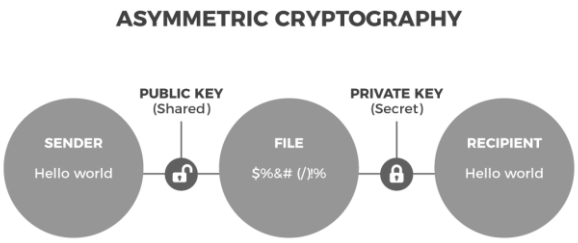

Figure 2 asymmetric cryptography

Advantages of Asymmetric Cryptography

a) It is convenient to use: the issue of distributing the key is solved and everyone can use their secret key to decrypt the information [10].
b) Gives room for authentication: the method uses digital signatures which the message receiver can verify who the sender is.
c) Prevents repudiation: due to digital signing, message sender accepts and can never deny or disown the sent information [10].
d) Easy to detect any interference: use of digital in encrypting information secures it from being altered on the way.

Disadvantages of Asymmetric Cryptography

a) Slow to decrypt: the method takes time to access information especially where large messages need to be decrypted
b) Due to the use of an individualized secret key, a loss of it may lead to loss of access to all your data.
c) It requires the use of several computers for the different types of keys used compared to a single key is used [10].

V. HYBRID CRYPTOGRAPHY

Given the challenges faced in the symmetric and asymmetric cryptography, hybrid merges the two to and makes use of their strengths in encrypting information [3]. Hybrid users refer its strengths as speed and security as information is kept secure and accessing it is easier. When both public and private keys are well protected, hybrid cryptography becomes the most secure method of protecting information. Its effectiveness is achieved through the incorporation of asymmetric convenience and workability of symmetric protection method [3]. It also combines a unique key and symmetric encryption when transmitting information making it more convenient for its users. Fig. 3 gives an illustration of hybrid cryptography.

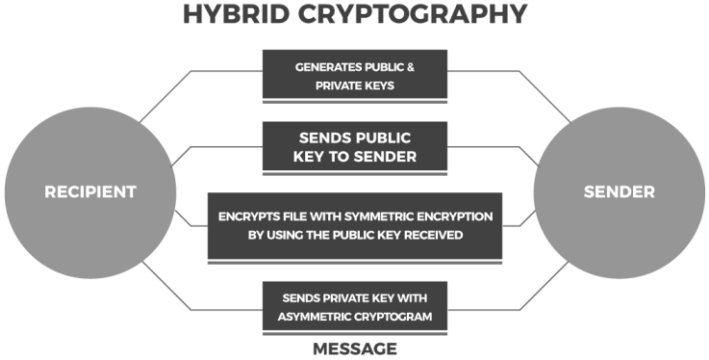

Figure 3 Hybrid Cryptography

VI. THE LIFE CYCLES OF KEYS AND PASSWORDS IN CRYPTOGRAPHY

Secret Key and Password Generation

The life cycle of any key or passwords used in encryption starts when they are generated [4]. Various protocols have to be observed to ensure that the generated passwords and keys are secure to guarantee the security of the information they protect .these protocols are:

a) The secret key and passwords should use a combination of both symbols and characters in an un-logical manner.
b) Use learning techniques such as mnemonics to enable one keep remembering the secret keys and passwords [4].
c) Personal information such as phone numbers, birth dates should not be used as they can easily be guessed giving access to the secured information [4].

Distribution

Once the key and passwords have been established, methods such as symmetric cryptography require that the key or the password be transferred to the other party to allow the communication flow [5]. This distribution method has to be well secured to ensure the security of the passwords and the secret keys. Distribution is usually through:

a. Manual Distribution: The secret key and the passwords are first encrypted then distributed through telephone fax, injection keys or through certified letters.
b. Central distribution: In this, a secured connection which is usually encrypted by a third party is used to transfer the encrypted secret key and the passwords to the parties involved [5]. The certified methods used operate under policies that manage passwords and secret keys.

Password Recovery

There are usually high chances of forgetting or losing the secret key or the passwords due to various issues that need to manage [1]. This calls for the use of password recovery protocols which are used when one needs to recover the secret key or the password or reset the two [1]. The process is done under the policies and set conditions that usually confirm the authenticity of all the information provided during key and password generation.

Use Policies

Use policies handle the issues of keys and password generation, how they are used, how they are recovered and replaced in case one forgets and the measures followed when disposing of the keys and the password [14]. These policies also determine the length and the characters used in the key and passwords .additionally, use policies also determine the password storage, the manner in which the passwords are disposed of as well as the expiration of the keys and passwords.

Storage

The fifth key and password lifecycle stage is the storage of the information containing them in the database [14]. This makes it possible to authenticate the secret key users. In preventing access to the database information by unauthorized persons:

a) All files containing the keys and passwords are encrypted
b) The access control is activated with the operating system
    1. The secret key and password obsolescence

This is the end of life of the passwords and keys and they have to be disposed of. The process is governed by policies to avoid theft or access by others [9]. The two disposal types are:

a) Expiration disposal: it is done when the passwords or secret keys reach their maximum usage time.
b) Disposal due to revocation: it triggered by a detection of access by unauthorized individuals or when the user resigns or dies [9].

The disposals are done through:

I. Erasing
II. Crypto-shredding
III. Demagnetization of the magnetic Media.

VII. CONLUSION

In conclusion, cryptography through the three methods of information encryption which are the symmetric, asymmetric and the hybrid is considered the most secure way of protecting information in the information technology (IT) world today. The mode in which the data is changed into ensures that only the intended users can have access to it. This ensures that organizational confidential data, as well as important client information especially in institutions like banks, are secured from access by unwanted persons. Additionally, the process, through which the secret keys and passwords are generated, transferred up to the point of disposal shows how cryptography process effectively protects information. Its significance, especially in organization related information, is realized through the provision of authentications where individuals sharing the information have to be verified. This ensures that sensitive company data is only shared by specific persons hence kept secure. Additionally, the use of digital signatures in cryptography guarantees security as it is hard to forge a digitalized signatures and helps in maintaining integrity. Further, this data protection method has led to maintenance of confidentiality such that very sensitive information can be sent through the networks without the fear of it being accessed.

REFERENCES

[1] Arthan, R. D. (2004). *U.S. Patent No. 6,754,349*. Washington, DC: U.S. Patent and Trademark Office.

[2] Bishop, M. (2003). What is computer security?. *IEEE Security & Privacy*, *99*(1), 67-69.

[3] Dent, A. W. (2004). Hybrid cryptography. *IACR Cryptology ePrint Archive*, *2004*, 210.

[4] Ishii, S. (1998). *U.S. Patent No. 5,768,389*. Washington, DC: U.S. Patent and Trademark Office.

[5] Karnin, E., Greene, J., & Hellman, M. (1983). On secret sharing systems. *IEEE Transactions on Information Theory*,*29*(1), 35-41.

[6] Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[7] Lim, H. W., & Robshaw, M. J. (2004, June). On identity-based cryptography and grid computing. In *International Conference on Computational Science* (pp. 474-477). Springer, Berlin, Heidelberg.

[8] Marcia Ojeda. (2018, May 2). Cryptography and Computer Security: The life cycle of Passwords & Keys Life cycle and their relationship with your protection. Retrieved from https://www.gb-advisors.com/cryptography-and-computer-security

[9] Narendra, S. G., Tadepalli, P., & Spitzer, T. N. (2013). *U.S. Patent No. 8,477,940*. Washington, DC: U.S. Patent and Trademark Office.

[10] Patarin, J. (1996, August). Asymmetric cryptography with a hidden monomial. In *Annual International Cryptology Conference* (pp. 45-60). Springer, Berlin, Heidelberg.

[11] Salem, Y., Abomhara, M., Khalifa, O. O., Zaidan, A. A., & Zaidan, B. B. (2011). A review on multimedia communications cryptography. *Res. J. Inform. Technol*, *3*, 146-152.

[12] Shree, D. (2017). A Review on Cryptography, Attacks and Cyber Security. *International Journal of Advanced Research in Computer Science*, *8*(5).

[13] Tripathi, R., & Agrawal, S. (2014). Comparative study of symmetric and asymmetric cryptography techniques.*International Journal of Advance Foundation and Research in Computer (IJAFRC)*, *1*(6), 68-76.

[14] Utin, D. (2013). *U.S. Patent No. 8,447,990*. Washington, DC: U.S. Patent and Trademark Office.

[15] Vikas agarwal et al., "Analysis and Review of Encryption and Decryption for Secure Communication", International Journal of Scientific Engineering and Research IJSER), ISSN (Online): 2347-3878, Volume 2, Issue 2 (February 2014)