Xournals

Academic Journal of Information Security

ISSN UA | Volume 01 | Issue 01 | January-2019

Cryptography: A Way to Secure Network Information

Aman Sharma[1] and Prakhar Saxena[1]

Available online at: www.xournals.com

Received 12th September 2018 | Revised 16th October 2018 | Accepted 12th December 2018

Abstract:

In information and communication technology, a modern ear of networking and wireless networks has been come in which security is an important factor. Now, the exchange and transmitting of information through the internet and other communication medium is common due to which the vulnerability of the information is increased. To reduce the chance of threatening of data, information security plays a vital role. In information security, the process of cryptography technique provides the security to the network. It protects the data or information from the unauthorized user and give the guarantee that the contents of a message are transmitted with confidentiality and it would not be changed. Various techniques of cryptography has been emerged to obtain secure communication. In cryptography, there are two types of techniques; symmetric and asymmetric key encryption. The secret data which is transferred over electrical cable is very sensitive. It can be accessed as the purpose of malignant. This paper discuss about the cryptographic technique with its objective, principle and types.

Keywords: *Cryptography, Encryption, Keys, Confidentiality*

Authors:

1. *Maharaja Ranjit Singh College of Professional Sciences, Indore, Madhya Pradesh, INDIA*

Introduction

In recent time, the information of technology applications is protected by the cryptography. For some applications such as ecommerce, e-mail, e-banking, medical databases and so on, information security has been made an important issue. All these information need the exchange of private information. This private information can be hacked by the hacker and modified by change the meaning of message. So, protecting the information or data, many techniques have been developed. In which cryptography plays a vital role.

Cryptography is a study of techniques that is used for securing the information from the third person. It involves the generation of codes that allows the information secure in a secret way. The word of cryptography was came from Greek word 'kryptos' means hidden and 'graphein' means writing. In general term, cryptography is the exercise and study of hidden writing or the science of text or message encryption and decryption. It is also defined as the art of concealing information that has been practiced. In early time, it is done in the form of secret writing which was written with the help of lemon and other biological fluids and generated by heat. (**AbuTaha *et al.*, 2014; Agrawal *et al.*, 2014)**

Goals of Cryptography

Encryption, a step of cryptography, is a techniques study that has many goals:

1. **Confidentiality:** It is the goal in which received message cannot be understand by anybody except the one who has the key for deciphering.
2. **Data Integrity:** By this objective, it is ensured that the data was not controlled in an unapproved way. The receiver gets information or data in unaltered form. This unaltered data can be attained by hashing used on both side sender and receiver.
3. **Authentication**: This goal has two classes in which one is entity authentication and another one is message authentication. It is used for proving the identity means system and user both can prove their identities to others.
4. **Non-repudiation:** This objective gives the guarantee that receiver can demonstrate that message is sent by the sender without any doubt. And sender cannot deny that he/she did not signed the computerized data.
5. **Access Control**: The prevention from an unauthorized use of resources is done by access control. It controls the access of anyone to the resources. The access can be occurred under the restrictions and conditions, and the permission level of the given access is also identified.

(Dhiman and Singh, 2017; AbuTaha *et al.*, 2014)

Principle of Cryptography

The principle of cryptography is explained in the term of discrete-value cryptosystem which is described as:

- Plaintexts, denoted by P
- Ciphertexts, denoted by C
- Cipher keys, denoted by K
- Encryption and decryption are denoted by E and D respectively.

(Dhiman and Singh, 2017)

Cipher is a framework of encryption. It is also called the cryptosystem. In Cryptosystem, message for encryption is called plaintext (P) while the scramble message is termed as cipher text (C). Cryptosystem is defined below in the form of diagram:

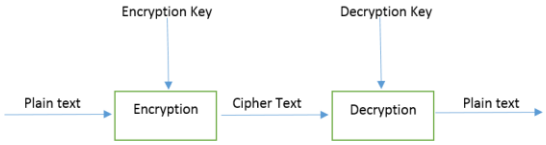
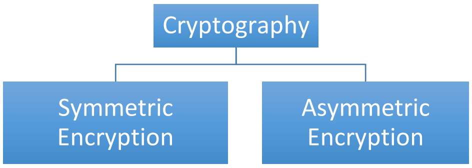


Figure: Cryptosystem (Dhiman and Singh, 2017)

Classification of Cryptography

There are two types of techniques for the encryption and decryption for protecting the data. These are as follows:



Symmetric Encryption: It is also called private key encryption. Same secret key is used by the symmetric key cryptography for the encryption and decryption. This key is relatively lightweight in processing and used for the data encryption and authentication. Because of the use of only one key, it is speedier and less difficult. In symmetric key encryption, there are two types: Stream ciphers and block ciphers. In stream cipher, the digits of a message are encrypted at a time. Advanced Encryption Standard (AES), Data Encryption Standards (DES), Triple DES, Blow fish, and multiphase encryption are examples of Symmetric key encryption.

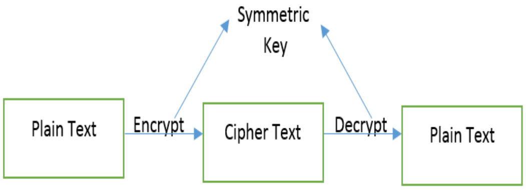


Figure: Symmetric Key Encryption (Tayal *et al*, 2017)

Advantages of Symmetrical Encryption

- For proving the receiver's identity password authentication is used by the symmetric cryptosystem.
- The message can be decrypted by that system has a secret key.

Disadvantages of Symmetric Encryption

- Digital signatures are not provided by it that cannot be repudiated.

Asymmetric Encryption: It is also called public key encryption. It is a technique that have two different keys for the encryption and decryption process. In which one key, called public key that is used for encryption the original message. And another key, called private key that is used for the decryption the message. Receiver generates both keys; private and public key. After that public key is distributed by the receiver to the sender through a public key distribution channel (**Suguna, Dhanakoti and Manjupriya, 2016; Toshihiko, 2017; Tayal *et al.*, 2017).**

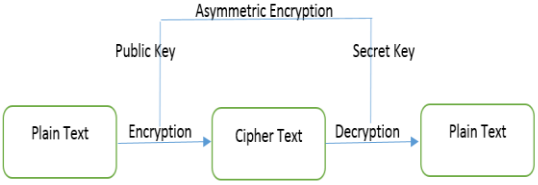


Figure- Asymmetric Encryption (Tayal *et al*, 2017)

Advantages of Asymmetric Encryption

- Digital signature is provided by it that can be rejected.
- In asymmetric encryption, there is no need of exchange keys.

Disadvantages of Asymmetric Encryption

- The speed is a main problem as it is slow as compared to other popular secret key encryption.

The mathematical function is used for both, encryption and decryption in asymmetric key cryptography while in case of symmetric key cryptography, substitution and permutation of symbols are used. For the authentication, digital signature and secret key exchanges, Asymmetric key cryptography is used. (http://www.uobabylon.edu.iq)

Review of Literature

Egele *et al.*, (2013) discussed about the cryptoline that checks the real world android applications. The violation of six security rules are checked. Approximately 10,327 applications were identified by researchers by which at least one of six rules were violated. In their paper, they also discussed about their current work which was on the cryptoline. They was working for making cryptoline as a publicly accessible online service. On this platform, developer and curious users can submit applications of android which can be evaluated to the cryptographic security rules. They also told about the future plan in which cryptoline with their security rules would be able to capture the misuse of asymmetric cryptography.

Agrawal *et al* (2014) stated that asymmetric image encryption scheme have many salient features followed as: lossless encryption of image, convenient realization, less computational complexity, and according to size of image, suitable size of matrix is chosen. An image that is tagged in image file format (TIF) can be encrypted or decrypted by blowfish algorithm. This image may be colored or black and white with any size. In their paper, they discussed MREA algorithm which is used for encrypting the files and then transferring it to other place where it is decrypted. The main feature of this algorithm is to satisfying the properties of confusion and diffusion. This algorithm has a perfect prediction that decryption is made impossible by encryption key.

Joshi and Karkade (2015) stated that in information security, network security is an important component because of the securing the information that are passed through networked computers. In their paper, they studied about the various cryptographic techniques that are used to increase the security of networks. According to them, cryptography with communication protocols give a high degree of protection against intruder attacks in digital communications.

Suguna, Dhanakoti and Manjupriya (2016) studied about the algorithm of both key encryption (symmetric and asymmetric) such as AES, DES, TRIPLE DES, RC4, Multiphase encryption, and others. In network communication, a vital role is played by the data security. The best algorithm should be chosen that depends upon the communication and channel. In recent time, asymmetric and symmetric cryptography play a significant role in network security.

Dhiman and Singh (2017) proposed that by their review study that the digital images should be secured especially in an open networks. They reviewed on the various techniques that are used for the image encryption. By their study they concluded that all techniques used for image encryption are useful because they provide better security functions. They gave a suggestion to choose a fast and secure algorithm for superior security then, access to the data and image will not be easy by anyone.

Toshihiko (2017) in their paper, they discussed about the lightweight cryptographies that are used for the resource-constrained environments of IoT by the developed technology of NEC. According to the researchers, the key management functions and operation are required for the lightweight cryptography. They also conducted a research the field of lightweight cryptography on public key encryption.

According to Tayal et al., (2017), the information security is very important. Information security of client has been made an important question over cloud. Cryptography plans with more scientific instruments are more acceptable because they includes numerous keys for the application of solitary. In their paper, they discussed various plans as a part of cryptography that are used for the network security reason. This paper also presented an idea of security of PC, and then, concentrates on PC system security’s dangers. By the use of key circulation and administration, and calculation of ideal cryptography for the information security, work is possible.

Conclusion

This paper study about the cryptographic technique that is used for securing the information from unauthorized person. In cryptography, different types of keys are used for the encryption and decryption. On the basis of use of key, different techniques are used in the cryptography which is used on the basis of communication and channel. All techniques of cryptography are useful for encryption and securing the information of many systems. Symmetric and asymmetric encryption techniques are used that have many advantages and disadvantages. In spite of these pros and cons, the cryptography is best technique in network security.

References:

AbuTaha, Mohammed, et al. "Survey Paper: Cryptography is the Science of Information Security." *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 3, 2011, pp. 288–309.

Advantages and Disadvantages of Cryptosystems. www.bing.com/cr?IG=57996A2013DE44CDA9E720BFC4FD27FD&CID=15135A45447563883FE4565C45886238&rd=1&h=yeVZGooLvj-0KCUoHC3ReKpU_e1EWx_k83O0qMMyoD8&v=1&r=http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf&p=DevEx.LB.1,5516.1.

Agrawal, Vikas, et al. "Analysis and Review of Encryption and Decryption for Secure Communication." *International Journal of Scientific Engineering and Research (IJSER)*, vol. 2, no. 2, Feb. 2014, pp. 1–3.

Amalraj, A. Joseph, and J. John Raybin Jose. "A Survey Paper on Cryptography Techniques." *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 8, Aug. 2016, pp. 55–59.

Dhiman, Reema. "Image Encryption Techniques: A Literature Review." *International Journal of Advanced Research in Computer Science*, vol. 8, no. 7, 2017, pp. 239–244.

Duong, Thai, and Juliano Rizzo. "Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET." *2011 IEEE Symposium on Security and Privacy*, 2011.

Egele, Manuel, et al. "An Empirical Study of Cryptographic Misuse in Android Applications." *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS 13*, 2013.

Joshi, Mukund R., and Renuka Avinash Karkade. "Network Security with Cryptography." *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 1, Jan. 2015, pp. 201–204.

Suguna, S., et al. "A Study on Symmetric and Asymmetric Key Encryption Algorithms." *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 4, Apr. 2016, pp. 27–31.

Tayal, Sandeep, et al. "A Review Paper on Network Security and Cryptography." *Advances in Computational Sciences and Technology*, vol. 10, no. 5, Nov. 2017, pp. 763–770.

Toshihiko, OKAMURA. "Lightweight Cryptography Applicable to Various IoT Devices." *NEC Technical Journal*, vol. 12, no. 1, Oct. 2017, pp. 67–71.