IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

OVERVIEW OF CRYPTOGRAPHY IN NETWORK SECURITY

Monika Khetarpal

Associate Professor
Department of Physics
Maharani Sudarshan College for Women, Bikaner, Rajasthan, India

Abstract: In the technological scenario the matter of security of information on the digital framework is of supreme concern. Data security protects any unauthorized communication of data and it is received only by the correct recipient without any alteration. Methodologies regarding secure transmission are developing in this technological world all across the globe. Cryptography is the art of maintaining the information safe and secret with the aid of codes so that only the correct person for whom the message is intended can read it. This paper deals with a detailed analysis of the functioning of cryptography in network security along with its types and applications.

Index Terms **- Cryptography, data, encryption, decryption, key**

I. INTRODUCTION

Cryptography is a technique of securing information through the means of various algorithms, so that person for which the message is intended can understand it and execute it [1]. The wrong intentions of people that they can alter the secret data are completely restricted by the use of cryptography. The precise meaning of term cryptography in Greek is 'secret writing'. Cryptography is the practice and study of hiding information. In cryptography a plain intelligible data is converted to unintelligible data and again retransforming the data in its original form. Major attributes [2] provided by application of cryptography are (1) Confidentiality –Information can only be retrieved by a person for whom it is planned and no other person except him can read it. (2) Integrity-Message cannot be reshaped for any wrong means and it is received by appropriate receiver as sent by sender. (3) Non-repudiation- The objective with which a sender is sending information cannot be retraced back at latter stages. (4) Authentication-The sender and receiver of the data are specific, that is, beginning and the end point of data are well defined in cryptography.

In the technological world the information has disguised in the digital form of bits and bytes. On communication channels information now gets stored, processed and transmitted in digital form. Majority of people using digital technology all across the globe are enjoying the use of cryptography daily to secure their data, although they are not familiar they are making its use. Whenever an online purchase is done or while doing bank transactions or sending e-mails cryptography is in action in the background. Without cryptography our modern world will not raise as the important and secret information are open for all [3].

II. BACKGROUND OF CRYPTOGRAPHY

Egyptians first raised the idea of cryptography in around 1900BC [4]. They used the concept of some unusual symbols 'hieroglyph'. The main objective of code was not to hide the message but simply to transmit the messages in dignified form on behalf of the kings. Later, Roman methodology of cryptography termed as 'Caesar Shift Cipher' was adopted by Julius Caesar to communicate with army generals on war front. The approach was based on the concept of shifting the letters of the message by specified numbers; the receipts of the message when then shift back the letters by same and will regain the original protected message. In 1914, Hebern rotating machine created by Edward Hebern was discovered. In this Cipher device first time electrical circuit was adopted. Later on, cryptography played a key role in World War I and World War II. With technological advancements and passing over many stages today cryptography can protect the billions of online transactions, digital signature, computer passwords, sensitive data and private messages.

III. BASIC TERMINOLOGY AND PROCESS OF CRYPTOGRAPHY

Privacy regarding money matter transaction, important information, passwords etc. is a critical issue. In such cases sender has to be sure that message sent by him/her is received only by appropriate receiver, and that too without any type of alteration [5]. In this regard Cryptography is best tool frequently used everywhere in the world for authentic transfer of data. Terminologies [6] used to understand the workings of cryptography are:

1. Plain text: The actual and secret message that sender intends to send to receiver is represented as plain text. This text can be read and understood without any special measures. This text is intelligible data as it is clearly readable. This is the information that we need to hide.
2. Cipher text: The message that cannot be understood by anybody or gibberish text is termed as Cipher text. In cryptography the original message is changed into unintelligible message prior to the communication of actual message. This coded text is only meaningful for the appropriate receiver.
3. Encryption: The mechanism of converting understandable data (plain text) into meaningless data (Cipher text) is termed as Encryption. The process of encryption requires specific mathematical calculations and steps, collectively named as Ciphers. Additionally, with Cipher an encryption key is required to encrypt message. Encipherment takes place at the side of sender.
4. Decryption: Decryption is process for extracting the data that has been encrypted. In this process same Cipher is required to restore the plain text from cipher text. Decryption approach is done on the receiver end to get original message from scrambled message. Typically, the encryption key which is used to scramble the data can descript the data; however, the type of key used depends on the type of cryptography.
5 Key: A key is a number, unique symbol or character. Key is used at the time of Encipherment on the plain text and at the time of decode of cipher text. The proper choice of key is requisite parameter as the privacy of encryption algorithm relies strictly on it.

IV. TYPES OF CRYPTOGRAPHY

Cryptography can be classified into three different types -

1. Symmetric Key Cryptography-Symmetric cryptography [7] or secret key cryptography is the category in which the same key is employed both in encryption and decryption of the message. As the data has to be accessed again all the receipts must be familiar with the same key as used by sender, otherwise the data could not be decrypted by conventional means. The major shortcoming is that two parties that is, sender and receiver should exchange the key in a safe and secure environment. If somehow, third party gets chance to intercept in the secret data will no longer remain secret.
2. Asymmetric key Cryptography –Asymmetric cryptography or public key cryptography [8] utilizes two keys in action. One key is used for encryption and other one is used for decryption. In contrast to symmetric cryptography in asymmetric cryptography if one key is employed to encrypt, the same cannot be used for decryption, other has to be used. One key termed as ‘public key’ is used for encryption and other key termed as ‘private key’ is used for decryption. The private key remains with the owner only, whereas the public key is shared across the network, so that data can be transmitted with the aid of public key. The private key cannot be deduced from the public key but it is possible that the public key can be obtained from the private key. Public key cryptography is advanced and secure form of cryptography.
3. Hash function- Hash function [9] uses no key. It is a mathematical function which transforms the input value which is plain text into unreadable string of text. The input is of random length whereas output is always of definite length. Hash functions are greatly utilized in all information security. .

V. APPLICATIONS

Computer technology [10] has large impact on daily activity of human being and the scenario how the people relate with one other and environment has been drastically affected a lot. With the great advancement in technological field applications in the domain of education, banking, marketing and software has been widened. Cryptography can be regarded as a boon for numerous applications [11]. Almost all the websites use cryptography to tackle their secure data. Hence, cryptography is acting as a shield for protection of private data [12]. Major application incorporate-

1. Digital currency- There is large number of avenues where cryptography has found its place. Most significant being digital currency where crypto currencies are traded over the Internet. Today the world scenario is moving towards cashless economy and digital currencies have grabbed the attention of the world. It is decentralized and secure system. So one can regard that cryptography has been emerged as boon in this direction.
2. Military operations- Since long time back military operation have availed great use of cryptography. The real communication between military officials is kept secret by the use of cryptography so that enemies cannot know regarding the forthcoming strategies.
3. Digital signature- A mathematical process involved to confirm the authenticity and integrity of message, software or digital document.
4. Secure chatting services-Messaging applications like WhatsApp make use of cryptography, which ensures that no other person except the sender and receiver can read the message. Cryptography has provided safe and secret platform for communication.
5. Safe online banking-Cryptography has paramount application in the banking sector. Because of cryptography protective monetary transactions has been possible. Safe and secure use of ATM card is also possible due to cryptography.

6. E-commerce-E-commerce helps to do online shopping and also to pay online. The passwords set for online transactions are protected by the use of cryptography, no hacker get an approach to do adverse effect on our e-commerce details.

VI. CONCLUSIONS

Cryptography is a tool used all across the globe and with its use we can live in a secure digital world. In this paper review analysis showed that without cryptography, digital trust would not be possible. Mathematical algorithm with proper combination of key can ensure security. Mathematical algorithm changes the data in a gibberish language which is not easy for hackers to decode. Our daily transmission of the data cannot be achieved if cryptography does not exit.

REFERENCES

[1] Gupta R.K. 2020 A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function. European Journal of Molecular & Clinical Medicine, 7(7) 3397-3408
[2] Alemami Yahia, Mohamad Afendee Mohamed, Atiewi Saleh 2019 Research on Various Cryptography Techniques. International Journal of Recent Technology and Engineering (IJRTE), 8(253) 395-405
[3] Esther Jyothi V, Prasad BDCN and Mojjada R.K.2020 Analysis of Cryptography Encryption for Network Security. IOP Conf. Series: Materials Science and Engineering 981(022028) 1-7
[4] Naser S.M. 2021 Cryptography: from the ancient history to now, it's applications and a new complete numerical model. International Journal of Mathematics and Statistics Studies, 9(3) 11-30
[5] Chanana D.2019 Research Paper on Cyber Security & Cryptography. International Journal of Innovative Science and Research Technology, 4(3) 14-15
[6] Singh G., Kumar P., Taneja N. and Kaur G.2019 A Research Paper on cryptography. International Journal For Technological Research In Engineering, 7(4) 6266-6268
[7] Abinaya M..2019 Analysis of Cryptography and its Types. IJESC, 9(6) 23036-23039
[8] Anjali Krishna A and Manikandan L.C 2020 A study on cryptographic techniques International Journal of Scientific research on computer science, Engineering and Information technology, 6(4) 321-327
[9] Swathi E., Vivek G. and Sandhya Rani G.2016 Role of Hash Function in Cryptography. International Journal of Advanced Engineering Research and Science (IJAERS) Special Issue (NCCSIGMA-16) 10-13
[10] Nadeem M., Arshad A., Riaz S., Wajiha Zahra S. Dutta A.K. and Almotairi S 2022 A secure architecture to protect the network from replay attacks during client-to-client data transmission. Appl.Sci. 12, 8143 1-18
[11] Shreyas M. , Sudarshan U. B. ,Verneker R., Ankitha S. and Sayeesh 2022 A Review Paper on Cryptography. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 2(2) 389-395
[12] Sujatha .K, Ramya Devi Kala D. and Rathinam. D 2018 A review paper on cryptography and network security. International Journal of Pure and Applied Mathematics, 119(17) 1279-1284