A Review Paper on Cryptography

Ashutosh Upadhyay, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id - ashutosh.upadhyay@Galgotiasuniversity.edu.in

Abstract*—With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender. Data security guarantees that only the intended recipient accesses our data and prohibits any change or alteration of the data. Cryptography can be described as techniques that encrypt data, based on different algorithms to make the data unreadable to the human eye unless decrypted by the sender's predefined algorithms. A cryptographic system's basic concept is to encrypt knowledge or data in order to achieve secrecy of the information in such a manner that an unauthorized person would not be able to derive its significance.

***Keywords*—Cryptography, Security, Algorithm, Cipher, Decryption, Data Security.**

INTRODUCTION

Cryptography is a method for getting messages private. In Greek the word has a special meaning: "hidden prose." Nevertheless, today, the protection of individuals and organizations is protected at a high level by encryption, ensuring that the information sent is secure in such a way that the designated recipient can access this information. Cryptography can be called, with historical roots, an ancient methodology that is still under progress [1]. Sources date back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics, as well as other facts in the form of ancient Greek secret writings or the famed Caesar cypher of ancient Rome. Billions of people around the globe use cryptography on a daily basis to encrypt data and information, even though most don't know they use it. It is also considered highly vulnerable, since cryptographic structures can be broken due to a single programming or design flaw [2].

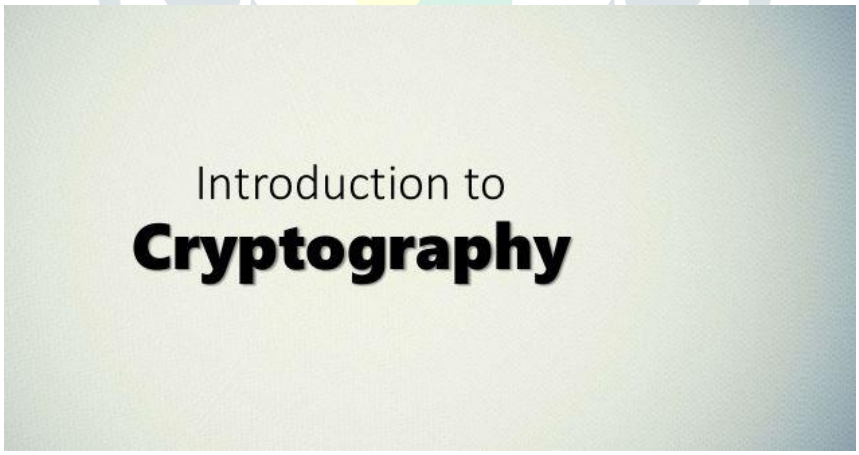

Fig 1. Introduction to cryptography

LITERATURE REVIEW

Susan et al. pointed out that network and computer security is a new and fast-moving technology within the computer science field, with computer security teaching to be a target that never stops moving. Security classes concentrate on the algorithmic and mathematical aspects, such as cryptographic algorithms and encryption [3].When crackers find ways to hack network systems, new courses are developed to address the newest type of attacks, but each of these attacks get old every day due to the new defense software's responses. As the security language begins to evolve, security technologies and capabilities begin to emerge in business practice, network management, computer engineering, and legal

foundation. The key basic concepts, features and purposes of cryptography were outlined by Othman O. Khalifa et al. We addressed that connectivity has contributed to the growth of technology in our era, i.e. the digital age, and therefore has an essential role that requires the security and guarantee of privacy as data is sent through the communication medium. Nitin Jirwan et al. referred to data communication as focusing mainly on digital data processing, where data security is of the highest priority when using cryptography algorithms to ensure that data reaches the intended users safely without sacrificing [4].

et al. mentioned that with the emergence of social networks and commerce applications, huge amounts of data are produced daily by organizations across the world. This makes information security a huge issue in terms of ensuring data is allowed to be transmitted through the network. With more internet users communicating this problem further illustrates the need for cryptography techniques [5]. This paper provides an overview of the different techniques that networks use to improve security, such as cryptography. Anjula Gupta et al. discussed the roots and importance of cryptography, as well as how information security has become a complex topic in computer and communications fields. In addition to demonstrating cryptography as a means of ensuring users ' identity, availability, fairness, authentication, and confidentiality by providing security and privacy, this paper also provides numerous asymmetric algorithms which have provided us the ability to protect and secure data [6].

Undertaken by Callas, J. Discussed issues such as encryption, technology-enhancing anonymity, and legal changes related to cryptography, security and privacy-enhancing technologies. He noted that it is how society uses cryptography that will determine the future of cryptography and relies on legislation, existing laws and customs as well as what society expects it to do. He suggested that there are many holes for potential scholars to fill in in the area of cryptography. In fact, cryptography's future depends on a management system producing strong keys to ensure that access is only open to the right people with the right keys, while others without the keys cannot. Eventually, Callas suggested that people's views and feelings on privacy in defense and correspondence are a mirror of the changes that occur in legislation that come into being through incidents such as the September 2001 terrorist attacks.

Therefore, cryptography will always play a role in the protection of data and information, for now and in the future. James L. Massey points out that there are two purposes that cryptography aims to achieve as they are: reliability and/or confidentiality. He discussed both Shannon's theory of theoretical confidentiality as well as Simmon's theory of theoretical honesty in terms of the protection it affords (which can be either realistic or theoretic). Finally, Schneier argued that the anonymity of defense as a good thing is a fallacy and that confidentiality is not a good thing, because protection that relies entirely on secrecy can be fragile. If that confidentiality is compromised, it would be impossible to recover it. Schneier further explained that cryptography based on short secret keys that can be easily transferred and modified would rely on a basic principle to ensure that cryptographic algorithms are both secure and transparent at the same time in order to provide good security. Accepting public scrutiny is the only effective way to make further safety improvements. Varol,N. ET al.learned symmetrical encryption that is used to encrypt a given text or expression. The material to be authenticated in this analysis is first translated to an encapsulation cipher which cannot be interpreted by a cipher algorithm [7].

A cryptographic system's basic concept is to encrypt knowledge or data in order to achieve secrecy of the information in such a manner that an unauthorized person would not be able to derive its significance. The encoded material is usually called "plaintext" in cryptography, and the method of disguising the plaintext is known as "encryption;" the authenticated plaintext is referred to as "cipher text.' Which is then given along with the details to the encryption algorithm as input. Using a "decryption algorithm," the receiving side can use the correct "decryption key" to get the content.

HISTORICAL ALGORITHMS

A few historical algorithms will be included in this section, along with illustrations of pencils and paper for a nonmathematical reader. Such algorithms were developed and used even before the suggestion was made for a public key cryptography.

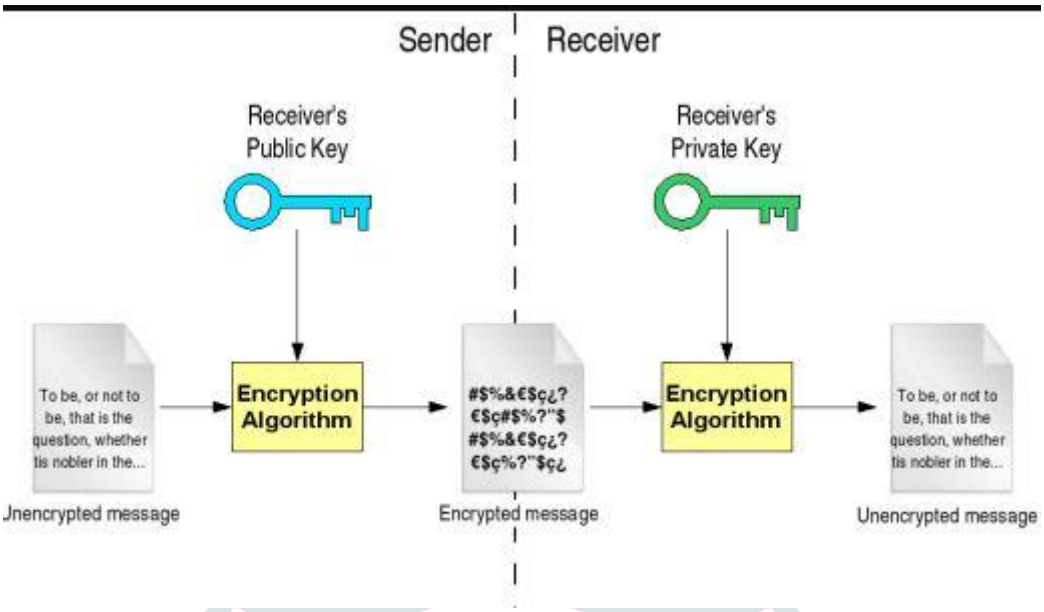

Fig 2. Public Key

Caesar Cipher

This is one of the oldest and early examples of cryptography, invented during the Gallic Wars by Julius Caesar, the emperor of Rome. The letters A through We are encrypted in this form of algorithm by being represented with the letters falling three positions ahead of each letter in the alphabet, while the remaining letters A, B, and C are represented by X, Y, and Z. This means that a "move" of 3 is used although we could achieve a similar effect on the encrypted text by using any of the numbers between 1 and 25. Therefore, a transfer is often seen as a Caesar Cipher nowadays given this vulnerability, Julius Caesar's use of it during his battles may have been good enough in historical times. Although there are still three changed letters in the Caesar Cipher, someone trying to decode the cipher text has only to change the letters to decipher them. Since the Caesar cipher is one of cryptography's easiest examples, it's easy to crack. To decode the cipher text, the letters which were moved are shifted back to their previous positions by three characters [8].

Simple Substitution Ciphers

Take for example the Simple Substitutions Cypher, also known as the Monoalphabetic Cipher. In a Simple Substitution Cipher, we using the letters of the alphabet and place them for random order under the correctly written alphabet. The same key is used in the encryption and the decryption. The encryption rule here is that "the key underneath is replaced by each message," and the decryption rule will be the same. For eg, the corresponding plaintext CAN cipher text is QDN.

Transposition Ciphers

Some cipher families work by ordering the plaintext letters to use a key and a specific law to convert it into cipher text. Transposition can be described as modifying the letters in plaintext by means of rules and a particular key. A columnar transposition figure can be considered as one of the least difficult kinds of transposition figure and has two structures: the first is called "total columnar transposition", while the second is "deficient columnar".". A rectangular shape is used to represent the written plaintext horizontally, regardless of whatever form being used, and its width will equate to the length of the key being used [9].

Public key systems

The development of public key cryptography can be called a cryptographic movement. It is clear that general cryptography and encryption remain restricted to the military and intelligence fields even during

the 70s and 80s. Open key encryption enables us to set up correspondence without relying upon private channels, as the open key can be promoted while never agonizing over it. A rundown of the open key and its highlights follows:

- With the utilization of open key encryption, key dissemination is permitted on open diverts in which the framework's starting sending can be possibly disentangled, facilitating the framework's upkeep when gatherings join or leave.
- Open key encryption restricts the need to store numerous mystery keys. Indeed, even for a situation where all gatherings need the capacity to build up secure correspondence, each gathering can utilize a protected design to store their own private key. The open keys of different gatherings can be put away in a non-secure design or can be acquired when required.
- On account of open conditions, open key cryptography is increasingly reasonable, particularly when parties that have never interfaced beforehand need to impart safely and associate. For instance, a trader may be able to uncover their open key on the web, and any individual who needs to buy something can get to the open key of the trader as essential when they need their Visa data encoded.

DIGITAL SIGNATURES

In contrast to cryptography, advanced marks didn't exist previously the innovation of PCs. As PC correspondences were presented, the need emerged for advanced marks to be talked about, particularly in the business situations where numerous gatherings happen and each must focus on keeping their assertions as well as proposition. The subject of unforgeable marks was first talked about hundreds of years back, aside from those were written by hand marks. The thought behind advanced marks was first presented in a paper by Diffie and Hellman titled "New Bearings in Cryptography"[10]. Therefore, in a case where the sender and receiver do not trust each other fully, authentication alone cannot fill the gap between them. In a manner similar to the handwritten signature, something more is anticipated, i.e., digital signature.

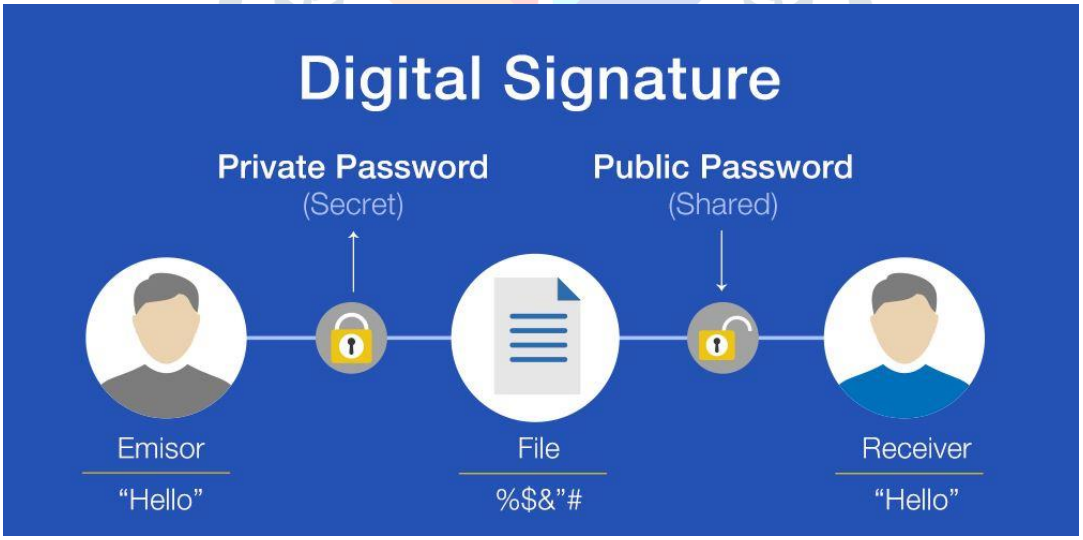

Fig 3. Digital Signature

CONCLUSION

A device thus designed in this paper contains temperature, blood pressure or oximeter sensor for measuring the temperature, pulse rate and oxygen level in the blood. These data are then processed by the controller and are transmitted from node to gateway and further to cloud. If any vital sign or symptoms are recorded in the human body, the concerned doctor or the contacts of that person is informed regarding the emergency through SMS. The paper focuses on system with low power and is immune to noise with long range transmission of power.

REFERENCES

[1] W. J. Buchanan, *Cryptography*. 2017.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, 2002, doi: 10.1103/RevModPhys.74.145.

[3] J. D. Franson and B. C. Jacobs, "Quantum cryptography," in *Advanced Sciences and Technologies for Security Applications*, 2005.

[4] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. 1996.

[5] D. Ganguly and S. Lahiri, "Cryptography and Network Security," in *Network and Application Security*, 2011.

[6] J. Knudsen, "Java Cryptography," *EDPACS*, 1999, doi: 10.1201/1079/43250.27.4.19991001/30275.5.

[7] W. M. H. Company, "Modern Cryptography: Theory and Practice," *Theory Pract.*, 2003.

[8] S. Robinson and S. Robinson, "Understanding Cryptography," in *Expert .NET 1.1 Programming*, 2004.

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, 2014, doi: 10.1016/j.tcs.2014.05.025.

[10] *Practical Cryptography*. 2014.