www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 02, February 2023, pp : 281-283

e-ISSN : 2583-1062

Impact Factor : 5.725

SURVEY ON CRYPTOGRAPHY

Mrs.M.Kundalakesi[1], Lavanya.A[2], Jay Ragavendra.G[3]

[1]Assistant Professor, Department Of Computer Application, Sri Krishna Arts and Science College, Coimbatore, India.

[2,3]BCA Students, Department Of Computer Application, Sri Krishna Arts and Science College, Coimbatore, India.

ABSTRACT

Data security ensures that only the intended recipients have access to our information and prohibits any data modification or manipulation. Various techniques and approaches have been developed to reach this level of security. Cryptography is a set of techniques for encrypting data using specified algorithms that render the data unreadable to the naked eye unless decrypted using predefined procedures by the sender.

Keywords: Krypto, Plaintext, Prompt, Confidentiality, Digitalsignatures.

1. INTRODUCTION

The Art of Cryptography was hatched along with the Art of Writing. The starting point of Cryptography was found in Roman and Egyptian civilizations. Human beings got organized into tribes and kingdoms when civilizations begun to evolve[1]. Hieroglyph is the oldest cryptographic technique. It prevents from malicious third parties from retrieving information.

2. METHODOLOGY

CRYPTOGRAPHY:

Cryptography is derived from a Greek word krypto which means Hidden, Graphy means Written[2]. Cryptography is a secure means of communication from the third party called Adversaries.

Secure communications means the data and information shared with two parties cannot be accessed by the third party. Consider two parties Jack and Bob. Jack wants to send message m to Bob over a secure channel. The Sender's message or sometimes called Plaintext, which is converted into an unreadable form using a key K. The resultant text obtained is called the Ciphertext. The process is known as Encryption. When receival is happening, the ciphertext is converted back into the plaintex t using the same key K, so that it can be read by the receiver. This process is known as Decryption.

CRYPTOGRAPHY TECHNIQUES:

Cryptography and cryptology, as well as cryptanalysis[3], are closely linked subjects. Techniques such as microdots, combining words with visuals, and other methods of concealing information in storage or transit are included. However, in today's computer- centric world, cryptography is most commonly linked with scrambling plaintext (regular text, also known as cleartext) into ciphertext (a process known as encryption), then back again (known as decryption).

Cryptographers are professionals who work in this sector.

ENCRYPTION:

Encryption is a type of cryptography that makes data unintelligible in order to protect its confidentiality. Encryption is the process of disguising data or information in such a way that it looks random to authorised users but is inaccessible to unauthorised users. It refers to the process of converting a plaintext message into an encrypted message (referred to as ciphertext)[4].

Encryption converts plaintext to ciphertext, and decryption converts ciphertext to plaintext. Encryption works by encrypting data with an algorithm and decrypting it with a secret Key.

DECRYPTION:

Decryption is the process of converting encrypted data back to its original form. In most cases, it's a reversal of the encryption process. Because decryption requires a secret key or password, it decodes the encrypted information so that only an authorised user can decrypt the data. Privacy is one of the benefits of implementing an encryption - decryption system.

Because information goes across the Internet, it's important to check for unauthorised organisations or individuals. As a result, the data is encrypted in order to prevent data loss and theft [5]. Text files, photos, e-mail messages, user data, and directories are just a few examples of encrypted stuff. The decryption receiver receives a prompt or window asking

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 02, February 2023, pp : 281-283

e-ISSN : 2583-1062

Impact Factor : 5.725

for a password to access the encrypted. The system extracts and convertsthe jumbled data into words and graphics that are understandable not only by a reader but also by a system for decryption. Manual or automatic decryption is possible. It can also be done with a combination of keys or passwords.

Hill cypher Encryption and Decryption, which generates the random Matrix and is fundamentally the power of security, is one of the most important and popular ways of conventional cryptography[6].In Hill cypher, decryption requires the inverse of the matrix. As a result, one issue that arises during decryption is that the Inverse of the matrix does not necessarily exist. The updated Hill cypher method totally eliminates this flaw. Furthermore, this method necessitates the cracker finding the inverse of a largenumber of square matrices, which is a difficult computingtask. As a result, the modified Hill-Cipher approach is both simple touse and tough to break.

TYPES OF CRYPTOGRAPHY:

In general, there arethree sorts of cryptographic procedures.

- Cryptography with symmetric keys.
- Hash functions are thesecond type.
- Cryptography based onpublic keys.

SYMMETRIC - KEY CRYPTOGRAPHY:

A single key is shared by both the sender and the recipient.

The senderencrypts plaintext and sends the cypher text to the receiver using this key.

The receiver, on the other hand, uses the same key to decryptthe message and retrieve theplain text.

PUBLIC – KEY CRYPTOGRAPHY:

The most revolutionary concept in thelast 300-400 years is public- key cryptography. Two related keys (public and private key) are utilised in public key cryptography. Thepublic key can be freely transmitted, but the private key that goes with it must bekept secret. The public key isused for encryption, whereasthe private key is utilised for decryption.

HASH FUNCTIONS:

This algorithm doesnot use a key. The plain text is hashed with a fixed-lengthhash value that prevents theplain text's contents from being recovered. Many operating systems also employ hash algorithms tosecure passwords.

USES OF CRYPTOGRAPHY IN DAILY LIFE:

a. Digital signatures/Authentication

The use of public-keycryptography for authentication and digitalsignatures is particularly significant For example, if you receive a message from me that has been encrypted using my private key and canbe decrypted with my publickey, you can be relatively assured that the message was send by me.

If I believe itis vital to keep the communication private, I may encrypt it with my private key and then decryptit with your public key,so that only you can read it and you will know it originated from me. The only stipulation is that public keys are linked to their owners in a secure manner, such as through atrusted directory.

b. Time stamping:

Time stamping is ameans of certifying that a valid digital report or communication exists or wasaltered at a valid time. Time stamping employs a blind signature system, which is a type of encryption. Blind signature techniques allow the sender to have a message acknowledged by another party without giving any information about the message to the other party. Time stamping is similar to sending a registered letter through the US mail, but it provides an additional level of proof. It can demonstrate that a receiver received a specific report. Patent packages, copyright archives, and contracts are examples of possible packages To be able to assist, time stamping is a necessary tool. Time stamping is an important toolfor assisting in the transition to digital criminal records.

c. Secure Socket Layer:

Secure Socket Layer (SSL) is a public key protocol developed by Netscape provide information security layered between TCP/IP (the foundation of Internet-based global communications) and alerting protocols (together with HTTP, Telnet,

NNTP, or FTP). For TCP/IP communications, SSL aids data encryption, server authentication, message integrity, and patron authentication.

3. CONCLUSION

We use distinct sorts of algorithms to establish security offerings in exceptional service mechanisms. We use both non-public key cryptography or public key cryptography in accordance to requirement. If we choose to send message shortly we use non-public key algorithm and if we prefer to ship messages secretly we use public key algorithm.

4. REFERENCES

[1] Esslinger, Bernhard, et al. TheCryp Tool Script: Cryptography, Mathematics, and More. 11th ed.

[2] .Hoffstein, Jeffrey, Jill Pipher, Joseph H.Silverman. An Introduction toMathematical Cryptography. 2nd ed.

[3] katz, Jonathan, and Yehuda Lindell. Introduction to Modern Cryptography. 2nd ed. Boca Raton:CRC, 2015.

[4] Menezes, Alfred J., Paul C. van Oorschot, and Scott A.Vanstone. Handbook of Applied Cryptography. Boca Raton: CRC, 1996.

[5] T.Neiderreiter, Harald, and Chaoping Xing. Algebraic Geometry in Coding Theory and Cryptography. Princeton: Princeton UP, 2009.

[6] Paar, Christof, and JanPelzi. Understanding Cryptography: A Textbook for Students and Practitioners. Heidelberg: Springer,2010.