International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Secured Commutation Through Fibonacci Numbers and Unicode Symbols

Mohini Gaikwad , Sagar yashvantrao, Bharat kathore
Vishwatmak Om Gurudev College of Engineering, Aghai, Mohili, Maharashtra, India

ABSTRACT
Today's life every person is deeply connected to the internet, many peoples are mostly used the social media to connect each other. Through the social media many peoples are shared there data such as image file, text file, pdf file, but there is no guarantee that the shared data are secured, that's why we going to developed the advanced security project. For such a type of security we select the cryptography for secure communication and data transferred. The objective of cryptography is to make it Possible for two persons to exchange a message in such a way those other persons cannot understand. There is no end to the number of ways this can be done, but here the proposed method will be more concerned with a technique of encoding the text in such a way that the recipient can only discover the original message. The original message usually called plain text is converted into cipher text by finding each character in the message and replacing it with another character based on the Fibonacci number generated. Further cipher text is converted into Unicode.

I. INTRODUCTION

In current situation, the major problem is security, security companies and systems expend cryptography to channelize information around the Internet. from the down side citizen people the highly networked so-cities that we live in today, communication has always been an integral part of our existence. What started as simple sign communication centuries ago have evolved into many forms of communication today, the internet being just one such example. Methods of communication today include radio communication, telephonic communication, network communication and mobile communication. But all of these communication is not as much secure All these communication channel plays the important role in our day to day life but in the past few years, network communication, has not secure as much we wanespecially over the internet, has emerged as one of the most powerful methods of communication with an over-whelming impact on our lifeCryptography involves creating written or generated codes that allows information to be kept secret Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the dataInformation security uses cryptographyonseveral levels. Thdn symbols, which avoid suspicion from the third party when send through an unsecured communication channel.There are two levels in the proposed system(i) converting plain text to cipher text and (ii) converting cipher text to Unicode symbols. In each each character in the message and replacing it with another character based on the Fibonacci number generated. Further cipher text is converted into Unicode symbols, which avoid suspicion from the third party when send through an unsecured communication channel. There are two levels in the proposed system; (i) converting plain text to cipher text and (ii) converting cipher text to Unicode symbols. In each level, security key is used

to encode the original message which provides two levels of security from intruders. On the other end, the extraction algorithm is designed in such a way that the process converts the Unicode symbols into cipher text and then cipher text to plain text. This encoding and decoding scheme of the proposed method is significantly different as compared to the traditional method information cannot be read without a key to decrypt it. The information maintains its integrity during transit anwhile being stored. Cryptography also aids in non-repudiation. This means that neither the creator nor the receiver of the information may claim they did not create or receive it.

II. CRYPTOGRAPHY

Cryptography is the best way to encryption and decryption your message and makes the secure communication and avoid the interruption of third party or unauthorized user. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers. Modern cryptography concerns itself with the following four objectives:

1. **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)
2. **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3. **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information

2.1. Encryption Method

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the

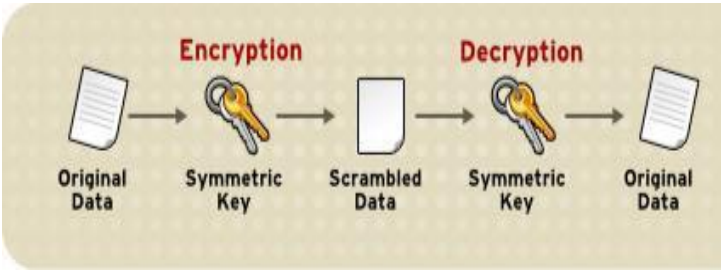

Figure 1.(a) encryption

B. Decryption Method

process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption.

With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a key that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes.

The sections that follow introduce the use of keys for encryption and decryption.

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

Steps For Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information.

1. Symmetric-Key Encryption-

In security we r going to use the various types of cryptography,in that we can use the symmetric key cryptography which help us to provide only one user key

2. Public-Key Encryption-

as a name suggest this is a public key cryptography which can provide the two types of key,that two key must be have to the receiver and sender side using that two key the system will done the encryption and decryption algo

3. Key Length and Encryption Strength:

key length is the major part in our project.the most important thing in our project is key so we should put such a type of key which the third party can not get intrrupt

2.3 Flowchart

in a flowchart we r going to going to explain how our system work it shows the totally description about hole the project.in that it shows the working of two people how they can access thaeir message the two people can be play the important role about their project the one person from the sender side n other one is receiver side.

III. CONCLUSION

We are studied the total security for communication, which need for easily share the data to other user without interrupt third person We can make the total file encryption and decryption techniqueFor secured communication

IV. REFERENCES

[1]. Dr. V. Sundaram, "Secured Communication through the Fibonacci Numbers and Unicode Symbols" International Journal & Engineering Research, Vol. 3, Issue 4, April 2012, pp. 490-494. Ahmad Abusukhon, Mohamad Talib, Issa Ottoum, "Secure Network Communication Based on Text - to - Image Encryption

[2]. Syed Khutubuddin Ahmed Khadri, Debabrata Samanta Mousumi Paul, "Approach of Message Communication Using Fibonacci Series: In

Cryptology", Engineering and Technology Publications", Vol. 2, No. 2, June 2014, pp. 168-171.

[3]. Raghu M.E., Ravishankar K.C., "Application of Classical Encryption Techniques for Securing Data - A Threaded Approach"

[4]. Raghu M.E., Ravishankar K.C., "Application of Classical Encryption Techniques for Securing Data - A Threaded Approach"