ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May2017

A Survey on Secure E-mailing System with Cryptography Using Fibonacci Series

Abdul Quader Quazi[1], Pavan Y. Maddikar[2] , Kiran K. Tangod[3]

B.E. Students, Dept. of Information Science, GIT, VTU University, Udyambag, Belagavi, Karnataka, India[1,2].

Assistant Professor, Dept of Information Science, GIT, VTU University, Udyambag, Belagavi, Karnataka, India[3]

ABSTRACT: Cryptography enables exchange of messages between two entities and prevents unauthorized access to the message. There are many different ways of performing this exchange; hereby we propose a technique of encoding the text so that the receiver can retrieve the original message. The contents of original message are changed to the cipher text by taking each character from the message and converting it with character based on the Fibonacci number generated. Further, the cipher text is converted into the Unicode symbols. This avoids suspicion from the third Party when data is sent through this Emailing System on Cloud Channel. This Emailing System varies from traditional Mailing System in encryption and decryption of text message without bothering about sending and remembering about the key to both participating entities.

KEYWORDS: Cipher text; Decryption; Encryption; Fibonacci number; Key; Plain text; Unicode Symbols

I. INTRODUCTION

CRYPTOGRAPHY is an ancient technique back from thousands of years used to exchange information between two people without any intrusion .This was achieved with the help of ciphers. The cipher text is encrypted information which cannot be read by any other intruder without the key. Early 20th century witnessed the invention of mechanical as well as electromechanical machines but encryption technique in modern world is achieved by using algorithms that uses a key to encrypt and decrypt the information. Cryptography is a scientific technology that uses complex mathematics and logics to design strong and efficient encryption methods. It is important in now a day as it allows people to keep confidence on electric channel without worrying of deceit and deception. In present world millions of people interact electronically each and every day through mediums like e-mails, telephonic communication and many more. The rigorously increase of information transmitted electronically resulted to an increased reliance on cryptography and authentication.

In cryptography, Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. In this, the written information or message, referred as plaintext, is converted into cipher text which is known as encrypted text using an encryption algorithm, generating a cipher text that can only be read if decrypted using a proper key.

In our proposed system the original message usually called plain text is converted into cipher 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 symbols, which is sent to recipient on a cloud.

There are three levels in the proposed method; (i) Secured login to the emailing system (ii) Converting plain text to cipher text and (iii) Converting cipher text to Unicode symbols.

In the all levels security key is used, to enter into emailing system, to encode the original message which provide 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. The encoding and decoding of the proposed method is significantly different as compared to traditional methods.

II. RELATED WORK

In [1] Authors method 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 symbols, which avoid suspicion from the third party when send through an

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

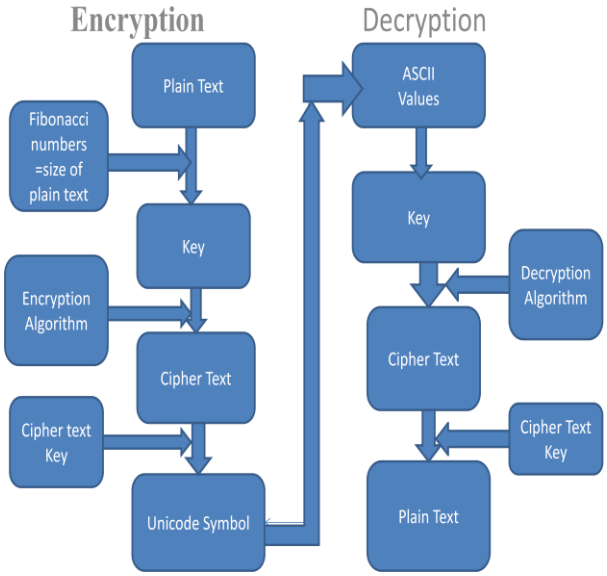
International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May2017

unsecured communication channel. There are two levels in the proposed method; (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. This encoding and decoding scheme of the proposed method is significantly different as compared to the traditional methods. In [2] Authors method The Cryptography enables two persons to exchange a message so that unauthorized persons cannot access the original message. There are many different ways of performing this exchange, but the method hereby proposed a technique of encoding the text so that the receiver can retrieve the original message. The contents of original message or the plain text are converted into the cipher text by searching each character in the message and interchanging it with character based on the Fibonacci number generated. Further, the cipher text is converted into the Unicode symbols. This helps avoid from the third party when data is send through an unsecured communication channel. This proposed method is different as compared to the traditional security methods. In [3] Authors approach of cryptography is to make it feasible for more than one person to do secure communication without intrusion. In the process of sending messages, security of the message is an important challenge as the messages are more vital or secret and protecting data stored in and transferred between distributed components from unauthorized access is very important. Cryptography provides various ways to safe guard messages 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 without any data loss or without any alteration or data getting leaked. In this paper highlights the problem and provides some possible approach to solve this problem using Fibonacci series. The Encryption of data is done by combining the original data with Fibonacci numbers to get a Cipher text which is non-understandable to any intruder. Only the receiver knows the logic to do so. In [4] Authors the developed techniques for securing data to avoid hacking as well as providing the user with some additional features such as key for integrity and validation of user. The proposed encryption/decryption algorithm is loss-less, key-dependent. The performance of the popular symmetric key algorithms including DES, 3DES, AES, Blowfish are compared with Fibonacci Series encryption/decryption by encrypting input files of varying contents and sizes

III. PROPOSED ALGORITHM

Description of the Proposed Algorithm:

Aim of the proposed algorithm is to improve the Emailing Security and minimizing the threat of intrusion by Fibonacci Series Encryption using Unicode Symbols.The following figure shows the encryption and decryption process.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May2017

Encryption Method

In this proposed method, the original E-Mail message is called plain text which is converted into cipher text with the help of Fibonacci number generated. Here, each character is extracted from the original e-mail message and replaced with another character, the way the characters are chosen to replace the original character makes this method unique and different when compared to the traditional methods. The obtained Cipher text is converted into Unicode symbols, and these symbols are stored in the text file along with the key hidden in Unicode symbols which cannot be seen in the encrypted message and sent to the cloud server. Since the encrypted e-mail message is sent to the cloud server it makes intrusion more complex as this provides a 2 level encryption. The conversion of plain text to Unicode symbols undergoes two phases namely; converting plain text to cipher text and converting cipher text to Unicode symbols.

Steps involved in Encryption

1. A sender sends a plain text message to a recipient.
2. The original message is converted into cipher text by using an automated key and Fibonacci numbers equal to the plain text characters. The algorithm being used can produce a different output each time is used, based on the key generated.
3. Cipher text is converted into Unicode symbol using another key from the predefined Unicode symbols table and the key is hidden in the Unicode symbols which cannot be seen by any one.
4. The Unicode encrypted text is transmitted over a cloud network, and encrypted data will be stored in cloud.

Decryption Method

The decryption process follows the reverse process of encryption with the help of two keys. At the recipient end, from the received encrypted text file each symbol is extracted and mapped in the predefined Unicode symbol table to find the equivalent decimal value, further the obtained value is taken to find the plain text using the key. Without the knowledge of the key an intruder cannot predict the existence of any secret messages in the Unicode symbols.

Steps involved in decryption

1. At the recipient end, Unicode symbols are extracted and compared for matching symbols and respective decimal values will be retrieved from the predefined Unicode symbol table.
2. The key is extracted from the encrypted text and perform subtraction with the decimal values and the ASCII code of characters from cipher text
3. After the subtraction the remainder will be the ASCII code of the character which further converted into plain text character.
4. This process is repeated for the number of characters in the cipher text and accumulates the character that forms the original plain text.

IV. ADVANTAGES

1. The proposed method user needs to authenticate user before using this process of securely sending the textual information from sender to receiver, by making the textual message unreadable to any intrusion.
2. The security key is automatically generated for each and every textual message created which removes the burden of user for selecting the key for each message; the key is then used for converting plain text to cipher and from cipher text another key is used to generate Unicode symbols.
3. Another advantage is that the encrypted message is stored in the cloud server which can be accessed by receiver from anywhere with this system
4. The encrypted text is very difficult to decode the Unicode symbol from the text file and information to be conveyed is kept secret

V. CONCLUSION AND FUTURE WORK

Cryptography has become an important issue in modern world of technology where lots of information is transmitted over unsecured channel. The above method refers to symmetrical cryptography. In this paper three levels of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May2017

securities are discussed. This method of E-mailing system secures the information without any difficulties of sending the private key and remembering each private key for each message it is made simple and easy use for the users to encrypt and decrypt on a cloud server. The proposed system is better, secure and efficient from all the traditional systems. The system in the near future is planned to send attachments that include big file size like pdfs, .doc, .docx documents, images, videos and other file formats.

REFERENCES

1. Secured Communication through Fibonacci Numbers and Unicode Symbols, International Journal of Scientific & Engineering Research, A . Joseph Raphael & Dr. V. Sundaram. Volume 3, Issue 4, April-2012 1 ISSN 2229-5518 4
2. Data Encryption through Fibonacci Sequence and Unicode Characters, MIT International journal of computer Science and Information technology, Prachi Agarwal, Navita Agarwal & RichaSaxena, Vol. 5, No. 2, August 2015, pp. 79-82 79 ISSN 2230-7621©MIT Publications
3. Approach of Message Communication Using Fibonacci Series: In Cryptology, Lecture notes on Information Theory Vol.2 ,No 2,June2014 Syed Khutubuddin Ahmed Khadri Dept of MCA, REVA Institute of Technology & Management, Bangalore, India Debabrata Samanta Dept of MCA, Acharya Institute of Technology, Bangalore, India Mousumi Paul Dept of CSE, National Institute of Technology, West Bengal, India
4. The Information Security Using Fibonacci Series, International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India B. S.Tarle & G. L. Prajapati
5. Michael Blaha, James Rumbaugh, Object Oriented Modelling and Design with UML, Pearson Education, 2nd Edition, 2005.
6. I.Venkata Sai Manoj, Cryptography and Steganography, Interna-tional Journal of Computer Applications (0975 – 8887), Volume 1 – No.12
7. Sashikala Channalli and Ajay Jadhav, Steganography An Art of Hiding Data, International Journal on Computer Science and Engi-neering Vol.1(3), 2009, 137-141 .
8. Dipti Kapoor Sarmah, Neha bajpai, Proposed System for Data Hid-ing Using Cryptography and Steganography, International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010
9. B.B. Zaidan, A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, On the Differences between Hiding Information and Cryptography Tech-niques: An Overview, Journal of Applied Sciences (2010), ISSN 1812-5654
10. http://media.wiley.com/product_data/excerpt/94/07645487/0764548794.pdf, Chapter 1, Basics of Cryptography

BIOGRAPHY

Abdul Quader Quazi is a Student in the Information Science Department, KLS Gogte Institute of Technology, Affiliated VTU University. He is pursuing Bachelor of Engineering (B.E) degree from GIT, Belgavi, and Karnataka, India. His research interests are Cryptography, Algorithms, etc.

Pavan Y Maddikar is a student in KLS Gogte Institute of Technology, Affiliated to VTU University, studying Information Science and Engineering. He is pursuing Bachelor of Engineering (B.E) degree from GIT, Belgavi, state: Karnataka, India. His research interests are Cryptography, Web Technology

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May2017

Prof Kiran K Tangod is presently working as Assistant Professor in Department of Information Science & Engineering, KLS Gogte Institute of Technology and has teaching experience of 15 years, he has obtained his masters in Computer Network Engineering from VTU Belgavi and bachelors from Karnatak University Dharwad. His research area is distributed data-ming and secured communication**.**