RESEARCH ARTICLE OPEN ACCESS

CRYPTOGRAPHIC TECHNIQUE FOR COMMUNICATION

Dr. Aradhana. D*, Chaithra. V. N**, Evelyn Arpitha Joseph***, Gouri Pooja. H. M****

*(Professor Department of Computer Science of Engineering, , Bellari Institute Of Technology And Management, Bellari
Email: aradhanabm@gmail.com)

** (Computer Science Of Engineering, Bellari Institute Of Technology And Management, and Bellari.
Email: chaithrashree100@gmail.com)

*** (Computer Science Of Engineering, Bellari Institute Of Technology And Management, and Bellari.
Email: arpjoseph6399@gmail.com)

**** (Computer Science Of Engineering, Bellari Institute Of Technology And Management, and Bellari.
Email: gourihm05659@gmail.com)

--*************************-----------------------------------

Abstract:

Cryptography provides for secure communication in the presence of the malicious third party or adversaries. In present world, the sensitive data are increasingly used in communication over the internet. Thus security of data is the biggest concern of internet users. Best solution is use of some cryptography algorithm which encrypts data in some cipher and again decrypted to original data. The field of cryptography deals with the procedure for conveying information securely. The encryption uses an algorithm and a key to transform an input that is plain text into an encrypted output that is the cipher text. The algorithms recently used for cryptographic communication are digital signature algorithm, hash function, MD5 algorithm, SHA-256, RSA algorithm etc. where the drawbacks of these algorithms are RSA has too much of computation, as it uses more prime numbers which is complex in factorization. MD5 is the message digest algorithm where it can be broken relatively easy and is no longer suitable for secure systems. This project we use two algorithms they are vigenere and polybius algorithm. Vigenere cipher is a method of encrypting alphabetic text. It uses a simple form of poly alphabetic substitutions. Thus, lightweight cryptography methods combined to form Complex and secure Hybrid Cipher is proposed to overcome many of the problems of conventional cryptography.

.

Keywords — **Cryptography, Encryption, Decyption, vigenere cipher, Polybius cipher.**

--*************************-----------------------------------

I. INTRODUCTION

In the present direction of the world, the innovations have progressed so much that the vast majority of the people incline towards utilizing the internet as the essential intends to consign the data starting with one end then onto the next over the world. There are numerous potential approaches to communicate data utilizing the internet: through messages, talks, and so on. In any case, one of the primary tests with sending data over the internet is the "security risk". For example, the individual or private data can be hacked through various methods. In this way, it turns out to be essential to mull over data security, as it is one of the most vital variables that need consideration during the process of data transfer. Security is a significant factor in the open system. Cryptography assumes a significant job in this field. Cryptography is old and made sure about the system of information out but, overtime problem in the open system. Cryptography is a term defined as encrypting and decrypting the data, which is to be protected. Cryptography is a systematic technique and procedure to hide the data and information over a communication channel. As the innovation grows step by step the need for data security over the communication channel is expanded to a high degree. Encryption is defined as a systematic procedure of changing over plain message text into cipher text. Encryption process needs any programmed encryption algorithm and a key to change over the plain message text into cipher. In the cryptography system encryption execute at the message sender side. Encryption executes the message at sender's side before sending it to the receiver. Decryption is an opposite systematic procedure of encryption. It transforms the encrypted cipher text into a message plaintext. In cryptography system decryption procedure execute at the receiver side. The process of decryption algorithm requires a couple of steps such as Decryption algorithm and a key. Cryptography is extensively isolated into two classes relying on the Key, which is characterized as the guidelines used to change over a unique book into scrambled content.

II. PROBLEM STATEMENT

To develop a system of encryption scheme that provide decryption of original data which conveys information securely for users.

III. OBJECTIVES

- To encrypt the privacy data of the recipient.
- To decrypt the data at the receiver which is encrypted by the recipient.
- To implement a data which is converted from the readable message to secret code.
- To design a developing system which will decure the data transfer.

IV. LITERATURE SURVEY

I. DESIGN OF HYBRID CRYPTOGRAPHY ALGORITHM FOR SECURE COMMUNICATION.

Authors: Arpit Agrawal, & Gunjan Patankar Published in: Jan-2016.

Following algorithm will be used to develop hybrid security model. Diffie-Hellman Key Exchange Algorithm are RSA algorithm for Confidentiality, Private Key Encryption for Authentication, SHA-1 for Integrity, RC5 to provide confidentiality over cipher text and message digest. There is no special memory requirement of proposed solution. A basic memory requirement of java application is recommended. Encryption and Decryption will be the leading operations of the proposed solution. Subsequently, calculation of SHA-1[MAC] and SHA1[MAC] verification process is also. The study of the conventional system concludes that there is big scope of improvement in security policy of highly security expected applications. The complete work concludes that proposed solution will give an alternative security model than SSL and digital envelop to maintain security in intranet. SSL require HTTPs protocol, where proposed solution does not require any kind of protocol.

II. AN EFFICIENT DEVELOPED NEW SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM FOR INFORMATION SECURITY.

Authors: SuyashVerma , Rajnish Choubey, Roopali soni. Published in: July 2012.

Security is the important factor in the public network and cryptography play an important role in this field. Cryptography is very old and secured technique of information in public network. However, the objective of cryptography is used not only to provide confidentiality, but also to provide solutions. Basically this paper is proposing a new encryption algorithm. Because it known that, any type of information requires more effort during encryption and decryption. Proposed algorithm will enhanced efficiency of encryption/decryption algorithm as compare to existing algorithms. This algorithm uses symmetric key technique for encoding and decoding of data i.e. it uses the same key at both ends. It protects the cipher text from Brute-force attacks as the key length is 128 bit in the encryption process. The proposed encryption algorithm has been designed in a beneficial approach but of-course not sacrificing the security issues. It will be successfully implement on the various type of data. We have also tried to benchmark the performance of proposed encryption algorithm against some selected algorithms.

III. A MODIFIED VERSION OF POLYBIUS CIPHER USING MAGIC SQUARE AND WESTERN MUSIC NOTES

Authors: Moumita Maity

Published in: June-2014.

In this section, a brief introduction is provided on Polybius cipher, western music notes and magic square those are used to design the proposed system. Cryptographic protocols deal with the application of cryptographic algorithms. Symmetric and asymmetric algorithms are the building blocks with which applications such as secure internet communication can be established. All Cryptographic algorithms are based on two general principles: [3] substitution, in which each element in the plaintext (bit, letter, and group of bits or letters) is mapped into another element and transposition; the elements of the plaintext have simply been re-arranged in different order position with relation to each other has been changed. In the proposed system a unique 6x6 magic square and heptatonic increasing C major scale C–D–E–F–G–A–B is used for encryption. First any unique 6x6 normal magic square is taken which is arranged with integers from 1 to 36. Next all the alphanumeric characters are placed like this: as A is first letter, it is placed in cell with digit 1, second letter B in the cell with digit 2 and so on. A-Z is placed in the cell numbered 1 to 26. Likewise 0-9 is placed in cell with number 27 to 36 respectively. Each time the arrangements of integers in magic square are changed, the arrangements of characters are also different. Hence for every substitution, each single character would have different types of codes. The order of alphanumeric characters are very difficult to guess as there are 1.77x1019 possible 6x6 normal magic squares any of which can be chosen during key selection.

IV. AN ENHANCED VIGINERE CIPHER FOR DATA SECURITY.

Authors: Aized Amin Soofi, Irfan Riaz, Umair Raseed.

Published in: March 2016.

There are many aspects to security and applications, ranging from secure commerce and payments to private communications and protecting passwords. Cryptography is an essential aspect for secure communications [2]. Although the crucial goal of cryptography is to hide information from unauthorized individuals, most algorithms can be broken and the information can be exposed if the attacker has enough time, desire, and resources. In traditional Vigenere cipher each alphabet has one fixed numeric value but in our proposed technique we have eight tables. In each table every alphabet represent with different numeric value. In traditional Vigenere technique the plaintext is considered as a sequence of alphabets without any space between them. It may create a problem for receiver to read the message by inserting spaces between words and receiver needs to guess the exact place to insert space in decrypted plaintext. To overcome the limitations of Vigenere cipher we proposed an enhanced version of Vigenere cipher that is much secure against Kasiski and Friedman attacks. Cryptanalysis, frequency analysis, pattern prediction and brute attack on proposed technique are also much difficult due to use of multiples tables for encryption. Although there are many cryptographic methods but this domain still requires serious attention of research community for the improvement of data security.

V. A REVIEW PAPER ON CRYPTOGRAPHY.

Authors: abdalbasit Mohammed Qadir & Nurhayat Varol.

Published in: June 2016.

Cryptography is a technique to achieve confidentiality of messages. The term has a specific meaning in Greek: "secret writing". Nowadays, however, the privacy of individuals and organizations is provided through cryptography at a high level, making sure that information sent is secure in a way that the authorized receiver can access this information [1]. With historical roots, cryptography can be considered an old technique that is still being developed. Examples reach back to 2000 B.C., In this section, a few historical algorithms will be introduced, along with pencil and paper examples for a nonmathematical reader. These algorithms were designed and used long before public key cryptography was proposed. Cryptography has the important purpose of providing reliable, strong, and robust network and data security. In this paper, we demonstrated a review of some of the research that has been conducted in the field of cryptography as well as of how the various algorithms used in cryptography for different security purposes work.

V. METHODOLOGY

MODE – Sender and receiver as to choose the mode. Initially, sender has to choose the encode mode and the receiver has to choose the decode mode and it takes to the encryption and decryption mode respectively.

ENCRYPTION (at sender) – the encryption is the module where in the sender has to encode the message that need to be sent to the receiver.

DECRYPTION (at receiver) – the decryption is the module is the where in the receiver has to decode the message that is received from sender.

The strategy utilizes a combination of Vigenere cipher ` and Polybius Square Cipher in its encryption process. The cipher text will initially be worked on utilizing Vigenere cipher. ` A picked key out of arbitrary will start the process. Toward the finish of the process, the subsequent cipher text then turns into a key for the Polybius Square Cipher process. The key is used to work on the message which is the plaintext to create the last cipher text. This process will wind up making the last cipher text progressively hard to be broken utilizing existing cryptanalysis processes. Decryption will be done by the receiver in reverse order for retrieval of a message from the sender. A product program will be composed to exhibit the viability of the calculation utilizing python coding and different cryptanalysis technique will be performed on the cipher text.

A. Encryption Phase 1 (Vigenere Cipher) `
STEP1: MESSAGE - AMERICANVIRUS
STEP2: KEY- DELHI
STEP3: OUTPUT- DQPYQFEYCQUYD
Phase 2 (Polybius Cipher)
STEP4:
TEXT-DQPYQFEYCQUYD
STEP5:
OUTPUT-41145345141251453114544541

We can see output is in a NUMERICAL format where sender has sent as in ALPHABETICAL format. Even the Vigenere cipher result outputs in ALPHABETS which is also secured but again passing that treating Vigenere outputs as Polybius input and then result in numerical format that makes it greater secure and complex than the use of single ciphers.

B. Decryption Phase 1 (Polybius Cipher)
STEP1: MESSAGE- 41
STEP2: OUTPUT- D Phase 2 (Vigenere Cipher) `
STEP3: TEXT- D STEP3: KEY- DELHI
STEP4: OUTPUT-A

We can see decode output is arriving after reversing the process of through first and foremost Polybius cipher and then Vigenere cipher. This makes complexity for intruders, ` attackers and hackers to confuse them and stop them to

Replicate, copy, or harm the system through various attacks.

Hence, we can see the implementation of the Encryption and Decryption process of the Hybrid cipher process that flows systematically through Polybius and Vigenere cipher system.'` Python Program is written as for the Implementation of Hybrid cipher.

VI. RESULT AND DISCUSSION

The system is about encryption and decryption of the data. There are two modes in the system that is encoding mode and decoding mode for the sender and receiver respectively. the sender has to choose the encoding mode to encode the message in the alphabetical input text and then the result of the encoding message will be displayed in the form of numeric as output .this output is understandable the receiver but not for others. in case if the encoding message input is written in numerically first then is an incorrect entry because sender may go wrong while sending message in numeric form. if it is alphabetic then it is easy to know the correct message is encoded after the result of encoding is displayed. Similarly the next part is decryption where the receiver has to decode the message that has been encoded. the encoded message will be numeric form when the result will be in the alphabets. The receiver has to gives the decoding input same as the message that is in the result of encoding in the numeric form only not in alphabet if the alphabetic input is given at the decoding input then it will not accept the input instead displays an error. the system will provide correct result. as it encodes the message by the sender to the receiver and decodes the message by the receiver from the sender.

CONCLUSION

The High level security provided by the encryption key remain secret, the original message remains same. This includes vigenere cipher and Polybius square cipher which results the output of encoding and decoding of ciphers. Cryptography is emerging as the root for enterprise data security and consent, and quickly becoming the prop of security best practice. Therefore the process of securing data or message communication remain secure due to unique security communication as provided by Hybrid Algorithm. At the end we need to protect our attacks.

REFERENCES

[1]. Design Of Hybrid Cryptography Algorithm For Secure Communication By,,"Arpit Agrawal ,& Gunjan Patankar "" Volume: 03, Issue: 01 1323-1326, Jan-2016.

[2]. An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security By "Suyash Verma, Rajnish Choubey, Roopali Soni" Volume:02, Issue 7, July 2012.

[3]. A Modified Version of Polybius cipher using Magic Square and Western Music Notes By " Moumita Maity" Volume:01, Issue 10, June 2014.

[4]. An Enhanced Vigenere Cipher For Data Security By "Aized Amin Soofi, Irfan Riaz, Umair Rasheed" Volume:05, Issue 03, March 2016.

[5]. A Review Paper on Cryptography By "Abdalbasit Mohammed Qadir, Nurhayat Varol" June 2019.

[6]. A Research Paper on New Hybrid Cryptography Algorithm By "Prof. Swapnil Chaudhari, Mangesh Pahade , Sahil Bhat , Chetan Jadhav ,Tejaswini Sawant" Volume:09, Issue 05, May 2018.

[7]. Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique By "Vittal Kumar Mittal, Manish Mukhija" Volume:03, Issue 05, August 2019.

[8]. NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment By "Ali Abdulridha Taha, Dr. Diaa Salama AbdElminaam, Prof.Dr. Khalid M Hosny" Volume:08, Issue 11, 2017.

[9]. A Cryptosystem Based On Vigenere Cipher By Using Mulitlevel Encryption Scheme By "Sanjeev Kumar Mandal, A.R Deepti" Volume:07, Issue 04, 2016.

[10]. Polybius Square in Cryptography: A Brief Review of Literature By "Jan Carlo T. Arroyo, Cristina E. Dumdumaya, Allemar Jhone P. Delima" Volume:09, Issue 03, June 2020.