International Journal of Engineering &Technology, 7 (1.7) (2018) 152-155

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An efficient cryptographic scheme for text message protection

Manikandan N K[1*], Manivannan D[2], Antony kumar K[3]

[1,2,3]*Assistant Professor,*
Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India.
**Corresponding author E-mail: manikandan1488@gmail.com*

Abstract

Interchange of information is increasing very rapidly. Transferring any information on internet arises with the biggest issue that is security. Cryptography plays an important role in achieving security. For any type of business our primary focus is mainly on the security of information for that we require a robust and unbreakable process that provides great safety. This project is concerned with the development of a secure messaging system based on cryptographic algorithm that is which is more faster, better immune to attacks, more complex, easy to encrypt. This is well featured and provides encryption/decryption that can protect message from unauthorized access. we proposed an algorithm, which uses triple keys for encryption and decryption of text to secure the information. This application is well featured and provides security that can protect message from unauthorized access. To send a message, a sender types and encrypts a text message using Three Keys algorithm with a key selected from keylist .The encrypted message is stored in database and receiver's inbox serial number of key .The receiver, after logging into account ,selects key value and then decrypts with key to see the original message

Keyword: *Cryptography,Text message,Protection of Message*

1. Introduction

The main aim of this group work is to develop a security concept for communication. Our security concept takes the aspect of secure data transmission over a reliable network. This data transmission is done through TCP using terminal .Now a days security is the most concerned thing in data transmission. Many theories and algorithms came into existence to secure information.
Every algorithm has its own advantages and disadvantages, but the main aim for any algorithm is to prove efficiency in securing information. Here in this project an efficient algorithm with extra security is to be implemented and executed for securing information in between communication. To develop an algorithm this will be difficult for intruders to crack the information. And this developed algorithm must be fit enough for usage in various application for security purpose.
To add additional security using additional keys in this algorithm which works efficiently and to transmit the information between sender and receiver using TCP in which terminal in Ubuntu operating system is used as interface

1.1 Overview

Security measures must be incorporated into computer systems whenever they are potential targets for malicious or mischievous attacks. This is especially for systems which handle financial transactions or confidential, classified or other information whose secrecy and integrity are critical.
The purpose of System Implementation can be summarized as follows: making the new system available to a prepared set of users (the deployment), and positioning on-going support and maintenance of the system within the Performing Organization (the transition). At a finer level of detail, deploying the system consists of executing all steps necessary to educate the consumers on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate, and validating that business functions that interact with the system are functioning properly.
Transitioning the system support responsibilities involves changing from a system development to a system support and maintenance mode of operation, with ownership of the new system moving from the Project Team to the Performing Organization. A key difference between System Implementation and all other phases of the lifecycle is that all project activities up to this point have been performed in safe, protected, and secure environments, where project issues that arise have little or no impact on day-to-day business operations. Once the system goes live, however, this is no longer the case. Any miscues at this point will almost certainly translate into direct operational and/or financial impacts on the Performing Organization. It is through the careful planning, execution, and management of System Implementation active ties that the Project Team can minimize the likelihood of these occurrences and determine appropriate contingency plans in the event of a problem.
This project is well featured and provides encryption/decryption that can protect message from unauthorized access. In this project, we proposed an algorithm, which uses triple keys for encryption and decryption of text to secure the information.
Here in this project a plain text that is original data is converted into cipher text using encryption algorithm. And the cipher text is converted into plain text using decryption algorithm. Plain text can be converted into cipher text by adding additional data. These additional data are called as keys. Normally only one key is used an additional data and encrypted. The same key is used for decrypting. But in this algorithm as an additional data three keys are

used which is more secure. These three keys keep data secure from hacking or any other unauthorized user.
These three keys are used for encryption of plain text from one end. At the other end the same three keys are used for decryption of cipher text into plain text. These keys acts as known keys only for sender and receiver. This algorithm has step by step process to implement using three keys. And usage of ASCII values gives more security rather than direct values of alphabet.
After implementing this algorithm the information is encrypted and sent to the receiver where the information is decrypted . The data transmission here in this project is done using TCP. The interface we used is terminal in Ubuntu operating system. By using terminal, the client-server connection is done using TCP and after connection the information sharing is done securely using this algorithm. By using TCP algorithm is attached to protocol for transmission of data between ends of communication.

2. Problem Statement

Cryptography and digital watermarking are the traditionally used mechanisms for authentication of genuine user as well as for secure information. In traditional cryptographic systems, one or more keys are used to convert the plain text into cipher text at the sending side, and the plain text will be retrieved back at the receiving side by using appropriate decrypting keys. Without the knowledge of the correct decrypting keys the conversion is 32 infeasible considering both in time and cost. Hence if the cipher text is secured, even if the intruder can obtain the cipher text it is not possible by the intruder to extract the useful information. The first main big drawback of information secure scheme based on traditional cryptography is illegal sharing of key between sender and receiver, i.e. key distribution problem.
This project addresses the security problem of providing fundamental cryptographic mechanisms for the implementation of a secure communication infrastructure that can provide strong security guarantees for sharing information in this modern era.

2.1 Existing System

The existing system, algorithm uses the text information and encrypts by ASCII values uses only one or two keys as an additional data to convert plain text into cipher text or to convert cipher text into plain text . In the existing system, the hacker's can easily access the information because of easily imaginable keys or probability checking or less usage of keys.
The encrypted message will have only one or two secret keys for securing the data due to this the text can be easily decrypted.

2.2 Issues

- Due to the existence of only one or two keys on either sides of communication. The accessibility towards information becomes easy for intruders. The security is the main issue for this algorithm.
- Wrong distribution of keys while encryption or decryption.

2.3 Proposed System

In proposed system, the algorithm consists of three keys each for encryption and decryption. The inclusion of these three keys algorithm gets more secured and efficient.
In this proposed technique, we focus mainly on providing security to the information from an unauthorized user by using triple key authentication algorithm. The algorithm uses triple keys i.e. k1, K2, k3. The key k1 is generated from the message and also transferred along with the message. The cipher text obtained after applying encryption using key1 is considered as plaintext for the rest of the two keys. The PTK1 (plain text using k1) is now encrypted with the help of two keys (k2, k3) in order to obtain the final cipher text i.e. CT. In decryption the reverse operation is performed , the CT is decrypted with the help of two keys (k2, k3) to obtain the PTK1.Thereafter PTK1 is decrypted using key 1 to obtain the final output which is the plaintext .

2.4 Advantages

- Due to inclusion of three keys the security for information gets increased. It is difficult to crack the information in between communication.
- This algorithm is very efficient and faster.

Fixed keys for distribution so that encryption and decryption is always correct.

3. Methodology

ALGORITHM

Enhanced Cryptographic Algorithm
The algorithm follows procedure

3.1 Encryption

Step 1: Enter the plain text from the user. Add the ASCII value of plain text starting from first alphabet with last alphabet i.e. moving right from first and left from last. If message is of odd length, then write the ASCII value of middle alphabet as it is.
Step 2: Store these values in an array and take modulus of these values from 26 i.e. (%26) and store the result in another array.
Step 3: To obtain the value of PTK1 i.e. (plain text encrypted with the help of key1) we perform the following steps: Add the ASCII value of first half of message with the values stored in Array 2. Now perform further calculations i.e. values obtained in step 1 – key1-ASCII value of first half of the message.
d) Step 4: Now PTK1 is considered as plaintext for rest of the two keys (K2, K3) in order to achieve triple keys algorithm.
e) Step 5: By entering encryption keys (K2, K3) from the user, encrypt the PTK1using the given formulae,

$$CT = ((PTK1 * K2) + K3) \bmod 26.$$

f) Step 6: Thus the CT (Cipher text) is obtained using the above formulae.

3.2 Decryption

a) Step 1: Before proceeding the decryption, perform an algorithm for calculating modulo inverse of a number (MODINV), MODINV is used to calculate the inverse of K2 (one of the encryption key). This algorithm is performed using Extended Euclidean Algorithm (EEA); EEA is explained at step6. Now K2 is given to EEA to get the output as INVK2.
b) Step 2: Decryption is done by using Ciphertext, (INVK2, and K3) pair. For getting the plaintext, apply the formulae PTK1= (INVK2 (Ct-K3)) mod 26 Store the ASCII value of PTK1 in an array.
c) Step 3: Add the ASCII value of First + K1+ (n/2+1)th positions elements and perform this operation in right direction to obtain the array 3.
d) Step 4: Array 4 is equal to ASCII value of alphabets of Array2 from position first to n/2 th position- Array 3 mod 26.
e) Step 5: Array 5 can be computed by the expansion of Array 4. Fill the ASCII value up to n/2 th position as it is. Calculate the remaining values of the message by n th element of Array 3- n th element of Array 4 and store it in (n/2 + 1)th the position of Array 5 and so on.

f) Step 6: EEA: The Extended Euclidean Algorithm is used to calculate the modular multiplicative inverse of an integer a modulo m. The Euclidean Algorithm determines the greatest common divisor (gcd) of two integers say, a and m. If a has a multiplicative inverse modulo m, this gcd must be 1. The algorithm of EEA is described below.

```
r1<-a;r2<-b;
            t1<-0;t2<-1;
while(r2>0)
            {
             q<--r1/r2;
            r<--r1-q*r2;
            r1<--r2;
            r2<--r1;
             t<--t1-q*t2;
             t1<--t2;
             t2<--t1;
            }
gcd(a,b)<--r1;t<--t1;
```

g) The EEA Algorithm: Step 7: By doing all above steps, we will get back the Plaintext or original message.

3.3 Example

a) Encryption:
STEP 1:

204	235	225	210

Enter the plain text from the user. Say "Symmetry" for this example.
Array 1:

s+y=204y+r=235	m+t=225	m+e=210

STEP 2:
Array 2= Array 1%26

22	1	17	2

STEP 3:
To obtain the value of PTK1 the steps are as follows.
PTK1= Add ASCII value of first half of message with the values stored in Array 2. Remaining values are calculated by (values stored in Array 1 – key 1 – right half of values obtained for PTK1)

105	122	100	111

83	97	107	83

STEP 4:
PTK1= value obtained by performing encryption to the plaintext with the help of key1. PTK1 is considered as plaintext for the rest of the two keys in order to achieve triple key algorithm.
PTK1= "izdoSamS"
STEP 5:
Enter the encryption keys (k2, k3) from the user. Now the ciphertext is obtained by using the formulae,

CT= ((PTK1* K2) +K3) mod 26

104	119	121	120	80	100	106	80

H	W	Y	X	P	D	J	P

STEP 6: CT= "hwyxPdjP"
b) Decryption:
STEP 1: Before proceeding the decryption process, we perform an algorithm for calculating the module inverse of K2 i.e. one of the encryption key. This algorithm is performed using EEA (Extended Euclidean Algorithm)
INVK2= MODINVK2 by using EEA.
STEP 2: Decryption is done by using following pair (CT, INVK2, K3) to get the PTK1. For getting PTK1 apply the formulae,
PTK1= (INVK2 (Ct-K3)) mod 26

After applying the formulae, the value of PTK1 is obtained and store in an array.
Array 1:

105	122	100	111	83	97	109	83

L	Z	D	O	S	A	M	S

83	121	109	109
101	116	114	121

PTK1= "izdoSamS"
Array 2= ASCII value of PTK1 stored in array 1.

105	122	100	111
83	97	109	83

STEP 3: Array 3= Add ASCII values of (1st to n/2)th + K1+ (n/2+1)th in right direction and so on.
STEP 4: Array 4: ASCII value of alphabets of Array 2 from first to n/2 position – Array 3 mod 26

83	121	109

STEP 5: Array 5: Array 5 can be computed by the expansion of Array 4. Place the ASCII value up to n/2th position as it is. Remaining values are calculated by nth element of Array 3 – nth element of Array 4 and store these values in n/2+1th position of array 5 and so on. Hence by doing all above steps we are able to achieve the plaintext which is entered by the user i.e. "Symmetry"..

STEP 4: Array 4: ASCII value of alphabets of Array 2 from first to n/2 position – Array 3 mod 26

83	121	109

STEP 5: Array 5: Array 5 can be computed by the expansion of Array 4. Place the ASCII value up to n/2th position as it is. Remaining values are calculated by nth element of Array 3 – nth element of Array 4 and store these values in n/2+1th position of array 5 and so on. Hence by
doing all above steps we are able to achieve the plaintext which is entered by the user i.e. "Symmetry".

4. Conclusion

A symmetric key algorithm is presented in this project. This algorithm provides security of transmitted message by making use of triple keys and the simulation results are shown in the project which shows that the new algorithm is good in terms of security.

Reference

[1]. ManiKandan N.K, "A Novel Cipher Security Mechanism for IEEE 802.11i",2015, International Journal of Applied and Engineering Research, published by Research India Publication, Volume:10, Issue:3, October 2015

[2]. C.N. Mathur and K.P.Subbalakshmi. "Energy Efficient WirelesEncryption",Networking and Communications (MSyNC) Lab, 2005

[3]. Karthik,.S, Muruganadam. A,"Data Encryption and Decryption by using Triple DES and Performance Analysis of Crypto System", International Journal of Scientific Engineering and Research (IJSER), Vol 2, Issue 11, November 2014.

[4]. C. N. Mathur, K. Narayan, and K. Subbalakshmi. High Diffusioncipher: Encryption and error correction in a single cryptographic primitive. To appear in the 4th International Conference on Applied Cryptography and Network Security Conference (ACNS), June 2006.

[5]. M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in cryptology -EUROCRYPT93, Lecture Notes in Computer Science*, volume 765, pages 1–11, 1993.

[6]. K. Nyberg. Differentially uniform mappings for cryptography. In *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages

55–64, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[7]. L. M. S. C. of the IEEE Computer Society. Wireless lan medium access control (mac) and physical layer (phy) specifications. 1999.

[8]. S. Durai , N. Rajkumar, N. K. Manikandan and D. Manivannan "Data Entry Works in computer usingVoice Keyboard", Indian Journal of Science and Technology, Vol 9(2), DOI:10.17485/ijst/2016/v9i2/85814, January 2016