A Symmetric Key Cryptographic Algorithm

Vashitva Kumar Srivastava
ITM, GIDA Gorakhpur
303, Arya Samaj Mandir Road
Buxipur,Gorakhpur

Amitesh Kumar Srivastava
ITM, GIDA Gorakhpur
EWS-10 Phase-1, Raptinagar
Gorakhpur

Majhar Khan
ITM, GIDA Gorakhpur
273-L Shakti Nagar
Colony, Gorakhpur

Abstract

Any general communication which is carried out between humans for exchanging thoughts and knowledge can be understood by anyone who knows that language. It is called plain text, so we bother to make such a scheme which converts this general message into a coded message which can be understudied by only authorized people. So we need to hide the information which is written into general message, from those who are not intended, even they can see the coded data .

***Cryptography** can be stated as the art and science of transforming the message into coded form to make them secure and immune to attacks which reveals its secrecy. Cryptography is basically affiliated with the information security, Computer system security and engineering, cryptography is used in all kind of advance application technology like ATM, online banking, online trading. Cryptography has its two basic forms i.e. one is symmetric key cryptography and other is asymmetric key cryptography. An Asymmetric key algorithm uses two keys, one is public and other is private key both are used for encryption and decryption, and symmetric key cryptography algorithms are quick and most commonly used, In symmetric key algorithms single key is used for both encryption and decryption, this is also called secret key which is shared between both sender and receiver. Some common symmetric key algorithms are DES, RC2.RC4, and IDEA etc. This paper describes an new symmetric key algorithm which uses basic additive cipher and some new component to encrypt the information. We provide both algorithms for encryptions and decryption. The advantage of this algorithm over others is also explained.*

Categories & subject descriptors

[Cryptography & Steganography]: A New Algorithm.

General Terms

Algorithms, Design, Security.

Keywords

Cryptography, Network security, Symmetric Key.

1. Introduction

Now a day's internet is the easiest and simplest way of exchanging information between ten's of million people, and it is also used for the trading activity which includes the transfer of funds, so by providing these facilities security became very essential aspect to be dealt with There are many aspects to security and many application like secure trading , secure payments system and securing personal communication to provide secure virtual envoirment .

One way of securing communication or it can also be stated as Cryptography is an essential aspect of secure communication. Cryptography has a very old history, Julius Ceaser has created a one of the oldest and popular cryptographic algorithm, which he used to send the confidential information to his generals, which is later called as ceaser cipher and also named as additive cipher.

Cryptographic system uses mathematical view or mathematical approach to encrypt and decrypt the information, and it gives us a way to store the data securely or transmit the data over the secure network in secured form so that it cannot be read by any other unauthorized recipient. Cryptography embraces both cryptography and cryptanalysis.

A Cryptographic system can also be viewed as an mathematical function which is used for both encryption and decryption, A cryptographic algorithm is set of elements algorithms for encryption and decryption both and key(s) for encryption and decryption both, For symmetric key algorithms same key is used for both encryption and decryption. A key can be an alphabet, a number, or a phrase to encrypt or decrypt the plaintext and cipher text respectively. The same plaintext can be encrypted to different cipher text with the help of same algorithm but with application of different keys.

Kirchhoff has given a principle which states that the resistance of the cipher to attack must be based on the secrecy of the keys. i.e. the encryption and decryption algorithm both are known to everyone only the key is kept secret. We have to make an algorithm which is strong enough that it can hide relationship between cipher text and plaintext and also hides the relationship between the cipher text and key.

2. NEW SYMMETRIC KEY ALGORITHM

Our algorithm is based on the basic encryption technique called additive cipher, but it includes some new components to make our information more secure. One of those two components is Middle text Generator and other is mixer which enhances the complexity of the cipher text to be broken. In this algorithm we provide a logic by which one digit is mapped with four digits i.e. 1 to 4 mapping is done and then we apply additive cipher algorithm to encrypt the middle text into Z10 domain. And after encryption we apply a mixer which mixes the cipher text that it became hard to find the relationship between the cipher text and the key and plaintext and cipher text because of congruence. This algorithm is applicable for numbers of range 0-9 and we take 64 digit blocks for encryption and decryption algorithm.

This Algorithm consists of two phases:

i)Middle Text Generation phase
ii) Encryption and Mixing Phase

2.1 Encryption algorithm

Step 1: Generate the middle text with the help of Middle Text Generator by applying key k.
Step 2: Now divide the middle text in blocks of size 64 each.
Step 3: Now encrypt the 64 digit block with the additive cipher algorithm with following formula

C= (P+k) mod 10

Step 4: Now calculate key **k`** with the help of following formula

k'=k+(next prime number after key).

Step 5: Now calculate key k" with the help of following formula

k''=k'+n*32.

(Where n=1, 2, 3…….)

Step 6; Now apply mixer to the encrypted data with key k''.

2.1.1 Middle Text Generator

Middle Text Generator is used to generate the middle text of plaintext; it maps one digit with four digits i.e. one to four mapping.

I) To generate the middle text of 1,3,9,7 we have following 4 set's

1- | 1 | 3 | 9 | 7 |

2- | 3 | 9 | 7 | 1 |

3- | 9 | 7 | 1 | 3 |

4 - | 7 | 1 | 3 | 9 |

Sender and receiver must have to agree on any one of the following sets to generate the middle text.

II) To generate the middle text of 2,4,6,8 we have following 4 sets

1- | 2 | 4 | 6 | 8 |

2- | 4 | 6 | 8 | 2 |

3- | 6 | 8 | 2 | 4 |

4- | 8 | 2 | 4 | 6 |

Sender and receiver must have to agree on any one of the following sets to generate the middle text.

III) To generate the middle text of 0, 5 we have following 4 sets

1- | **2** | **5** | **8** | **0** |

2- | **5** | **8** | **0** | **2** |

3-

8	0	2	5

4-

0	2	5	8

Sender and receiver must have to agree on any one of the following sets to generate the middle text.

NOTE: Sender and receiver must have to agree on 1 set from each different group (i.e. one from group I, one from group II and one from group III) i.e. they both have to agree on 3 sets.

For generating middle text we have to left circular shift the corresponding set, resultant generated by the following formula with key k.

Shift=(k+position+value) mod 4

2.2.1.2 A Middle Text Generator Example

We have to generate the middle text of 9, key k is 56 and the shared matrix between sender and receiver is given below

Value ⟹	**1**	**3**	**9**	**7**
Position	**0**	**1**	**2**	**3**

Now apply formula shift=(k+position+value) mod 4.

Shift= (56+2+9) mod 4

=67 mod 4

=3

i.e. we have to circular shift the shared matrix 3 times.

7	1	3	9

i.e. 9 will be replaced by 7139.

2.1.2 Mixer

It mixes the encrypted text i.e. it enhances the complexity of the cipher text which hides the relationship between key and cipher text.

In this we divide the 64 digit block into two block, each of size 32 A and B.

0 A 31

0 B 31

I)-If key (k'') is even

Copy all the even position value as it is from both blocks A and B, and for odd position value ,swap that position value of block A with the position resultant from following formula with block B.

Swap ←(key+position+2)mod 32

NOTE: 0 well be considered here as Even.

II) - If key (k'') is odd:

Copy all the odd position value as it is in both blocks A and B, and for even position value swap that that position value of block A with the position resultant from following formula with block B.

Swap ←(key+position+1) mod 32

It enhances the complexity of the cipher text.

3. Decryption algorithm

Step 1: Calculate **key k' ←k + next prime number after key**

Step 2: Now apply key k' with the mixer.

Step 3: Decrypt the obtained encrypted data from the above step by following formula **p=(c-k) mod 10**

Step 4: Now apply Degenerator and obtain the original plain text.

3.1 Mixer

The working of Mixer will be same as it was in encryption.

It will be invertible with the application of same key.

3.2 Degenerator

Step 1: The received text from above step is divided into 16 groups of size 4 digit each.

Step 2: Receiver have already list of middle text for each number ranging 0-9, which receiver generated with the help of shared set's and shared secret key, each of size 4 digit.

Step 3: Then each group is compared with the list of middle text and replaced by corresponding plain text.

3.2.1 Example of Degenerator

The shared matrix between sender and receiver for no. 1,3,9,7 is {1,3,9,7} for 2,4,6,8 is{4,6,8,2} and for 0,5 is{2,5,8,0}, the shared key is 56.

1	3	9	7	2	4	6	8	……	4	6	8	2
0	1	2	3	4	5	6	7		60	61	62	63

Receiver has list of middle texts for each no. by application of formula **(Key+position+value) mod 4** and shifting the corresponding list resultant no. of times.

1 ←	3	9	7	1
2←	6	8	4	2
3←	1	3	9	7
4←	4	6	8	2
5←	8	0	2	5
6←	2	4	6	8
7←	9	7	1	3
8←	8	2	4	6
9←	7	1	3	9
0←	0	2	5	8

1	3	9	7	2	4	6	8	……	4	6	8	2
0	1	2	3	4	5	6	7		60	61	62	63

0-3,are considered as one group and they are compared with the list of middle text and replaced by corresponding plain text, here 0-3 are {1,3,9,7} and they are compared with list and corresponding plaintext is 3, for group 4-7 plaintext is 6, and so on calculated.

4. Advantages of the New Algorithm

1. This Algorithm uses one to four mapping i.e. one number is replaced by 4 numbers which enhances the complexity of cipher text.
2. This Algorithm uses a mixer which mixes the cipher text with help of key so it makes it more secured.
3. For a small amount of data this algorithm will work very smoothly.
4. This Algorithm uses additive cipher for encryption which is simple.
5. This Algorithm is easy to implement.

5. Conclusion

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data now, in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data and increases the complexity of data which reduces the chances of attacks on data. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but off-course not sacrificing the security issues. A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm. But as public key cryptography is more secured then secret key cryptography our next task would be to develop and design a public key cryptographic algorithm in a simple manner as it is done in this paper.

6. References

1) S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.
2) Computer and Network security by ATUL KAHATE.

3) S. Hebert, “A Brief History of Cryptography”, an article available at http://cybercrimes.net/aindex.html
4)”Cryptography and Network Security ” By Behrouz A. Forozen.
5)”Data Communication and Networking” By Behrouz A. Forozen.