A New Substitution Transposition Method- A New Technique of Encryption

Sabina Priyadarshini
Department of Computer Science and Engineering
Birla Institute of Technology

Abstract - Secure transmission of confidential data is a demand these days. Encryption is a process of turning intelligible data into unintelligible form so that intruders cannot understand the meaning of the data that is being sent. In this paper, a new method of encryption has been proposed.. It does not involve complex mathematical operations or large storage space for storing big tables. It is simple to implement and at the same time, difficult for an attacker to decrypt easily.

Keywords: encryption, substitution, transposition

I. INTRODUCTION

These days, information is received and misused by means of attacks at various levels of communications [1]. The best way to combat the attacks is by means of data encryption [2]. The art and science of creating unintelligible text so that only intended person is able to read data is called cryptography [3]. For secure transfer of confidential data, cryptography is needed. Cryptography means sending data in an unintelligible and encrypted form. Encryption is the process of converting understandable data into garbage- like meaningless form using a key and an algorithm that is not understandable by anyone except the receiver. The original understandable text is called plaintext. The meaningless garbage-like form of the plaintext achieved by means of encryption process is called cipher text. The receiver uses the key and the algorithm to convert cipher text back to plaintext form. This process is called decryption and is exactly the opposite of encryption.

There are two types of encryption: symmetric key encryption and asymmetric key encryption. Symmetric key encryption uses the same key value for both encryption and decryption. Asymmetric key encryption uses two keys: public key and private key for encryption and decryption. The relationship between private key and public key is that anything encrypted with private key can be decrypted using public key and vice versa.

Symmetric key encryption makes use of a shared secret key which is communicated between sender and receiver before the encrypted data is sent. The key can be communicated via email, SMS phones or over the network in such a way that nobody is able to look at the key except the receiver. Examples of symmetric key encryption are Data Encryption Standard (DES), Advanced Encryption Standard, etc. [4].

Asymmetric key encryption makes use of two keys: public key and private key. The public key is known to everyone whereas private key is known only to the user and is not disclosed to anyone. Examples of asymmetric key encryption include RSA etc.

There are two ways to encrypt data – substitution and transposition. Substitution means replacing one character by another character in the alphabet set. Transposition means rearranging or shuffling the characters to different positions. When a character is substituted by another character, it is known as monoalphabetic substitution cipher. For example, the sentence I WILL BE COMING TOMORROW can become KYKNN DG EQOKPI VQOOQTQY if we change each character by a character two places down the line in the alphabet set. Transposition cipher changes positions of characters. For example, APPLE can become PALPE if we change the positions of the characters by the rule 1-2, 2-1, 3-4, 4-3, 5-5.

In this paper, a new method of symmetric key encryption has been designed. This method works in two steps: (i) individual repositioning and substitution and (ii) block repositioning. Individual repositioning involves repositioning of characters followed by substitution which means replacing each character by another character some places down the line in the alphabet set. Block repositioning means shuffling the positions of blocks into which data is divided.

This paper is organized in the following way. The section II gives the literature survey. Section III describes the proposed encryption algorithm. Section IV demonstrates the encryption algorithm with an example and gives a detailed explanation. Section V gives the decryption algorithm. Section VI gives the illustration of the decryption algorithm using example. Section VII gives the advantages of the technique. Section VIII concludes the paper.

II. LITERATURE SURVEY

Data Encryption standard (DES) [4] algorithm takes 64 bits of plaintext at a time and uses a 56 bit key. It has two permutation steps, first one done at the beginning and second one which is done in the last step. All 64 bits are permuted, with 16 identical rounds of operations in between. The operation of each round is identical. During each round, rightmost 32 bits of input are moved to left 32 bits of output. The 32 rightmost bits input to the ith round and the 48 bit key derived from 56 bit key for the same round are fed as input to a function. The function expands 4-bit input chunks into 6-bit chunks, making the 32 bits as 48 bits. Then, an exclusive OR of these 48 bits is done with 48 bit key. Then, a substitution operation is performed and 48 bits result is converted into 32 bits. Further, exclusive ORing of these 32 bits is done with leftmost 32 bits of input. The resulting 32 bits output of the function is then used as the rightmost 32 bits of the round's 64 bit output. These steps are repeated 16 times for 16 rounds. Finally a permutation of 64 bit result is done and a 64 bit output is generated.

Soraha et al. [5] have taken a message or plain text from the user. The key-1 is decided with the help of which characters are to be shifted. The message is decrypted by replacing each letter by decided key-1. Then this encrypted message is written in rectangular way row by row. The number of rows depends upon the amount of data. Then, the order of column becomes the key-2 to this algorithm, which is decided by sender and also known to receiver. The message is then read off column by column and the order of the column can be permuted. The output is written in rectangular form again row by row. After placing data in rectangular form, then it is read off column by column. Finally, we get the secure cipher text. They have come up with a technique of encryption that combines substitution and transposition techniques and come up with a cipher text that is so strong that it is difficult to break. It is more difficult to cryptanalyze than caeser cipher. The result is not easily reconstructed. Brute force attack is not possible.

Kumar et al. [6] review some of the encryption and modern techniques that are demanded in several fields. They have compared SDES, DES, Playfair and Vignere on the basis of avalanche effect [7] with the same key and plaintext. Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plaintext.

III. THE PROPOSED ENCRYPTION ALGORITHM

Step 1. The characters of the text are arranged into three columns.

Step 2. The characters so written are divided into blocks. Each block has nine characters.

Step 3. For each block, the following steps are performed:

i)An ordering is selected for transposition. If the ordering is 1-2-3-4, it means, first the top left part is chosen for character transposition, then the top right part, then, the bottom left part and finally, the bottom right part.

ii)For each part according to the order selected, the positions of characters that are diagonal to each other are exchanged.

iii)Then, a substitution with characters some places down the line in the alphabet set is done. The number of places is chosen by the user. It may be different each time.

Step 4. The step 3 is repeated for all the blocks.

Step 5. Step 3 and 4 are repeated five times, and each time a different order may be chosen by the user. For example, the order could be top right first, then top left, then, bottom left and finally bottom right. There are 24 orders possible. In part iii) of step 3, a different number of places may be chosen each time of how many places down the line in the alphabet set we have to go for substitution.

Step 6. Block transposition is done on the basis of an order according to the choice of the user. If the order is 3-1-2, then the third block is sent to the first block's position, the first block goes to the second position and second block goes to the third position.

IV. ILLUSTRATION OF THE ENCRYPTION ALGORITHM

The steps of the algorithm are illustrated by means of an example. The example sentence is I AM COMING TOMORROW.

Step 1: The characters of the text are arranged into three columns.

I A M

C O M

I N G

T O M

O R R

O W

Step 2: The characters so written are divided into blocks. Each block has nine characters.

I A M

C O M

I N G

T O M

O R R

O W $.

It can be noted that $ has been added for padding to make the block size as nine characters. It can be noted that for a block of nine characters, a maximum of eight $s will be required. $ will always be substituted by $ itself.

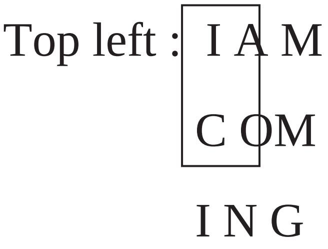
Step 3: For each block, the following steps are performed:

i)An ordering is selected for transposition. For example, if the ordering selected is 1-2-3-4, it means, first the top left part is chosen for character transposition, then, the top right part, then the bottom left part and finally the bottom right part. For example, for the first block of step 2, the following is done:

I A M

C O M

I N G

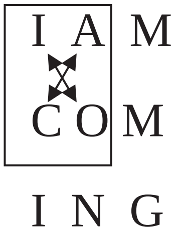


Top left : I A M

C OM

I N G

ii) The positions of characters that are diagonal to each other is exchanged.

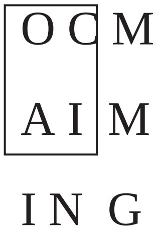


I A M

C O M

I N G

I and O are exchanged. A and C are exchanged. The result is as follows:

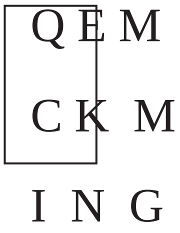


O C M

A I M

I N G

iii) Then , a substitution of characters of this part with characters some places down the line in the alphabet set is done. For example, if number of places chosen is 2, then, O will be replaced by Q, C by E, A by C and I by K. The result will be as shown below:

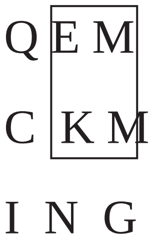


Q E M

C K M

I N G

Next, the top right part is taken as shown below:



Q E M

C K M

I N G

The positions of characters that are diagonal to each other are exchanged. The result is as shown below:

Q M K

C M E

I N G

Then, a substitution a substitution of characters of this part with characters some places down the line in the alphabet set is done. For example, if number of places chosen is 3 this time, then, the result is as shown below:

Q P N

C P H

I N G

Next, the bottom left part is taken as shown below:

Q P N

C P H

I N G

The positions of diagonal characters are exchanged as shown below:

Q P N

N I H

P C G

Next, a substitution of characters of this part with characters some places down the line in the alphabet set is done. For example, if number of places chosen is 4, then, the result is as shown below:

Q P N

R M H

T G G

Then, the bottom right part is taken as shown below:

Q	P	N
R	M	H
T	G	G

The positions of diagonal characters are exchanged:

Q	P	N
R	G	G
T	H	M

Then, a substitution of characters of this part with characters some places down the line in the alphabet set is done. For example, if number of places chosen is 2, then, the result is the following:

Q	P	N
R	I	I
T	J	O

Step 4: The same procedure is used for encrypting all the blocks.
Step 5: Steps 3 and 4 are repeated 5 times, each time using different orders and different places in the alphabet set for substitutions for each part.
Step 6: Block transposition is done. For example, in the above example, the output of the first block of step 2 is placed in the second block and that of the second block is placed in the first block.

V. THE PROPOSED DECRYPTION ALGORITHM

Step 1. The blocks are taken and block transposition is done on the basis of the order used by the sender for transposition. If the sender used the order 3-1-2, then, the first block is sent to the third position, the second block is sent to the first position and the third block is sent to the second position.
Step 2. For each block the following is done. The order used by the sender for substitution is taken and an exactly opposite order is used for decryption. For example, if the sender used the order as top right part first, then, the top left part, then, bottom left and finally bottom right, then, the order chosen for decryption would be bottom right part first, then bottom left, then, top left and finally top right. For each part according to the order, the following is done:

i) First, a substitution is performed which is exactly the opposite of the substitution performed by the sender. For example, if the sender substituted each character with a character two places down the line in the alphabet set, then, for decryption, the receiver would substitute each encrypted character with a character two places up the line in the alphabet set.

ii) Then, in the same part, the positions of characters that are diagonally opposite to each other are exchanged.

Step 3. Step 2 is repeated five times for each block, each time using exactly the opposite order as used by the sender and by using back substitutions of each encrypted character with the original character and exchanging the positions of characters that are diagonal to each other.

Step 4. Finally, we get the original text arranged into three columns. The text can then be written and read serially.

VI. ILLUSTRATION OF DECRYPTION ALGORITHM

Considering the length of the paper, all five iterations of the algorithm cannot be shown. But one iteration of the algorithm has been illustrated below:

From section IV, the encrypted block is as follows:

Q P N

R I I

I J O

The order chosen by the sender was top left-top right-bottom left- bottom right. So, for decryption, the order will be exactly the opposite, i.e. bottom right-bottom left-top right and finally top left. First, the bottom right part is taken into consideration:

Q P N

R I I

I J O

The sender had chosen the number of places for substitution as two places down the line in the alphabet set. So, the receiver would substitute the characters back with characters two places up the line in the alphabet set. So, the result will be as follows:

Q P N

R G G

T H M

Then, the positions of the characters that are diagonal to each other would be exchanged. The result will be as follows:

Q P N

R M H

T G G

Then, the bottom left part is taken into consideration.

Q P N

R M H

T G G

For this part, the sender had chosen four places down the line in the alphabet set for substitution. So, the receiver would substitute each character of this part with characters four places up the line in the alphabet set. The result will be as follows:

Q P N

N I H

P C G

Next, the positions of characters that are diagonal to each other in this part are exchanged. The result is as follows:

Q P N

C P H

I N G

Then, the top right part is taken into consideration:

Q P N

C P H

I N G

The sender had chosen three places down the line in the alphabet set for substitution for this part. So, the receiver would substitute the characters with characters three places up the line in the alphabet set. The result will be as follows:

Q M K

C M E

I N G

Next, the positions of characters that are diagonal to each other are exchanged. The result will be as follows:

Q	E	M
C	K	M
I	N	G

Then, the top left part is taken into consideration:

Q	E	M
C	K	M
I	N	G

The sender substituted each character of this part with characters two places down the line in the alphabet set. So, receiver would do the opposite. The result will be as follows:

O	C	M
A	I	M
I	N	G

Next, the positions of characters that are diagonal to each other are exchanged. The result will be as follows:

I	A	M
C	O	M
I	N	G

We get the original text arranged in three columns. We write them serially row by row as follows:

I AM COMING

This is how we get the decrypted data.

VII. ADVANTAGES OF THE PROPOSED ALGORITHM

The proposed method has the following advantages:

I) It does not require large amount of storage space for large tables as is the case with algorithms like DES and runs in smaller time.

II) It is very simple to implement.
III) It is difficult to cryptanalyze when compared to Caeser cipher.
IV) It is very difficult for attacker to decrypt. For a block of nine characters, it would require (24 x25x25x25x25x25)x (24x25x25x25x25)x (24x25x25x25x25) x (24 x25x25x25x25x25)x(24 x25x25x25x25x25)operations to decrypt.

VIII. CONCLUSION

A better technique of encrypting text has been proposed that is difficult to crypt analyze than Caeser cipher and is better than DES in the sense that it does not require large storage space for large tables. And runs in lesser time. This technique can be used to send data in a secure way from the sender to the receiver.

REFERENCES

[1] William Stalling, “Network Security Essentials (Applications and Standards)” Pearson Education, 2004, pp 2-80.
[2] Charles P. Pfleeger, Shari Lawrence PFleeger ,“Security in Computing” Pearson Education, 2004, pp 642-666.
[3] Atul Kahate, “cryptography and Network Security”, 2nd edition Mc-Graw Hill.
[4] Kurose J. F, “Computer Netoworks”, IInd edition , Tata Mc. Graw Hill.
[5] Saroha V., Mor S., Dagar A. “Enhancing Security of Caeser Cipher by Double Columnar Transposition Method” ,International journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 10, Oct. 2012, pp 86-88.
[6] Kumar Mohit, Mishra Reena, Pandey Rakesh, Singh Poonam, “Comparing Classical Encryption with Modern Techniques, Journal of Physical Sciences, Engineering and Technology, Vol. 1, Issue 1, pp 49-54.
[7] Fauzan Saeed, Mustafa Rashid, “Integrating Classical Encryption with Modern Techniques”, International Journal of Computer Science and Network Security, Vol. 10, No. 5.