Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.46 – 53

A Proposed Cipher Technique with a Study of Existing Cryptography Techniques

Sumit Suri[1], Yashpal Singh[2]

[1]Computer Science Department Ganga Institute of Technology and Management, India

[2]Computer Science Department Ganga Institute of Technology and Management, India

[1] sumitsuri292@gmail.com; [2] yashpalsingh009@gmail.com

Abstract— Ciphers have been in existence for a long while. In ancient times people used to send encoded messages using some of the cipher techniques. When a plain text which is human understandable in any language is coded into a non-comprehensible form the resultant text is termed as Cipher Text. The task of converting the plain text into the cipher text is termed as Cryptography. Historically the task of cipher creation was used to be done manually but with growing development in computer systems there are now automated ways to perform the task. This article aims at a review of some manual cryptography techniques and also conceptualization of a modified cipher technique. The modified technique is named after the initials of the two authors of the article S-Sumit and Y-Yashpal.

Keywords— Cryptology, Cryptography, Cryptanalysis, SY Cipher (name given to the modified technique), Encryption, Decryption, JAVA

I. INTRODUCTION

We start by giving some of the definitions to elaborate the concepts of cryptography [12].

Definition 1 – Cryptography – can be defined as the task of achieving the security by encoding the original message into a non-readable form.

Definition 2 – Cryptanalysis – may be viewed as reverse of the Cryptography i.e. decoding the message to the readable format without explicitly knowing how the message was encoded.

Definition 3 – Cryptology – is the combination of the above two i.e. Cryptography + Cryptanalysis.

Definition 4 – Encryption – is the conversion of plain text to the encoded text or more formally Cipher [11] Text.

Definition 5 – Decryption – is the conversion of the cipher text to the plain text.

There are mainly two techniques used for generating the Cipher text.

Substitution Technique – relies on the replacement of characters in the plain text by different characters e.g. 'A' replaced by 'C'. There by making the original message into a non readable message.

Transposition Technique – On the other hand does the task of performing the permutations on the plain text.

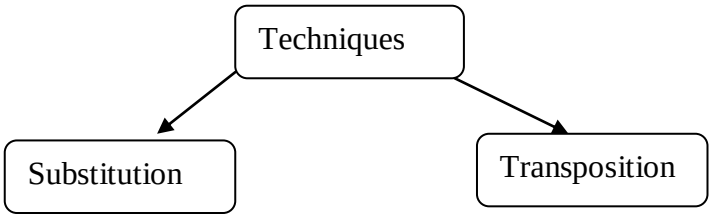

Fig. 1 Cipher Techniques

II. REVIEW OF SUBSTITUTION TECHNIQUES

A few of the substitution techniques are explained in this section.

Caesar ([1], [7]) Cipher is one of the oldest and very simple Ciphers. In this technique each letter is replaced by a different character in the alphabet sequence. One of the simplest techniques would be to replace the character by another alphabet three places up in the line. For example 'A' to be replaced 'D'. The process of getting the plain text from Cipher text would be to simply reversing the process.

Various modified versions of Caesar cipher can be applied; one technique may be to remove the restriction of replacing by certain character up the line, but allowing the replacement of one alphabet with any other alphabet. For instance character A can be replaced by any of the remaining 25 alphabets in the line. There by increasing more combinations and more secure. But the modified version is also very weak as we just need to manually try the replacements of the alphabets to crack the code.

Mono-alphabetic [2] Cipher is another technique which is stronger than Caesar approach. In this technique an alphabet can be replaced by any of 25 different alphabets. But the replacement of different characters is not dependant on other characters e.g. if A can be replaced by D it is not necessary that B to be replaced by E. B can also be replaced by any of the 25 alphabets available even A.

Poly-alphabetic [3] Cipher – This Cipher was invented by Leon Battista in 1568 [3]. In this technique multiple one character keys are used. The first key encrypts the first plain character and second key applies to second character and so on. The cycle is traversed once the keys are exhausted. There are two example of this cipher Vigenere Cipher and Beaufort Cipher.

Polygram Cipher [4] – In this technique rather than single character substitution group of characters is replaced by a different group or we may say word by word replacement. For instance we may replace THEM – PTHXZ and THE by RMZ.

One of the ciphers which is most common poly-graphic Cipher is Hill Cipher which depends on the Matrix theory.

III. REVIEW OF TRANSPOSITION TECHNIQUES

As discussed above in the transposition [13] techniques the permutations or reordering of characters is done to generate more randomness or more security. A few techniques are explained here.

Rail-Fence ([5], [10]) Technique – is a very simple and weak technique in which each row of sentence is written over multiple rows based on a key value and then those characters are read row by row to generate the Cipher Sentence. This is explained with an example below.

HE IS SOLVING A SUM – the key is 3.

H S I S

E S O V N A U

I L G M

Cipher text becomes –

HSISESOVNAUILGM

Vernam [6] Cipher – One Time Pad [8] - This cipher is applied using random non repeating characters – called as one time Pad as once this is used for ciphering one message it is not used again for any other message. Vernam Cipher has been observed to have a greater degree of Randomness. The modified Cipher Technique discussed in the next section also at places has similarity to this cipher.

IV. CONCEPT OF A MODIFIED TECHNIQUE – SY CIPHER

The modified technique is based on the combination of substitution and transposition techniques discussed in the last section. The resulting cipher has been named as SY (pronounced as si) taking initials from the names of the author of this Article. Though no claims are being made as this technique being a never thought before scheme and similar schemes may exist already. The concept is built in various stages as explained below with every stage trying to inject some improvements in the previous stage technique and also removing some of the loop holes. The new schemes are explained on the encryption of the Text Messages but these can be easily extended to be applied over the numerical or special character messages.

A. Approach -1

The first approach can be thought as a modified Caesar Cipher ([1], [7]). But instead of replacing one character in the plain text with a different text it is replaced by two characters. The two characters to be used for substitution were thought to be immediate next two characters – e.g. A will be replaced by BC, B will be replaced by CD and so on.

Given a string 'Hello' will become 'IJFGMNMNPQ'. To encrypt each character's ASCII Code is taken and 1 is added to generate the new character. At each step this new character is appended with the next character in the sequence. The character Y is replaced by ZA and Z is replaced by AB – in a cyclic manner. To decipher the text every character on the even location is discarded e.g. IJFGMNMNPQ becomes IFMMP. From this text the plain text can be obtained by subtracting 1 from the ASCII value generating original text HELLO. Though this scheme is more powerful that simple replacement of one character by one character but is a weaker technique. For instance attacker can visualize cipher text IJFGMNMNPQ as combination of characters in sequence e.g. IJ – FG – MN – MN – PQ and with careful observation various options may be tried to replace them with a single character neared to this combination e.g. trying L, M, N, O for MN. Using this attacker can decode the sequence.

The second main problem with these substitution techniques has been the presence of the common strings like 'of', 'and', 'the' which have higher probability of occurrence in the plain text than other words. These words become the soft target for the attackers.

B. Approach – 2

To overcome the problems discussed in the first approach some modifications were observed.

1. Each character will be replaced not by immediate next two characters but the nth character is used for replacement e.g. A is replaced by CD i.e. 2 characters away from A.
2. The plain text is to be adjusted so that common words are spread across. This technique is explained below with an example.

Consider the text 'Ram is the best player' the text is first re-adjusted to have strings of equal number of words – say 4 character length.

RAM IS THE BEST PLAYER will become RAMI STHE BEST PLAY ER.

This will give more strength as common words will not be distinguished. This approach is found to be stronger that the approach 1 but will require answer to two new problems.

1. What should be value of 'n'?
2. How to decipher the string where words are now at different spaces?

To answer these questions the third approach is discussed below.

C. Approach – 3

The various steps of this approach are explained below.

Step 1- the plain text is scanned and all the space positions are stored in a one dimensional array. For instance below is a plain text and corresponding array. We call it the space array.

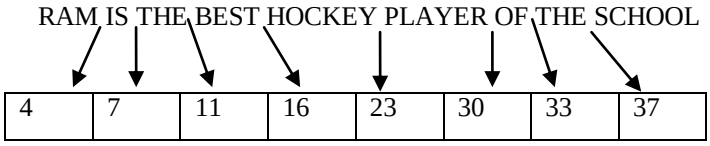

Fig. 2 space array having sy key

Now the spaces are stripped off from the string giving the string as:

RAMISTHEBESTHOCKEYPLAYEROFTHESCHOOL

The array will serve as the key to the cipher. We call it as the **sy-key**.

Step 2- Now the string is broken down in the group of 4 characters, giving the output as

RAMI-STHE–BEST-HOCK-EYPL-AYER-OFTH-SCHO-OL

If there are some trailing word with < 4 letter that is kept as it is e.g. 'OL'.

Step 3 – Each character of this string is substituted by 2 characters based on the value in the sy-key or the array of spaces. Following example shows the replacement –

R → R + 4 = VW
A → A + 7 = HI
M → M + 11 = XY
I → I + 16 = YZ

This provides the first word as VWHIXYYZ.

Similarly each word is substituted with corresponding two characters – generating the cipher text.

This method is similar to Vernam ([6], [9]) one time pad where a random one use key is used for ciphering. But in our approach we utilize the property of the string only – the space location to generate the cipher text. The sy-key is also required to be sent to the receiver as it will be used to decipher the text. This can be sent separately from the message using a different encryption technique – giving more security over the message.

Step 4 – The string is sent along with the key as discussed and is received by the receiver. The task of deciphering the message will comprise of following steps –

a. The alternate characters are stripped off the string giving the 4 character word string.

VWHIXYYZ → VHXY

b. Using the sy-key the characters are deciphered giving the string of words of length 4 (the last word may be lesser than 4 letters).

c. The spaces are stripped off from the string giving a space-less string.

d. The spaces are now inserted at the position according to the sy-key giving the original string.

Special Case – In case of the single word string which has got no spaces the sy-key will be a default key i.e. a random string similar to the Vernam [6] cipher. The key we will use is the location of last 2 characters + 1 i.e. the key of length 3.

This approach has resolved the questions asked in the second approach by providing the value of n and generating the key for helping in ciphering and deciphering.

It may also be observed that the cipher is stronger for the attacks on the common words as they are spread out and also each character gets a different substitution characters generating more randomness.

V. PROCESS FLOW

The process flow can be depicted diagrammatically below:

Encryption –

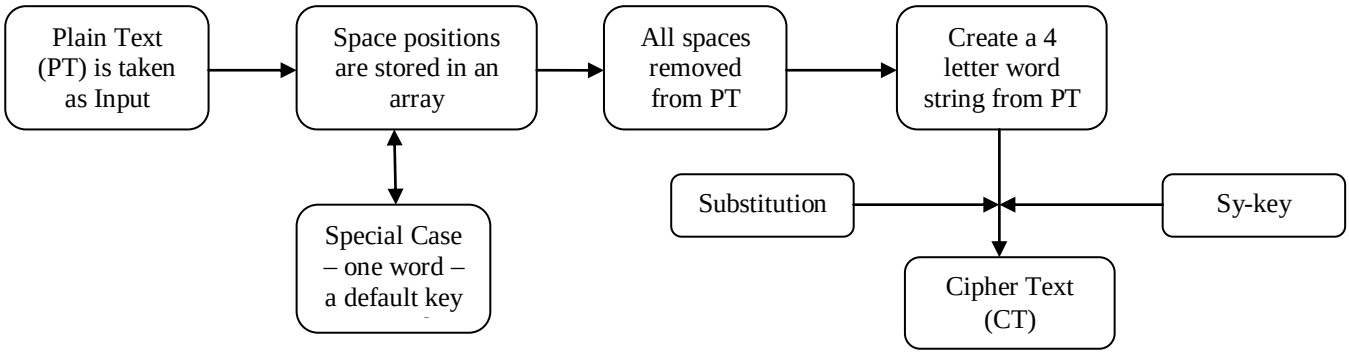

Fig. 3 Encryption using sy-key

Decryption –

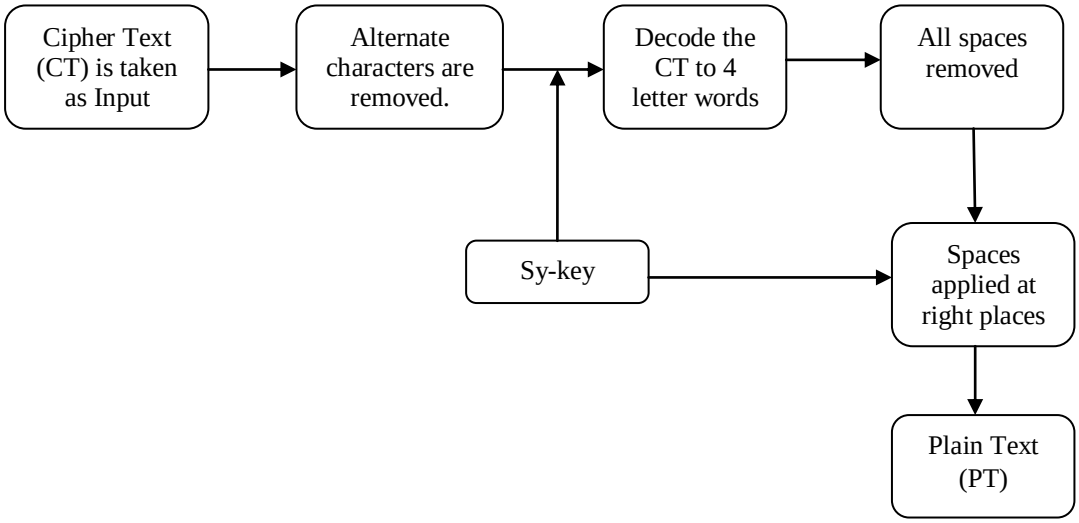

Fig. 4 Decryption using sy-key

VI. AUTOMATION OF TECHNIQUE IN JAVA WITH OUTPUT SCREENS

The various steps of Encryption and Decryption have been automated in Java [14] programming language.

Environment Specification:

Operating System – Windows 7 Ultimate
IDE – NetBeans [15] Version 8.0.2
Programming Language – Java [14]

A. Encryption Process Steps

Input -

Plain Text – RAM IS A GOOD BOY

Output -

Cipher Text - UVGHUVVW VWGHOPCD RSJKJKCD CD

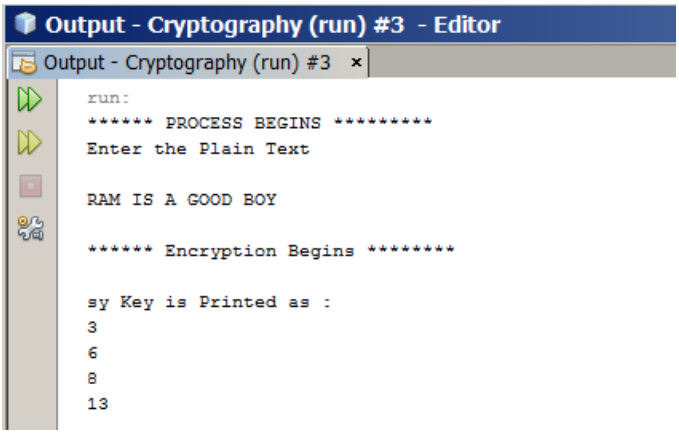

Fig. 5 Input is taken

Step 1 -

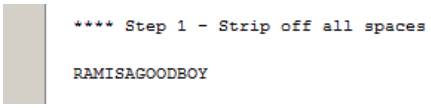

Fig 6 Step 1 illustrated

Step 2 –

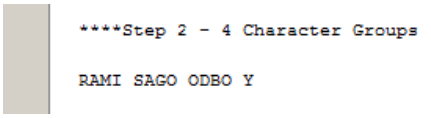

Fig. 7 Step 2 illustrated

Step 3 –

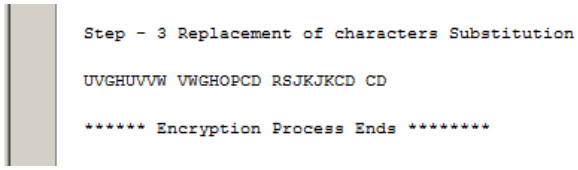

Fig 8 Step 3 illustrated

B. Decryption Process Steps

Input -

Cipher Text - UVGHUVVW VWGHOPCD RSJKJKCD CD

sy-key – 3 6 8 13

Output –

Plain Text – RAM IS A GOOD BOY

Step 1 –

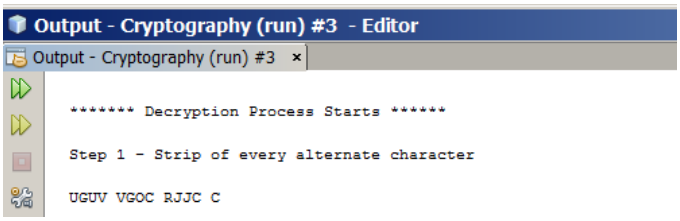

Fig 9 Step 1 illustrated

Step 2 –

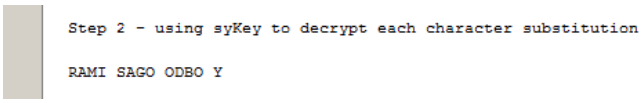

Fig 10 Step 2 illustrated

Step 3 –

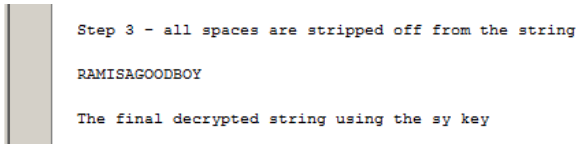

Fig 11 Step3 illustrated

Step 4 –

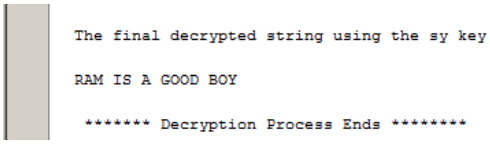

Fig 12 Step 4 illustrated

VII. ADVANTAGES

In this section we will draw a comparison between the existing cipher and the new modified scheme based on the observations.

a. This technique makes use of substitution of one character with more than one character there by giving more security over the simple Caesar [1] cipher which works on single substitutions.
b. The technique combines the substitution and transposition techniques giving more strong cipher text.
c. The technique provides more security over the attack on the common words in the string by generating more randomness and also generating a different cipher text for one character on its difference occurrence in the string.
d. The technique generates more randomness by hiding the actual semantics of the plain text by changing the space positions. This may avoid the obvious guess work by the attackers.
e. This scheme is good for shorter to relatively longer messages – depending on the key size.

VIII. LIMITATIONS

As this technique is a symmetric approach the key distribution becomes one major limitation for this. The space array is the main key which is required for the deciphering as well as construction of the original message. This can be overcome by sending this array separately from the message; also any existing asymmetric approach may be used to send the key to the receiver.

The other problem which can be observed is the large size of the array in case of larger messages. It is recommended though to use this technique for shorter messages giving manageable array size. The dynamic link list approach may be used for larger messages when we are not able to statically determine the size to be allocated to the sy-key array.

IX. THE FUTURE

The demand for security is increasing with a dramatic pace like never before. The use of internet for e-commerce and other mission critical applications is driving the needs for this security. There are various algorithms in use and also being developed to ensure more security and also ease of computation. The cipher technique detailed here is just a starter approach for understanding how the various ciphering techniques can be modified to inject more randomness. The future may use more concrete approaches like using artificial intelligence in this domain which is proven to be very efficient in other areas.

The sy-technique in its primitive form can also be amended to use more randomness. For instance the better implementations of the sy-key can be thought of to remove the problem of large sized array for larger messages.

The sy-key is purely based on the location of spaces in the messages. Alternate properties about the messages can be harnessed similar to the space property to generate the variations of the cipher techniques.

More combination of techniques can be applied to sy-technique to generate strong cipher text. For instance applying matrix operations on the cipher text will give a whole new dimension to this technique.

ACKNOWLEDGEMENT

We wish to acknowledge Dr. Yashpal Singh and other staff members for Computer Science Department of Ganga Institute of Technology and Management for the valuable guidance and support.

REFERENCES

[1] Articles Available [Online]: http://practicalcryptography.com/ciphers/caesar-cipher/
[2] Articles Available [Online]: https://en.wikipedia.org/wiki/Substitution_cipher
[3] Atul Kahate, Cryptography and Network Security, 3rd ed., Mc Graw Hill Education
[4] Lecture Notes Available [Online]: http://www.dcs.bbk.ac.uk/~dweston/infosec/Lecture4.pdf
[5] Pages Available [Online]: http://practicalcryptography.com/ciphers/rail-fence-cipher/
[6] Articles Available [Online]: http://www.pro-technix.com/information/crypto/pages/vernam_base.html
[7] Pages Available [Online]: https://en.wikipedia.org/wiki/Caesar_cipher
[8] Pages Available [Online]: https://en.wikipedia.org/wiki/One-time_pad
[9] Pages Available [Online]: http://www.cs.miami.edu/home/burt/learning/Csc609.051/notes/02.html
[10] Articles Available [Online]: https://en.wikipedia.org/wiki/Rail_fence_cipher
[11] Pages Available [Online]: https://en.wikipedia.org/wiki/Cipher
[12] Articles Available [Online]: http://nptel.ac.in/courses/106105031/
[13] Articles Available [Online]: https://en.wikipedia.org/wiki/Transposition_cipher
[14] Pages Available [Online]: https://www.oracle.com/java/
[15] Pages Available [Online]: https://netbeans.org/

