Int. J. Advanced Networking and Applications
Volume: 15 Issue: 04 Pages:100-200 (2023) ISSN: 0975-0290 (Special Issue – ASCIS 2023)

Improving Security of Message by Enhancement of Vigenère Cipher by Generating Keys Automatically deriving from the Plain Text

Syed Usman Basha Research Scholar
BIHER
Chennai, INDIA
syed.usman.mca@gmail.com
Orcid ID: 0000-0002-6406-9387

Dr. S. Brintha Rajakumari
Department of Computer Science
BIHER Chennai, INDIA
brintha.ramesh@gmail.com
Orcid ID: 0000-0003-4381-3493

***Abstract*— Researches are performed at present in large number to offer protection to data. From a very long time, Cryptography has been used for preserving the confidential data and information both during transfer and storage from unknown persons. There are many classifications of cryptography based on its implementation method. Ploy Alphabetic substitution cipher is one such method where the plain text is converted to cipher text with the help of Tabula Recta. Vigenère Cipher is considered as an important form. This Cipher uses a single Key, which is repeated to match the length of the Plain Text. For this reason, the encrypted message can be decoded using frequent analysis tests. A new method is adopted by which the key is generated automatically based on the Plain Text. This makes the Cipher Text more complex such that it would be difficult to be decoded without knowing the Key.**

Keywords—cryptography, cipher, Vigenère cipher, Tabula Recta, automatic key, cipher techniques

I. INTRODUCTION

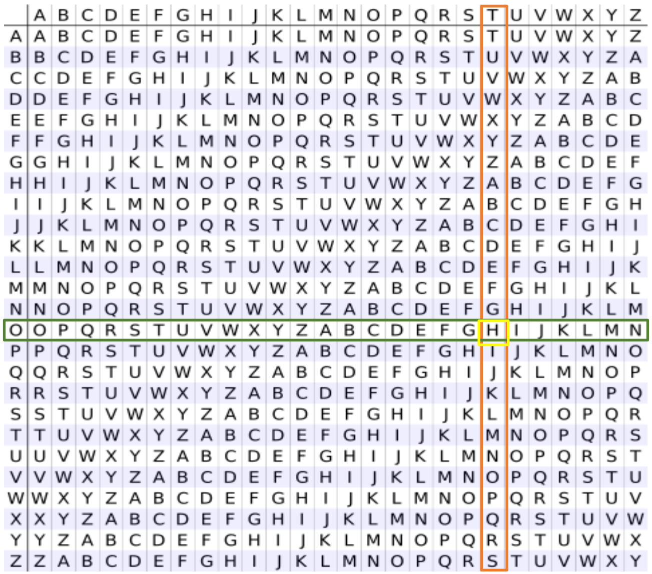
Cryptography[1] in Greek means “secret writing”. It is a technique to achieve confidentiality of messages. Most of the people around the globe use cryptography on a daily basis to protect data and information knowingly or unknowingly. Cryptography is the method of converting a normal message to unrelated and inconsequent ciphertext. The process of converting a plain text to coded text is termed as Encryption. The reverse process of converting back the coded text to normal message is termed as Decryption. The code in general is termed as Cipher[4]. The conversion is done using the plain text and a key. If same key used for both encryption and decryption, then it is termed as Symmetric Key Cryptography. If Public key used for encryption and Private key used for decryption., then it is termed as Asymmetric Key Cryptography. The conversion can be performed in two ways. Cipher generated by converting each digit of the plain text one at a time is termed as Stream Cipher. Cipher which is generated by converting the plain text as blocks is termed as Block Cipher. If the Cipher is obtained by changing the position of

replacing the alphabets of the plain text to other alphabets using formulas and computations, it is termed as Substitution Cipher. The security of the encrypted message depends on the strength of cryptographic algorithm. Algorithms of cryptography from traditional to modern methods mostly make use of alphabets. Vigenère Cipher, one of the Poly Alphabetic ciphers can be modified in such a way that the Key which is assumed between the sender and receiver are predefined, can be enhanced by automatic generation depending upon the Plain Text elements and it's length.

II. LITERATURE REVIEW

In the regions of Egypt, Greece and Rome during early civilizations, people used Cryptography for communication. As early as 1900 B.C., Hieroglyphs, a non-standard type of cryptography, secret carvings on stones were used. In Greece, a cryptographic method was used by Spartan Military named as "Scytale". Scytale[8] is a Tool which performs Transposition Cipher. The Plain Text written in rows, is encrypted by considering columnar text. A substitution Cipher, used in early days by ancient people of Rome, Ceaser Cipher, a Monoalphabetic cipher, generated by shifting of alphabets. The Plain Text message "ATTACKATDAWN", would be encrypted as "CVVCEMCVFCVP". In Hebrew language, Cipher named "Atbash". It's a monoalphabetic cipher, where the Alphabets in from ascending order are matched with alphabets in descending order. Two secret scripting methods were used sahariya for secret communications with other countries. Arab is the birth place of Modern Cryptography. Al Kindi, the Arab mathematician used frequency analysis in nineth century to build cipher text. Monoalphabetic Ciphers weakness is that they contain frequency of alphabets same as the message and Brute force algorithm can decrypt it. Vigenère Cipher is a Poly Alphabetic[6] cipher, which means each alphabet takes more than one form. The first description of a polyalphabetic cipher was contained in the work of Al-Qalqashandi. Early Polyalphabetic cipher include Alberti cipher[11] found by Leon Battista Alberti. For encrypting a message, Alberti used mixed alphabets, alphabet switching was done random intervals. A decoder device was used by Alberti for implementing polyalphabetic substitution with mixed alphabets. The device was cipher disk. The main advantage of Polyalphabetic ciphers is that they donot contain the same frequency of letters as in the message and brute force algorithm cannot decrypt them. Johannes Trithemius invented a progressive key polyalphabetic cipher called the Trithemius cipher[10]. In this method, cipher are obtained by shifting each letter of the message. A tabula recta was used for switching of letters of the plain text. The Trithemius Cipher is an incredibly important step in the development of very secure ciphers. But it is quite weak due to lack of key. One of the biggest advances in cryptography is the Vigenère Cipher [11]. It is a method of converting a normal text to coded text using series of interwoven Caesar Cipher. It was first developed

Even though it was decoded by Friedrich Kasiski, still it is a very secure cipher. This cipher uses the Tabula Recta for encryption and decryption. A key is assumed randomly. It can be of a single letter or a word. The letters of the key are repeated until it matches the number of characters in the plain text. Each letter in the plain text is matched with the key text using Tabula Recta Columns and Rows respectively. Each letter in the plain text is selected from the column list. Each letter from the key is selected from the row list. The intersection of the column and row for each letter in the tabula recta is the cipher text. The Plain text word "ATTACK" with a key "GO", can be decrypted as "GHZOIY". Vigenère Cipher was modified to be called as Auto Key Cipher in which the Key constitutes of it's actual key followed by the Plain Text to match the length of the Plain Text. The weakness of this cipher is that if the intruder tries to guess some parts of the actual message by applying common sequence of letters, the cipher can be broken. Although this cipher cannot be cracked by Kasiski examination or Index of Coincidence, trying common words can become a way to decode the message. Present techniques include Secure Hashing Algorithm[12](SHA). It is a hashing algorithm based on non-linear functions that performs a hashing function on a given data.It provides strong encryption including BTS, LBC and Andriod Studio. To avoid these drawbacks, a new methodology can be adopted to generate the Key automatically by formulating the Plain Text, which don't pay way for trying common words or any other means to decrypt the Cipher.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIGURE-1 VIGENÈRE ENCRYPTION FOR LETTER 'T' USING TABULA RECTA

In the Table 1.1 , we have a Plain Text letter 'T' matched with key 'O' to get the cipher text 'H'.

Plain Text	A	T	T	A	C	K
Key	G	O	G	O	G	O
Cipher Text	G	H	Z	O	I	Y

TABLE-1 EXAMPLE OF VIGENÈRE CIPHER

As per the Vigenère Cipher, the key would be repeated to match the number of characters in the plain text. In the Table 1, we could observe that the key "GO" is repeated three times to match with the Plain Text "ATTACK". The repeating of the key word becomes the drawback of this Vigenère cipher. This cipher could be broken if the key length is found out using frequency attacks. Hence here we propose a new method of generating the key.

III. METHODOLOGY

In the proposed method, one separate key is used. Instead of repeating the same key throughout the Plain text length, we shall have keys generated for each letter of the plain text. The Key would be generated using the tabula recta. For each letter in the plain text, the key would be matched with the ith row, where i represents the index of the plain text. In the Table 2, we have a Plain Text “ESCAPE”.

Plain Text	E	S	C	A	P	E
KEY	E	T	E	D	T	J

TABLE-2 GENERATING KEY FOR THE WORD ESCAPE

The first letter is E. So, the key is obtained from the first row corresponding to the plain text letter ‘E’. In other words, first letter in column ‘E’. Hence the first letter of the key is ‘E’ itself. Now for the second letter of the plain text ‘S’, the key to be found in the second row corresponding to the letter ‘S’. The second letter in column ‘S’ is the second letter of the key. - ‘T’. The third letter of the key is the third row element of the third Plain Text letter ‘C’- ‘E’. The next letter of the key is the fourth letter in the column ‘A’, which the fourth element of Plain Text. So the Key letter is ‘D’. The letter of the key is the fifth letter of the column ‘ P’., which is the fifth element of the Plain Text. So the Key letter is ‘T’. The last letter of the key is the sixth element of the column ‘E’, which is the sixth letter in the Plain text. So the key letter is ‘J’. The final Key obtained as mentioned in the Table 2 is “ETEDTJ”. This key doesn’t have any repeating characters in it as it was there in traditional Vigenère Cipher. The Plain Text plays a vital role in generating the key. As the Key is generated for each letter individually, each letter from the plain text have unique key letter. As mentioned in Table-2, Letter ‘E’ in plain text is in two positions and two keys letters are ‘e’ and ‘j’ respectively. Similarly, Key has letter ‘T’ obtained twice. But both are key letters for different plain text letters ‘S’ and ‘P’. Now the hackers would not be able to make any possibility of finding either the key or the Plain Text.

A. Generating Key

Key needs to be generated using the Plain Text and it’s Index value ‘i’. Using Tabula Recta, Key is obtained with respect to the Plain Text character and it’s index value.

$$K_i = EL_i(P_i)$$

where K_i represents the key for ith element of plain text, EL_i represents the element in the ith row corresponding to the column P_i, which represents the plain text. It is clearly explained in the Table 1.3.

B. Encryption

Encryption in done in the same method as it is done for standard Vigenère Cipher. The only difference is the new method of generation of Key. After the key is generated for each element of the plain text, the cipher text is obtained using tabula recta as shown in Table 1.1.

The elements of the Plain text are considered in the columns and the elements of the key generated are considered in rows. In the Table 1.3, the first element of the Plain Text ‘E’ is mapped with the first element of the Key ‘E’.

Similarly, the second element of the Plain Text ‘S’ is mapped with the second element of the Key ‘T’. and so on. An algorithm for encryption process can be drafted as given below:

```
Step 1: Input Plain Text : P_T[]
Step 2: Calculate length of Plain Text :
        P_T_Len← strlen(P_T)
Step 3: Repeat for i=0 until i<P_T_Len
        C_T[i] ←P_T[i]. Key_row[i]
Step 4: Output Cipher_Text : C_T[]
```

The flowchart Figure 2, well describes the encryption process.

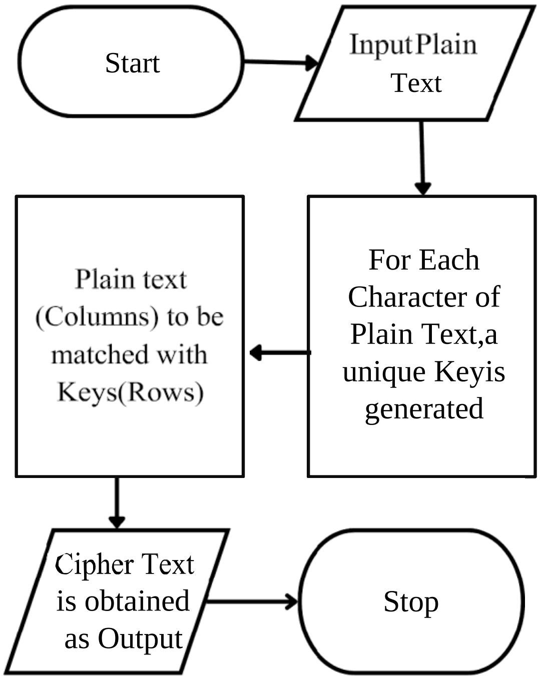

Start
Input Plain Text
For Each Character of Plain Text,a unique Keyis generated
Plain text (Columns) to be matched with Keys(Rows)
Cipher Text is obtained as Output
Stop

Figure 2 Encryption

Using the above methods, we formulate to generate the cipher text for the plain text given in Table 2 using the Tabula recta from Figure 1. The Cipher Text for the first element of Plain Text ‘E’ with key ‘E’ is ‘I’. Similarly, the Cipher Text for the second element of the Plain Text ‘S’ with key ‘T’ is ‘L’. In similar method, the Cipher Text for the entire Plain Text is obtained as described in the following Table 3. The final Cipher Text obtained for ‘ESCAPE’ is ‘ILGDIN’.

Plain Text	E	S	C	A	P	E
KEY	E	T	E	D	T	J
Cipher Text	I	L	G	D	I	N

TABLE-3 ENCRYPTION OF THE WORD ESCAPE

C. Decryption

For decryption of the Cipher Text, the same key which was used for encryption to be used. The rows in the tabula recta define the key and the Cipher Text element are message in a private means so that it doesn’t gets accessed by hackers. The Column corresponding to the key and Cipher Text represents the Plain Text. For the Cipher Text element ‘I’ with key ‘E’, the Plain Text will be ‘E’. Similarly, the Plain Text for the Cipher Text ‘L’ with key ‘T’ is ‘S’. The Cipher Text “ILGDIN” with Key “ETEDTJ” could be decoded as “ESCAPE”. The steps followed for decryption can be described as mentioned below:

```
Step 1: Input Cipher Text : C_T[]
Step 2: Calculate length of Cipher_Text :
        C_T_Len ← strlen(P_T)
Step 3: Repeat for i=0 until i<C_T_Len
Step 4: Output Plain_Text: P_T[]
```

The following flowchart Figure 3, describes the decryption process.

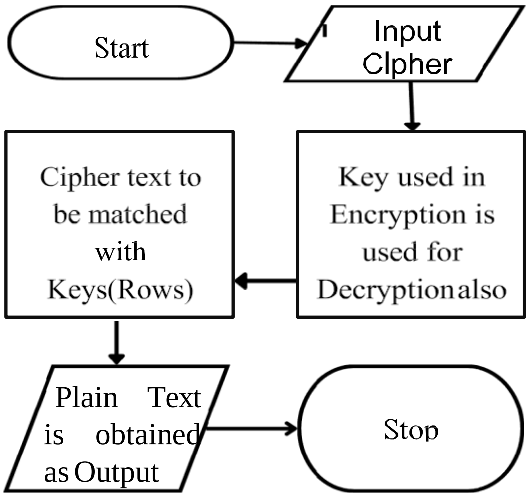

Start
Input Clpher
Key used in Encryption is used for Decryptionalso
Cipher text to be matched with Keys(Rows)
Plain Text is obtained as Output
Stop

Figure 3 Decryption

Decoding the Cipher Text obtained as in the Table 3. can be done in the above mentioned method. Each element of the Cipher Text to be matched with the corresponding Key row to obtain the Plain Text element in the column. The Cipher Text 'I' is matched with the Key in the row header 'E' to obtain the Plain Text element as column header 'E'. Similarly, Cipher Text 'L' matched with Key 'T' to obtain the Plain Text 'S'. The same process is continued for the entire Cipher Text "ILGDIN" to obtain the Plain Text "ESCAPE" as mentioned in Table 4.

Cipher Text	I	L	G	D	I	N
KEY	E	T	E	D	T	J
Plain Text	E	S	C	A	P	E

TABLE 4 DECODING THE CIPHER TEXT "ILGDIN"

IV. CONCLUSION

The Security of a message from can be enhanced by modifying the Vigenère Cipher. The modification is done by avoiding the repetition of the Key and generating a key in such a way that each element of the key corresponds to the index of the Plain Text. Vigenère Cipher which and be decrypted by frequent analysis, can now be modified in the above discussed methods in particular, the method of generating Keys, can be well prevented from attacks. This could surely improve the security of the messages. Future improvements can be done in such a way that the key used for decryption can also be generated automatically instead of using the same key used for encryption. This could add more strength to the security as there won't be any issue in sharing the key generated using the above method, from the sender to receiver.

REFERENCES

[1] Bellare, Mihir, Rogaway, Philip(2005) , " Introduction to Modern Cryptography", p.10.

[2] Hossain Saju, Mahmudul Haque and Hossain Lingcon(2021), " A Hybrid Cryptographic Scheme of modified Vigenère cipher using Randomized Approach for Enhancing Data Security", International Journal of Computer Applications(0975-8887), Volume 183 – No.2.

[3] Khairun Nahar and Partha Chakraborty(2020), " A Modified Version of Vigenère Cipher using 95X95 Table", International Journal of Engineering and Advanced Technology(IJEAT, 2249-8958), Volume-9, Issue-5.

[4] Khan, David(1967), " The Codebreakers", ISBN 978-0-684-83130-5.

[5] Laurence Dwight Smith(1955), " Cryptography: The Science of Secret Writing", p. 81, ISBN 978-0-486-20247-1.

[6] Lenon, Brian(2018), " Passwords: Philology, Security, Authentication", p. 26, ISBN: 978-0-674-98537-7.

[7] Purwidiantoro and Saputro Wibowo(2018), " Super Encryption Concepts using Vigenère Cipher Modification to Produce Colour Imaginary as Cipher Text" in Proceedings of the 1st International Conference on Recent Innovations(ICRI 2018), pp 3029-3025.

[8] Russel, Frank (1999).Information Gathering in Classical Greece. U. Michigan Press. p.117. ISBN 0-472-11064-0

[9] Salomon, David(2005), " Coding for Data and Computer Communications", ISBN 0-387-21245-0.

[10] Salomon, David(2003), " Data Privacy and Security", p. 63, ISBN 0-387-00311-8.

[11] Sands, Kevin(2015), " Top 10 Codes, Keys and Ciphers".

[12] Verma, Shahrukh, Krishna, Goel(2021), "A Critical Review on Cryptography Hashing Algorithm SHA-512", IRJMETS Vol :3, Issuse: 12, e ISSN – 2582 5208