Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 92 (2016) 355 – 360

Procedia Computer Science

2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016)

Srikanta Patnaik, Editor in Chief

Conference Organized by Interscience Institute of Management and Technology

Bhubaneswar, Odisha, India

An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication

Aditi Saraswat[a], Chahat Khatri[a], Sudhakar[a], Prateek Thakral[a], Prantik Biswas[a]*

[a]National Institute of Technology, Kurukshetra, 136119, India

Abstract

Cryptography is one of the most popular fields of study these days as it is necessary to maintain the confidentiality of the data which is sent over the network. There are various cipher techniques available for encrypting the messages such as vernam cipher, mono-alphabetic cipher, poly-alphabetic cipher, etc. One of the most popular cipher techniques is the vigenere cipher. It is a poly-alphabetic cipher technique which uses the vigenere table for the process of encryption of alphabets. This paper extends the vigenere table by including numerical data, so that the numbers can also be encrypted using this technique. It combines the encryption process of vigenere and Caesar cipher for getting the cipher text from the given plaintext and key.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

Keywords: Cryptography, Caesar Cipher, Polyalphabetic cipher, Modified Vigenere Table

1. Introduction

The term cryptography emerges from the Greek word *kryptos*, which means hidden or secret, and *graphein* which means writing. Normally, we do not care if someone is eavesdropping upon us but in some situations confidentiality becomes necessary and we want to protect the information from outsiders. In these situations, the

* Corresponding author. Tel.: +91-954-903-5732.

E-mail address: saraswat.aditi1993@gmail.com.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

doi:10.1016/j.procs.2016.07.390

role of cryptography comes into play. *Cryptography* is the technique to transfer information securely between two parties without getting intervened by external elements. Cryptography involves an algorithm and a key value to convert the information into a format which is un-understandable to anyone except the participants. The algorithm must be efficient and easy to be computed by the participants involved in communication. The key is used along with the algorithm so that we can use the algorithm again and again with different key value as it is very difficult to generate a new algorithm every time we want to share some information with someone. Even if the algorithm is known to external elements, they cannot get the message without any knowledge of key.

The figure illustrates the overall process of cryptography where the plaintext is encrypted using the algorithm and key by the sender whereas the cipher text is decrypted at the receivers end using the reverse process known as decryption. Cryptanalysis is the process of getting the original message from the encoded cipher text illegally, without knowing the algorithm use in the process of encryption

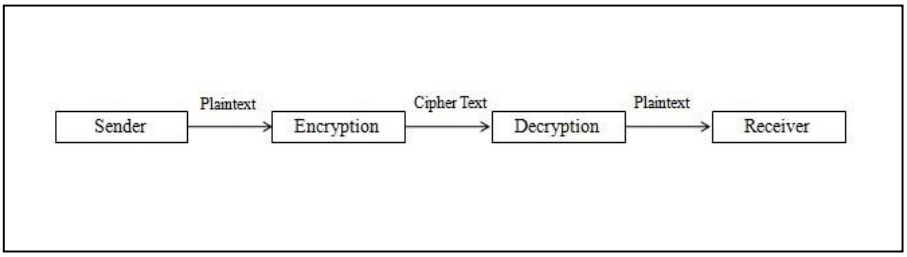

Fig 1. Process of Cryptography

The job of cryptographers is to produce intelligent cipher, whereas the cryptanalysts try to decipher them illegally. The success and competence of the cryptographic technique depends upon the fact that how difficult it is to be broken or cracked by a cryptanalyst. In this paper, vigenere cipher table has been modified to make the cryptanalysis process more difficult. Section 2 discusses some of the methods which were used to make the process of substitution cipher techniques more secure. Section 3 discusses various poly-alphabetic cipher techniques in detail. In section 4, we have proposed our new vigenere table which provides better level of security and attempts to encrypt the numeric data also along with character values. Finally, conclusion is done in section 5.

2. Related Work

Nacira et al. [1] proposed an extension to vigenere cipher. They provide two methods to include numbers in vigenere cipher. Firstly, a matrix V (26,10) is applied where decimal numbers are represented by columns and rows represent alphabets. Secondly, a letter is used to substitute each number, corresponding in order to alphabets. The theta -Vigenere algorithm is then applied to obtain the cryptogram. The paper explains that the cipher is dependent upon encryption degree; that is a part of key, and not only on the key length. For better security, the degree of encryption must be increased.

Senthil et al. [2] presented some new additions in the vigenere and Caesar cipher technique by using some rigorous mathematical tools which uses a prime factor, its primitive roots and their generator. The shifts and substitutions performed in both the cipher techniques are not uniform and follow a particular scientific procedure.

Blair [3] presents a new programming language known as HERCL. The aim of this programming language is to allow new programs creation by combining code patches from various parts of other programs. Smaller patches follow larger patches resulting in a random search strategy that can be applied globally and is called as Hierarchical Evolutionary Recombination.

Pal et al. [4] provides bit level conversion of inconsistent block length characters for encryption. Here they have considered a block of 16 characters/128 bits. Substitution technique is being followed on the block of characters along with transpositions using multidimensional array. The block is being operated with one-time sub key which will produce intermediate result of similar length. The previous text block is combined with consecutive 8 characters/64 bits of the plain text and gives a block containing 192 bits. This is used as present block of text which produces a new text block containing 24 characters with same technique. Next 8 characters are considered with previous block and same technique is applied to give a block of 256 bits. If there are more than 32 characters in plain text i.e. 256 bits then every 256 bit block is XORed with previous 256 bits block other than the first block. At the end bits are being chosen from MSB position and chosen bits are processed through a special substitution technique to give final encrypted block.

Piper [5] proposed the necessity of information security using the basic concept of cryptography. This paper involves the concept of encrypting the messages which are being delivered from one person to another using a public network. For encryption they are using cryptography as one of the major tool. The basic idea behind the encryption is to use another secret algorithm other than the one which is already there for encryption of the message. It must be beneficial that the whole system is not dependent on the secrecy of one algorithm. Now one method by which the attacker can attack this message just by using hit and trial method of all possible combinations known as exhaustive key search. So we must have enough keys to keep the attacker away from message as long as possible.

3. Poly-alphabetic Cipher Techniques

Various techniques are used to codify the plain text into the cipher text, by making use of some algorithm along with the key, known as cipher techniques. There are two types of cipher techniques: Substitution Cipher and Transposition Cipher. Transposition Cipher shifts the plain text characters into new positions in order to obtain the cipher text by making use of some algorithm Substitution Cipher as the name suggests replaces or substitutes the characters in the plain text with some other characters based on some algorithm. One of the most commonly used and secure substitution cipher technique is poly-alphabetic cipher technique which overcomes the disadvantages of previously used cipher techniques. In this, a particular character needs not to be replaced with the same character for each of its occurrence in the entire message like mono-alphabetic cipher technique. Instead, every time the same character is replaced by some different character for its occurrence in the message which makes it more secure as compared to various other techniques. There are many different algorithms which makes use of poly-alphabetic cipher techniques for secure communication. Various poly alphabetic cipher techniques are as follows:

3.1 Vigenere Cipher: The vigenere cipher technique encrypts alphabetic text with the help of various caesar ciphers on the basis of the letters of some keyword. In this technique, a shifting mechanism is used, which shifts the characters of the plain text by different amount using the vigenere table. The vigenere table proposed in this technique is used further to implement many different algorithms. According to this table, the plaintext CALLMEATNINE will be replaced by cipher text CTELOOAMGIPO using Key ATTACKATTACK. The

vigenere table is shown in figure 2 below.

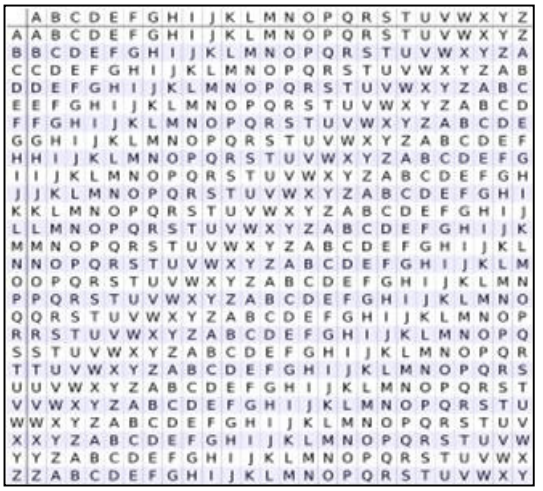

Fig 2. Vigenere Table

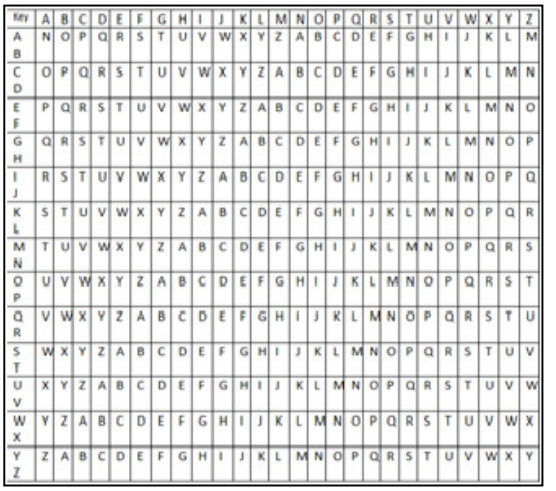

Fig 3. Porta Table

3.2 Autokey Cipher: The Autokey Cipher is similar to Vigenere cipher technique. The only difference is that, instead of developing the keyword by repeating one word again and again, the keyword is developed by affixing the keyword at the beginning of the plain text. It uses the vigenere table only, for the purpose of encryption and decryption. The plaintext CALLMEATNINE now will use the key ATTACKCALLME to produce the cipher text CTELOOCTYTZI.

3.3 Beaufort Cipher: It uses the same table as that of vigenere cipher but with a different technique for encryption. Here, we search for the plaintext letter in the first row of the table and start searching for the keyword letter in the particular column. After finding it, we trace to the leftmost letter in that row, which is our cipher for the given plain text letter. The plaintext CALLMEATNINE will now generate cipher text XTIPQGAAGSPG using key ATTACKATTACK.

3.4 Running Key Cipher: It is similar to the vigenere cipher technique. The difference is in the process of choosing the keyword. In vigenere cipher, a keyword is chosen which keeps repeating itself; whereas in this technique the keyword is selected from a particular book to match the length of the plain text, which is only used once and then discarded. The plain text CALLMEATNINE will use the random key ONCEUPONATIM to generate cipher text QNNPGTOGNBVQ.

3.5 Porta Cipher: The porta cipher technique is similar as that of the vigenere cipher technique; the only difference is that it uses 13 pairs of alphabets as keys, instead of using all the 26 alphabets individually. In this way two different key characters will be able to generate same enciphered text for a given plain text character. The porta table is shown in figure 3 above. The plaintext CALLMEATNINE using the key ATTACKATTACK will produce cipher text PWHYAWNPJVBW in this case.

4. Proposed Work

In the poly-alphabetic cipher tables discussed in the previous section, there are certain disadvantages. Firstly, we cannot include the numerals or digits in the plain text, as the tables do not provide any facility to

encrypt them directly. Secondly, as a result of the prior problem, the numeric data is also written as alphabets due to which the length of the plain text, as well as that of the key, increases. To remove the above stated disadvantages we are proposing a new table named modified vigenere table for the poly-alphabetic cipher techniques. This table includes the digits along with the alphabets. Here, the alphabets (A-Z) ranges from values (0-25) and the digits (0-9) are appended after the alphabets with values (26-35).

In our method of encryption, we have combined the encryption techniques of Vigenere and Caesar Ciphers. The first row represents the key character and the first column represents the plaintext characters. Firstly, we take an intersection of the key value and the plain text character in the modified vigenere table. And after getting the intersection character, we add 3 to it to get the cipher character. Finding the intersection of key character and the plain text character is equivalent to adding the numeric value of both and then taking mod 36 of the result.

The general formula for the above stated process of encryption is:

$C = (P+K) \bmod 36 + 3$

In the decryption process, we find the cipher character in the key character column, and then we subtract three from the first character in that row to obtain the plain text character, corresponding to that cipher text character.

The general formula for the above decryption process is as follows:

$P = ((C-3)-K) \bmod 36$

As an advantage of it, we would be able to include digits in the plaintext which will reduce the length of the plain text and the key used. Another advantage is that the complexity of the encrypting process will also increase as the possible number of replacement for each alphabet or digit will also increase by ten. The table that we are proposing is given below. So, now the plaintext length will get reduced along with the length of key. The plaintext CALLMEAT9 will use key ATTACKATT to produce cipher text FW7ORRDFV.

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

Fig 4. Modified Vigenere Table

5. Conclusion

This paper incorporates the various cipher techniques available. It majorly focuses on the poly alphabetic cipher techniques and the vigenere table. In this paper we extend the vigenere table by including the digits in the table so that numerical data can also be encrypted using the new proposed table. It also reduces the size of the plaintext, in case numbers are present in the plain text and also make cryptanalysis a difficult task. In future, the concept of introducing the special symbols in modified table can be added so as to make the process of cryptanalysis more complex.

References

[1] Nacira G Z,.Abdelaziz A. The θ -Vigenere Cipher Extended To Numerical Data, *Proceedings of International Conference on Information and Communication Technologies: From Theory to Applications*, 2004. DOI: 10.1109/ICTTA.2004.1307807

[2] Senthil K, Prasanthi K, Rajaram R. A Modern Avatar Of Julius Caesar and Vigenere Cipher. *Proceedings of IEEE International Conference on Computational Intelligence and Computing Research*, 2013, Enathi, Tamilnadu, India. http://dx.doi.org/10.1109/ICCIC.2013.6724109

[3] Blair A. Learning The Caesar And Vigenere Cipher by Hierarchical Evolutionary Re-combination, *Proceedings of IEEE Congress on Evolutionary Computation* June 20-23, Cancun, Mexico, 2013.

[4] Pal J K, Mandal J K, Gupta S. Composite Transposition Substitution Chaining Based Cipher Technique, *Proceedings of 16th International Conference on Advanced Computing and Communications,* 2008, Chennai, Tamil Nadu India.

[5] Piper F. Encryption.*Proceedings of European Conference On Security and Detection*, 28-30 April 1997, IEEE, 1997.