Improving Security of Vigenère Cipher by Double Columnar Transposition

Nishith Sinha
Department of Computer Science and Engineering
Manipal Institute of Technology,
Manipal University, Manipal

Kishore Bhamidipati
Assistant Professor
Department of Computer Science and Engineering
Manipal Institute of Technology,
Manipal University, Manipal

ABSTRACT

Protecting data from malicious attacks during storage and transmission is the reason for using encryption. Encryption can be achieved by two methods – Transposition and Substitution. Transposition refers to changing the order of characters in a given text. On the other hand, substitution is the process of replacing each character of the plaintext with some other character. Using a combination of transposition and substitution for encryption leads to greater security when compared to using either of them separately. Vigenère Cipher is a poly-alphabetic cipher. It is based on the substitution technique which uses multiple substitution alphabets. In this paper, we introduce double columnar transposition on Vigenère Cipher to enhance its security making cryptanalysis difficult.

General Terms

Encryption, Security, Cryptanalysis

Keywords

Transposition, Substitution, Poly-Alphabetic Cipher, Double Columnar Transposition

1. INTRODUCTION

The term cryptography, derived from the Greek word Kryptos is used to describe something that is hidden, secret or veiled. In the world of data communication, cryptography is the art and science of creating non readable data or cipher so that intended person is only able to read the data [1]. Cryptography is composed of two processes – encryption and decryption. Encryption is the process of converting the data to be communicated or plaintext into a form which is readable or understandable only by the authorized party, known as cipher text. On the other hand, the process of converting cipher text into plaintext is known as decryption. The objective of cryptography is to fulfill four basic objectives- authentication, privacy/confidentiality, integrity and non-repudiation [2]. Another important term in this context is cryptanalysis. Cryptanalysis is the process of deciphering encrypted communication without the knowledge of the key.

Vigenère Cipher involves the encryption of alphabetic plaintext by a series of different Caesar based on the letters of the keyword. In Caesar Cipher, each letter of the plaintext is shifted by some number of places; for example in Caesar Cipher of shift 5, character 'N' would become 'S', 'T' would become 'Y' and so on. Vigenère Cipher consists of several Caesar Ciphers which are applied in sequence with different shift values. In Vigenère Cipher, letters A-Z are taken to be numbers 0-25. Mathematically, Vigenère Cipher can be written as follows-

Encryption: $C_i = (P_i + K_i) \bmod 26$ – (Equation 1)

Decryption: $P_i = (C_i – K_i) \bmod 26$ – (Equation 2)

Where $C = C_0 \ldots C_n$ is the Cipher text, $P = P_0 \ldots P_n$ is the Plaintext and $K = K_0 \ldots K_m$ is the key.

Vigenère Cipher occurs from some flaws. The most important of them is the Kasiski examination which is also called the Kasiski test [3]. It takes advantage of the fact that repeated words may be encrypted using the same key letters, leading to repeated groups in the cipher text. In this paper, we introduce the concept of double columnar transposition on Vigenère Cipher in order to make cryptanalysis by Kasiski examination difficult.

Columnar transposition is a method in which the plaintext is written out in a 2-Dimensional matrix of a fixed size and the cipher text is created by reading the plaintext column by column. The order in which columns will be read is decided by the key. Columnar transposition is of two types – regular columnar transposition and irregular columnar transposition. The major difference between the two is that in regular columnar transposition, blank spaces are filled with null whereas in irregular columnar transposition, blank spaces are left blank. In double columnar transposition, an intermediate cipher text is obtained by doing a columnar transposition on the plain text. This is followed by another columnar transposition on the intermediate cipher text to get the final cipher text. Double columnar transposition is more secure than single columnar transposition. This is because single columnar transposition can be attacked by guessing the 2-Dimensional matrix size, writing it out in columns and then looking for possible anagrams.

2. RELATED WORK

Vigenère Cipher uses polyalphabetic cipher [4] which was considered to be unbreakable and secure till 1917. But later it was broken by Kasiski and Friedman. They exploited the repeating nature of the key to break it. If a cryptanalyst knows the length of the key, then Vigenère Cipher can be treated as multiple Caesar Ciphers which can be easily broken. The Kasiski test can help determine the key length [5]. Over the years, many improvements have been suggested to improve the security of Vigenère Cipher. Authors in [6] used of Linear Feedback Shift Registers for improving security of Vigenère Cipher. In [7], authors have proposed usage of reversible

square matrices for encryption and decryption using Vigenère Cipher. Another significant attempt is called Alpha-Qwerty Cipher [8]. This was an advanced Vigenère Cipher which worked on a set of 92 characters by adding case sensitivity, digits and other special symbols to existing Vigenère Cipher which was of 26 characters. However, this enhancement still does not provide resistance to Kasiski attack. In this paper, we try to enhance the security of Vigenère Cipher by converting it into a product cipher, thereby providing resistance to Kasiski attack.

3. PROPOSED TECHNIQUE

3.1 Modified Vigenère Cipher Algorithm

Proposed, Modified Vigenère Cipher Algorithm would require two keys to convert the plaintext into cipher text. The two keys, K_1 and K_2 would be used for substitution and transposition respectively. K_1 would be constituted of a string of alphabets and K_2 would be constituted of unique digits forming an integer. The Vigenère table or Vigenère square for encryption would be used to for substitution in accordance with the varying shift values derived from the K_1. This would give the first intermediately cipher text C'. In case of classical Vigenère Cipher, C' would have been the final cipher text obtained to be sent across to the sender. However, in the proposed Modified Vigenère Cipher Algorithm, we apply transposition to C' using K_2. The number of digits constituting K_2 is calculated. C' is then written out in rows of the same length as the number of digits in K_2.

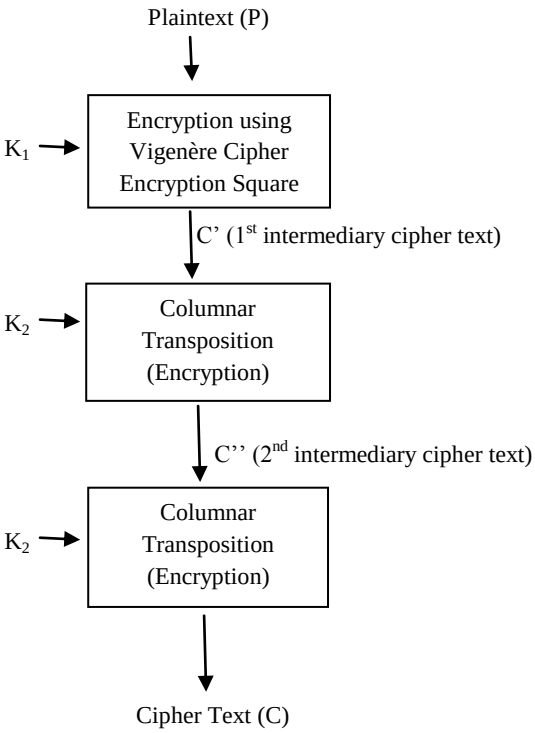
The second intermediate cipher text C'' is obtained by writing out the text obtained column by column. The order in which columns are chosen is defined by the key K_2. The second intermediate cipher text C'' is then subjected to the same transposition algorithm. C'' is written out in rows of the same length as the number of digits in K_2. The final cipher text, C from the algorithm is obtained by writing out the text obtained column by column. The order in which columns are chosen is defined by the key K_2. This completes the process of encryption using modified Vigenère Cipher algorithm.

The decryption process for the proposed Modified Vigenère Cipher Algorithm is similar to the encryption process. Both keys, K_1 and K_2 that were used in the encryption process would be required. The final cipher text, C is written out column by column using K_2. The matrix formed by this process is then written out row by row to form the first intermediate plaintext P''. This first intermediary plain text P'' is now written out column by column using K_2. The matrix formed by this process is then written out row by row to form the second intermediary plain text P'. The final plaintext P, is obtained from P' by the classical Vigenère Cipher decryption process i.e. by using either Equation 2, mentioned in Section 1.

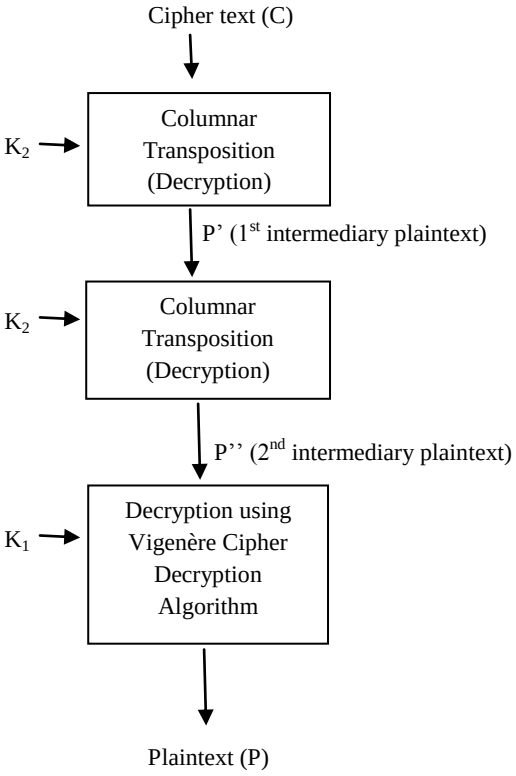
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

3.2 Encryption Process



3.3 Decryption Process



3.4 Comparison with Vigenère Cipher

Vigenère Cipher is a polyalphabetic cipher. No permutation is involved in the encryption process. This exposes Vigenère Cipher to Kasiski attack. The attack is based on finding repetitive patterns in the cipher text. The repetitive pattern should be three characters or more in length. If such is the case, then we can conclude that the distance between repetitive patterns is likely to be the key length or integral multiples of the key length.

However, in case of proposed Modified Vigenère Cipher, the cipher text obtained from polyalphabetic substitution is subjected to permutation in the double columnar transposition phase. Permutation ensures that proposed Modified Vigenère Cipher is resistant towards Kasiski attack. In this way, the proposed algorithm is better than the existing one.

4. EXPERIMENTAL RESULTS

4.1 Example - 1

A. Encryption

In Example – 1, let the plaintext and keys for encryption be as follows

Plaintext (P)	WEAREDISCOVEREDSAVEYOURSELF
Key 1 (K_1)	DECEPTIVEDECEPTIVEDECEPTIVE
Key 2 (K_2)	4 3 1 2 5 6 7

Using the Vigenère Cipher encryption square on plaintext using K_1, we get the 1st intermediary cipher text as follows –

C' = ZIC**VTW**QNGRZG**VTW**AVZHCQYGLMGJ

It can be seen as the intermediary cipher text has the pattern 'VTW' repeating twice. This makes it susceptible to Kasiski attack. To make this resistant to Kasiski attack, we proceed with the next phase of encryption. The 1st intermediary cipher text C' is subjected to columnar transposition using K_2 as follows –

4	**3**	**1**	**2**	**5**	**6**	**7**
Z	I	C	V	T	W	Q
N	G	R	Z	G	V	T
W	A	V	Z	H	C	Q
Y	G	L	M	G	J	

Reading the above matrix column wise with respect to K_2, we get the 2nd intermediary cipher text as follows -

C'' = CRVLVZZMIGAGZNWYTGHGWVCJQTQ

To obtain the final cipher text C, we apply another round of columnar transposition on the 2nd intermediary cipher text C'' using K_2 as the key.

4	**3**	**1**	**2**	**5**	**6**	**7**
C	R	V	L	V	Z	Z
M	I	G	A	G	Z	N
W	Y	T	G	H	G	W
V	C	J	Q	T	Q	

Reading the above matrix column wise with respect to K_2, we get the final cipher text as follows –

C = VGTJLAGQRIYCCMWVVGHTZZGQZNW

B. Decryption

In the first phase, the cipher text is written out column by column using K_2.

4	**3**	**1**	**2**	**5**	**6**	**7**
C	R	V	L	V	Z	Z
M	I	G	A	G	Z	N
W	Y	T	G	H	G	W
V	C	J	Q	T	Q	

The 1st intermediary plaintext P' is obtained by reading the matrix obtained above, row by row.

P' = CRVLVZZMIGAGZNWYTGHGWVCJQTQ

The 1st intermediary plaintext is again subjected to decryption by columnar transposition. In this process, the intermediary plaintext P' is written out column by column using K_2.

4	**3**	**1**	**2**	**5**	**6**	**7**
Z	I	C	V	T	W	Q
N	G	R	Z	G	V	T
W	A	V	Z	H	C	Q
Y	G	L	M	G	J	

The 2nd intermediary plaintext P'' is obtained by reading the matrix obtained above, row by row.

P'' = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

In the final phase of decryption, the 2nd intermediary plaintext is subjected to decryption using the Vigenère Cipher Decryption Algorithm using K_1.

2nd Intermediary Plaintext (P'')	ZICVTWQNGRZGVTWAVZHCQYGLMGJ
Key 1 (K_1)	DECEPTIVEDECEPTIVEDECEPTIVE

The final plaintext P, obtained by this process is as follows –

P = WEAREDISCOVEREDSAVEYOURSELF

4.2 Example – 2

A. Encryption

In Example – 2, let the plaintext and keys for encryption be as follows

Plaintext (P)	ALICEWASBEGINNINGTOGETVERYTIRED
Key 1 (K_1)	WONDERLANDWONDERLANDWONDERLANDW
Key 2 (K_2)	1 3 2 7 6 4 5

Using the Vigenère Cipher encryption square on plaintext using K_1, we get the 1st intermediary cipher text as follows –

C' = WZVFINLSOHCWAQMERTBJAHIHVPEIEHZ

The 1st intermediary cipher text C' is subjected to columnar transposition using K_2 as follows –

1	**3**	**2**	**7**	**6**	**4**	**5**
W	Z	V	F	I	N	L
S	O	H	C	W	A	Q
M	E	R	T	B	J	A
H	I	H	V	P	E	I
E	H	Z				

Reading the above matrix column wise with respect to K_2, we get the 2nd intermediary cipher text as follows -

C'' = WSMHEVHRHZZOEIHNAJELQAIIWBPFCTV

To obtain the final cipher text C, we apply another round of columnar transposition on the 2nd intermediary cipher text C'' using K_2 as the key.

1	**3**	**2**	**7**	**6**	**4**	**5**
W	S	M	H	E	V	H
R	H	Z	Z	O	E	I
H	N	A	J	E	L	Q
A	I	I	W	B	P	F
C	T	V				

Reading the above matrix column wise with respect to K_2, we get the final cipher text as follows –

C = WRHACMZAIVSHNITVELPHIQFEOEBHZJW

B. Decryption

In the first phase, the cipher text is written out column by column using K_2.

1	**3**	**2**	**7**	**6**	**4**	**5**
W	S	M	H	E	V	H
R	H	Z	Z	O	E	I
H	N	A	J	E	L	Q
A	I	I	W	B	P	F
C	T	V				

The 1st intermediary plaintext P' is obtained by reading the matrix obtained above, row by row.

P' = WSMHEVHRHZZOEIHNAJELQAIIWBPFCTV

The 1st intermediary plaintext is again subjected to decryption by columnar transposition. In this process, the intermediary plaintext P' is written out column by column using K_2.

1	**3**	**2**	**7**	**6**	**4**	**5**
W	Z	V	F	I	N	L
S	O	H	C	W	A	Q
M	E	R	T	B	J	A
H	I	H	V	P	E	I
E	H	Z				

The 2nd intermediary plaintext P'' is obtained by reading the matrix obtained above, row by row.

P'' = WZVFINLSOHCWAQMERTBJAHIHVPEIEHZ

In the final phase of decryption, the 2nd intermediary plaintext is subjected to decryption using the Vigenère Cipher Decryption Algorithm using K_1.

In the final phase of decryption, the 2nd intermediary plaintext is subjected to decryption using the Vigenère Cipher Decryption Algorithm using K_1.

2nd Intermediary Plaintext (P'')	WZVFINLSOHCWAQMERTBJAHIHVPEIEHZ
Key 1 (K_1)	WONDERLANDWONDERLANDWONDERLANDW

The final plaintext P, obtained by this process is as follows –

P = ALICEWASBEGINNINGTOGETVERYTIRED

5. CONCLUSION AND FUTURE WORK

Vigenère Cipher is a poly-alphabetic substitution cipher and is susceptible to Kasiski attack. Due to this, today there is a very limited usage of Vigenère Cipher. To enhance its security and make it resistant to Kasiski attack, this paper proposes modified Vigenère Cipher which incorporates double columnar transposition, making it a product cipher. Hence, the proposed algorithm becomes difficult to cryptanalyze. At the same time, the computational complexity is much lesser than most modern ciphers, making it a fit choice for light weight applications where resources are limited. Lesser computational complexity also ensures that the time required for encryption and decryption is significantly lesser than most modern ciphers. As a part of future work, we could consider different transposition algorithm to be combined with Vigenère Cipher with the intent of enhancing its security.

6. REFERENCES

[1] Atul Kahate (2009), *Cryptography and Network Security*, 2nd Edition, McGraw-Hill.

[2] Overview of Cryptograhy- http://www.garykessler.net/library/crypto.html.

[3] William Stallings: "Cryptography and Network Security: Principles and Practices" 4th Edition,

[4] Martin, Keith M. (2012). Everyday Cryptography. Oxford University Press. p. 142. ISBN 978-0-19-162588-6.

[5] Cryptanalysis of Vigenère Cipher- http://www.nku.edu/~christensen/section%2012%20vigenere%20cryptanalysis.pdf

[6] Abdul Razaq ,Yasir Mahmod, Faroq Ahmed, Ali Hur : Strong Key Machanism Generated by LFSR based Vigenère Cipher – 13th International Arab Conference on Information Technology (December 2012)

[7] Yumnam Kirani Singh :Generalization of Vigenère Cipher - ARPN Journal of Engineering and Applied Sciences (January 2012)

[8] Alpha-Qwerty Cipher: An Extended Vigenère Cipher- Advanced Computing, An International Journal, Vol. 3, No. 3, May 2012.