Vertically Scrambled Caesar Cipher Method

Asiya Abdus Salam
CIT
University of Dammam

Ruba Mahmoud Al Salah
CIT
University of Dammam

ABSTRACT
In this paper, a new technique for protected and locked broadcasting of message is presented. This approach uses improved version of ciphering with the combination of double phase encryption. To ripen this method of encryption, a simple technique of vertically selecting the text for ciphering is used. A 6 x 6 matrix based on the alphabets used in the text message. If the message is lengthy, the matrix can duplicate itself accordingly. Message will be fit in the matrix and remaining cells of the matrix will be filled by alphabets. After getting vertically scrambled text, substitution techniques for ciphering is used further to ensure secured transfer of message. The receiver will get to know about the length of the text and shift key for decryption procedure. By using this double phase encryption, the transmission of message will become more secure and robust. The main target of the technique proposed in this paper is that the information cannot be customized by any outsider or intruder.

General Terms
Modified Encryption / Decryption Method, Modified Caesar Cipher, Security Algorithm

Keywords
Caesar cipher, vertically scrambled text, encryption, decryption, double phase encryption method.

1. INTRODUCTION
In ancient times, Greek used word cryptography meaning secret writing. This method was used to share private messages publicly. Nowadays, in the times of technologies, cryptography is used for sending and receiving messages securely over protected medium [1]. Cryptography is the area of study which creates protected message using encryption and decryption methods and techniques. Cryptography is classified using Symmetric Key and Asymmetric Key [1]. Using encryption algorithm, message is encrypted and vice versa for decryption used by receiver.

In symmetric key, same key is used for encryption and decryption procedure. It is much useful and prompt approach as compared to asymmetrical key cryptography.

The message which has been encrypted is called ciphertext through which an algorithm is followed to transfer the message into ciphertext. Decryption method is followed in the reverse order to decrypt the ciphertext into original method with the information of length of message. Therefore, in the field of encrypting and decrypting, the process of transformation of plaintext to ciphertext with the use of special key takes place.

Caesar Cipher is a substitution type cipher in which every single alphabet in the message is substituted by a letter that has some fixed number of positions down the alphabet. Ciphers make textual statement vague to anyone who might unjustifiably seize it. Hence, it's a method for encoding characters to hide their values.

Caesar Cipher being the first encryption method was invented by Julius Caesar to converse with his soldiers for the sake of securing messages. His standard algorithm included shifting each letter three places down the alphabet in the message. One of the powerful points of this method is its ease and robustness. In combination of vertically scrambled strategy with Caesar ciphering makes it a better approach as shown in the Fig1.

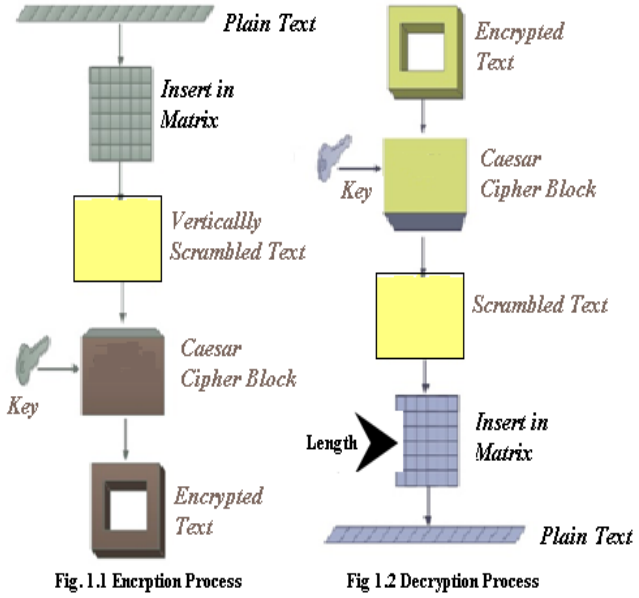


Fig 1: Encryption and Decryption Process

2. PREVIOUS WORK
Encryption is the process of converting information into ambiguous form for unauthorized users. In old era, this method was used in order to send private and confidential message which becomes a subject of study. Many techniques of encryption came into being with respect to time.

The two main techniques include method of substitution and transposition. In substitution method, plaintext alphabets are exchanged by other alphabets or symbols while transposition method is based on the swapping technique to have the encrypted text [4].

There are many other cipher techniques like Caesar cipher, playfair cipher, Hill cipher and Vigenere Cipher [5]. In modern times, encryption methods are based on substitution and transposition for ciphering the text for increasing the

security of data. For block cipher, Data Encryption Standard (DES) is used that uses 56 bit key and 64 bits for data encryption.

Unauthorized users can use lots of different methods to decipher the text with the key. Previously identification of permutation, substitute and vigenere ciphers were done using frequency analysis [6]. Pattern Recognition methods were also formed to know the pattern of hidden information. Other cipher like stream cipher SEAL and enhanced RC6 had been identified using neural networks [8].

Some inventors utilize the registers to enhance the functionality of the technique. They make use of flip flops for getting the best result. LFSR circuit was also used to generate random sequences, modified version of Playfair cipher using LFSR and transposition matrix, which appeared to be cost effective in comparison to other methods. The actual Playfair cipher is relatively easy to break because it still lags behind few holes in the method.

Most recent invention in this field is the modification in the playfair cipher. Different attempts are made to use playfair cipher using table in the form of different number of matrix. Cryptography is vast area in which different techniques can be applied to make this field better and more secure.

Transposition ciphering method is common method used for encryption in which alphabets position in the message is changed. Substitution method has been improved by number of researchers, sometimes with random number generation and sometimes by using alphanumeric and symbols and also combination of keys for higher secrecy.

3. PROPOSED TECHNIQUE

In this approach of encryption, a type of substitution cipher is used by replacing the text with the alphabets for better security enhancement. Plaintext is first scrambled vertically. For this purpose, message is placed in a matrix of size 6 x 6. If the message is lengthy and contains more letters not fit in the defined dimension then, more than one matrix of same size will be used. Once the text is scrambled vertically, Caesar cipher method is applied on its outcome with the shift key. The reason for doing this is to protect information in digital exchange of data electronically.

If we analyze this approach technically, it says that it involves replacing every alphabet of plaintext using shift key. If the shift key is 2 then it means the Caesar cipher substitutions will shift alphabet by 2 as shown below.

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
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

3.1 Important Characteristics

1. Matrix of size 6 x 6.
2. Vertically scrambled method.
3. The transformation of result from vertically scrambled method to ciphertext for no information lost.
4. Key from symmetric approach.
5. The way in which text is processed. Actually it is:

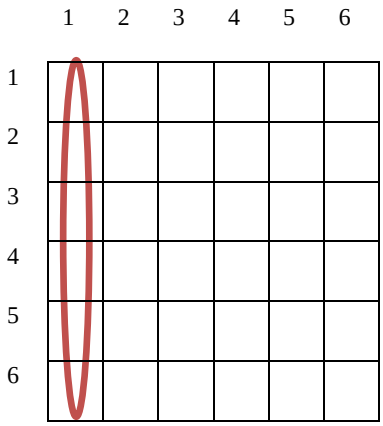
Ciphertext = vertically scrambled text + Key mod 26

4. ALGORITHM

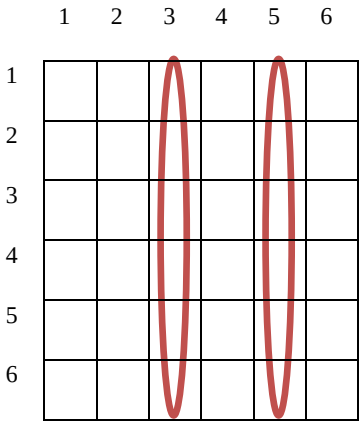
4.1 Analysis of Algorithm

To encrypt a plaintext in our proposed algorithm, apply the following steps:

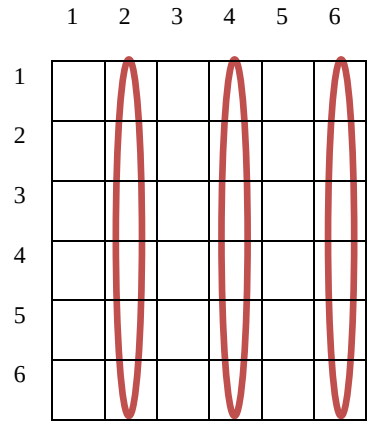
1. Construct a 6 X 6 matrix by filling the characters of the plaintext from left to right and top to bottom.
2. Fill the remaining cells of the matrix with alphabets from A to Z.
3. Get the elements of the matrix as follows:
   - Get the elements of the first column of the matrix.



   - Next, get the elements of the 3rd and 5th columns.



   - Now, get the elements of the 2nd, 4th and 6th columns.



4. Encrypt the resulting concatenated texts you get in step 3 using Caesar Cipher.

To decrypt the ciphertext at the receiver side follow the steps below:

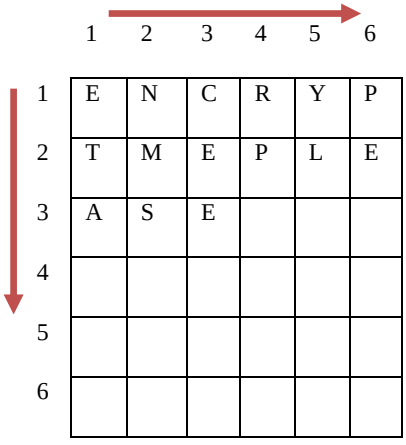
1. Construct a 6 X 6 matrix by filling the characters of the ciphertext vertically as follows: 1st, 3rd, 5th, 2nd, 4th and 6th columns.
2. Now, get the ciphertext from the matrix from left to right and top to bottom.
3. Decrypt the ciphertext using the same algorithm used in the encryption.

4.2 Paradigm

To encrypt a plaintext in our proposed algorithm, apply the following:

1. Construct a 6 X 6 matrix by filling the characters of the plaintext from left to right and top to bottom.

Plaintext: ENCRYPT ME PLEASE

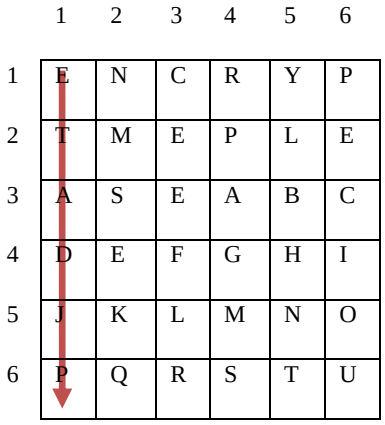


	1	2	3	4	5	6
1	E	N	C	R	Y	P
2	T	M	E	P	L	E
3	A	S	E			
4						
5						
6						

2. Fill the remaining cells of the matrix with alphabets from A to Z.

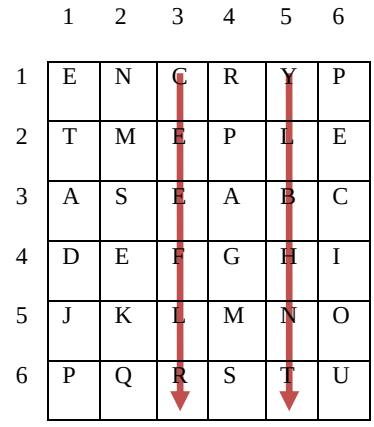
	1	2	3	4	5	6
1	E	N	C	R	Y	P
2	T	M	E	P	L	E
3	A	S	E	A	B	C
4	D	E	F	G	H	I
5	J	K	L	M	N	O
6	P	Q	R	S	T	U

3. Get the elements of the matrix as follows:
   a. Get the elements of the first column of the matrix.



	1	2	3	4	5	6
1	E	N	C	R	Y	P
2	T	M	E	P	L	E
3	A	S	E	A	B	C
4	D	E	F	G	H	I
5	J	K	L	M	N	O
6	P	Q	R	S	T	U

   b. Next, get the elements of the 3rd and 5th coloumns.



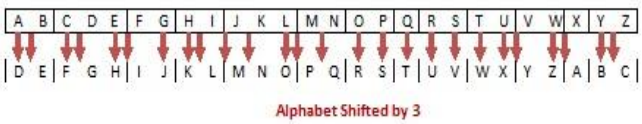
	1	2	3	4	5	6
1	E	N	C	R	Y	P
2	T	M	E	P	L	E
3	A	S	E	A	B	C
4	D	E	F	G	H	I
5	J	K	L	M	N	O
6	P	Q	R	S	T	U

- Now, get the elements of the 2nd, 4th and 6th columns.

	1	2	3	4	5	6
1	E	N	C	R	Y	P
2	T	M	E	P	L	E
3	A	S	E	A	B	C
4	D	E	F	G	H	I
5	J	K	L	M	N	O
6	P	Q	R	S	T	U

c. Text: ETADJP CEEFLR YLBHNT NMSEKQ RPAGMS PECIOU

4. Encrypt the resulting concatenated texts you get in step 3 using Caesar Cipher using the key (Shift of 3) and send the message.



Ciphertext: HWDGMS FHHLOU BOEKQW QPVHNT USDJPV SHFLRX

Decryption is done in reverse as follows:

1. Construct a 6 X 6 matrix by filling the characters of the ciphertext vertically as follows: 1st, 3rd, 5th, 2nd, 4th and 6th columns.

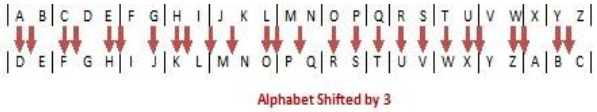
	1	2	3	4	5	6
1	H	Q	F	U	B	S
2	W	P	H	S	O	H
3	D	V	H	D	E	F
4	G	H	I	J	K	L
5	M	N	O	P	Q	R
6	S	T	U	V	W	X
	1	**4**	**2**	**5**	**3**	**6**

2. Now, get the ciphertext from the matrix from left to right and top to bottom.

	1	2	3	4	5	6
1	H	Q	F	U	B	S
2	W	P	H	S	O	H
3	D	V	H	D	E	F
4	G	H	I	J	K	L
5	M	N	O	P	Q	R
6	S	T	U	V	W	X

Ciphertext: HQFUBS WPHSOH DVHDEF GHIJKL MNOPQR STUVWX

Decrypt the ciphertext using Caesar Cipher with key (Shift 3).



5. CONCLUSION AND FUTURE WORK

.Cryptography's security system provides solution against malicious attack by making the message hard to be readable and understandable. This secure means help to improve protection. Vertically scrambling of text and then using Caesar cipher algorithm ensure new technique of secure data transfer. Future work includes exploring more techniques in providing protection and confidential delivery of information with variety of algorithms and their combination.

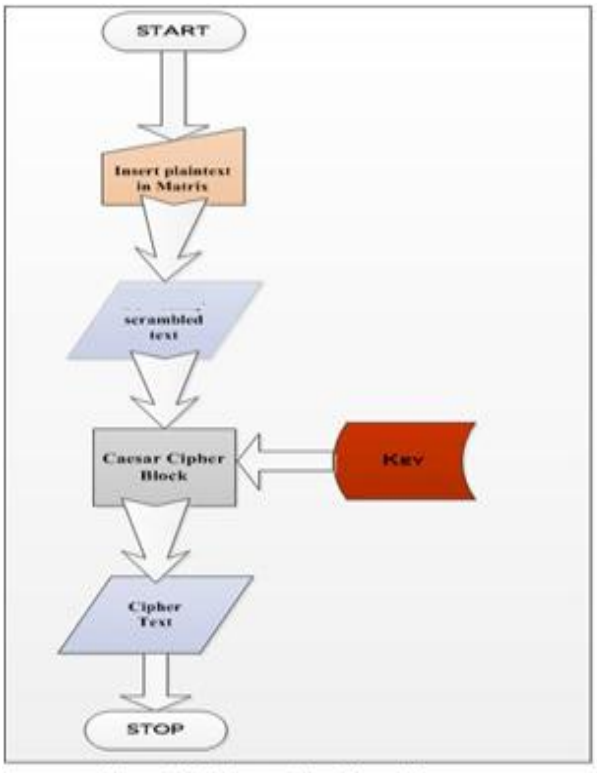


Figure 2.1 Encryption Algorithm

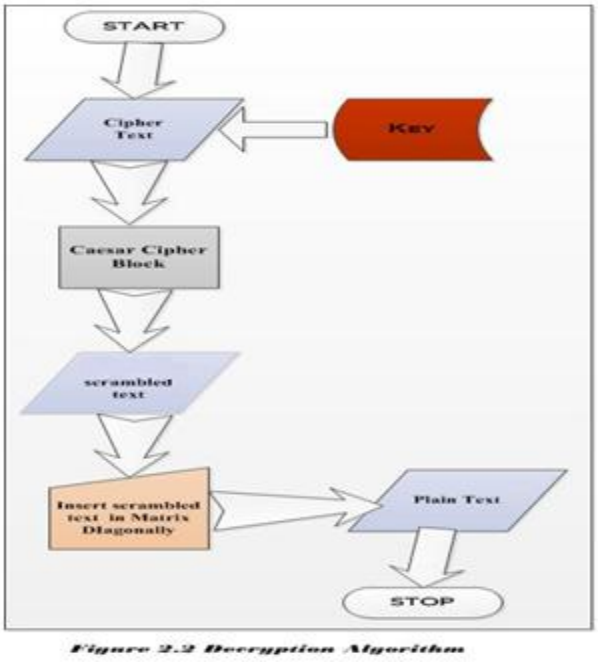


Fig 2: Encryption and Decryption Algorithm

6. REFERENCES

[1] Behrouz A. Forouzan and G. hill, 2006, Data Communications and Networking, 4th Edition by Behrouz.

[2] . Kashish Goyal, Supriya, July 2013 "Modified Caesar Cipher for Better Security Enhancement",International Journal of Computer Science, Volume 73 – No 3.

[3] Kashish Goyal, Supriya, March 2013 " Security Concerns in the world of cloud computing", IJARCS International Journal of Advanced Research in computer science, volume 4 no 4, pp230 – 234.

[4] Stamp M. , May 2011 " Information Security: Principles and Practice", 2nd Edition John Wiley and Sons Inc. ISBN:978-0-470-62639-9.

[5] Pooja Maheswari , 2001 ," Classification of Ciphers", Indian Institute of Technology, Kanpur

[6] G. Sivagurunathan, V. Rajendar and T. Purusothaman, March 2010, " Classification of Substitution Ciphers using Neural networks", IJCS &NS vol 10, no 3.

[7] Aftab Alam, Shah Mehmod, Muhammad Salam, August 2013, " A modified version of playfair cipher using 7 x 4 matrix", IJCT&E vol 5, no4.

[8] Enas Ismael, Farah, June 2014, " Enhancement Caesar Cipher for better Security"Journal of CE, ISSN: 2278-0661.

[9] Gaurav Sharma, Ajay Kakkar, 2012, "Cryptography Algorithms and approaches used for data security", International Journal of Scientific & Engineering Research Vol. 3, Issue 6.

[10] Ochoche Abraham, Ganiyu O. Shefiu, October 2012 , "AN IMPROVED CAESAR CIPHER (ICC) ALGORITHM", International Journal Of Engineering Science & Advanced Technology (IJESAT). Vol. 2, Issue -5. pp .1198 – 1202.