ENHANCING SECURITY OF CAESAR CIPHER USING DIFFERENT METHODS

Anupama Mishra

Anupama170588@gmail.com

Abstract

Cryptography is an art and science of converting original message into non readable form. There are two techniques for converting data into no readable form:1)Transposition technique 2)Substitution technique. Caesar cipher is an example of substitution method. As Caesar cipher has various limitations so this talk will present a perspective on combination of techniques substitution and transposition. In this paper I have focused on the well known classical techniques the aim was to induce some strength to these classical encryption for that purpose I blended classical encryption with the some more techniques. my proposed method showed that it is better in terms of providing more security to any given text message. In our experiments I took Caesaer Ciphers as representatives of Classical Techniques. To make it more secure I have used some techniques like I have used multiple level Row Transposition Ciphers, encryption with same key at each level and encryption with different key at each level.

Keywords— *substitution, transposition, cryptography, Caesar cipher*

----------***----------

1. INTRODUCTION

In today's information age, it is impossible to imagine without internet. This modern era is dominated by paperless offices-mail messages-cash transactions and virtual departmental stores. Due to this there is a great need of interchanging of data through internet. Various sensitive information like banking transactions, credit information, confidential data is transferred over internet. To protect this type of data there is a great need of security. We convert our data in a no readable form at sender side and convert that data in readable form again at receiver end. The art and science of creating no readable data or cipher so that only intended person is only able to read the data is called Cryptography [2]. Encryption is a process by which we convert our data in no readable form. Decryption is reverse of encryption process [3].Plaintext is the intended original message. Cipher text is the coded message. There are two techniques of encryption: Substitution Technique and Transposition Technique [4].

In substitution technique, the letters of plain text are replaced by other letters or any number or by symbols. Example Caesar cipher, hill cipher, monoalphabetic cipher etc[4].

In transposition technique, some sort of permutation is performed on plaintext.Example:rail fence method, columnar method etc[4].

2. BACKGROUND

In the field of cryptography there exist several techniques for encryption/decryption these techniques can be generally classified in to two major groups Conventional and Public key Cryptography, Conventional encryption is marked by its usage of single key for both the process of encryption and decryption whereas in public key cryptography separate keys are used. Further on conventional techniques are further broken in to Classical and Modern techniques. Ciphers are inter related a comprehensive hierarchal diagram can be seen below. Public key cryptography is also an option when it comes to encryption but it require excessive communication and processing resources [10]. In next sections we will discuss some of the conventional methodologies after which we will come to our proposed technique and finally we will compare our proposal with some standard conventional encryption models and display the results.

2.1 CLASSICAL ENCRYPTION:

Several encryption algorithms are available and used in information security [6, 7, 8] There are several algorithms that can be categorized as classical but out of many in this section we will be shedding some light on 3 such techniques:
i) Caesar Cipher:
ii) Vigenere Cipher
iii) Playfair Cipher

2.1.1 Caesar Cipher:

It is a classical substitution cipher, and one of the simplest example of substitution cipher [9], which replaces the letter of alphabet with a letter that is 3 paces ahead of it [1], for example "ZULU" will be converted in to "CXOX" as one can see that such a IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010 281 cipher may be difficult to break if you are trying to solve it on

paper and have no clue of the key, but it has no standing these days in the age of computers and technology and through brute force attack it can be easily broken because in the end there are only 25 possible options of key available.

2.1.2 Vigenere Cipher:

This cipher when compared with Caesar gives some level of security with the introduction of a keyword; this key word is repeated to cover the length of the plain text that is to be encrypted example is Shown below:

KEY: f a u z a n f a u z a n
P.T: c r y p t o g r a p h y
Cipher: H R S O T B L R U O H L

As we can see from above example that "fauzan" is our keyword and plain text is "cryptography" which was encrypted in to "HRSOTBLRUOHL" this was done using Vigenere table which contains alphabets in form of rows and columns left most column indicates keywords and top most row indicates plaintext and at the junction of two alphabetic letters resides our replacement and after individually transforming every letter we get an encrypted message.

2.1.3 Playfair Cipher:

Another example of classical cipher is Playfair cipher that has a square of matrix of 5X5 alphabetic letters arranged in an appropriate manner [2]. We can select a key and place it in the matrix the remaining letters of English alphabet are then one by one placed in the matrix of Playfair cipher, the plain text is broken in to pairs and if a pair has same alphabet then they are separated by introducing a filler letter like 'x', other wise if the pair are different alphabetic letters and reside in the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters are in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters are neither in same column nor in same row then are they replaced by the letter in their row that resides at the intersection of paired letters. Reverse method is applied to yield the result.

3. PURPOSE

The purpose of this document is to present different methods that enhances the security of transposition cipher. In this paper I have focused on the well known classical techniques the aim was to induce some strength to these classical encryption for that purpose I blended classical encryption with the some more techniques. my proposed method showed that it is better in terms of providing more security to any given text message. In our experiments I took Caesaer Ciphers as representatives of Classical Techniques. To make it more secure I have used some techniques like I have used multiple level Row Transposition Ciphers , encryption with same key at each level and encryption with different key at each level.

4. CAESAR CIPHER AND ITS CRYPTANALYSIS

Caesar cipher is one of the simplest type of substitution method. In this letters of alphabets are replaced by letters three places further down the alphabet. But in general, this shift may be of any places[4]. Using the Caesar cipher, the message "RETURN TO ROME" is encrypted as "UHWXUA WR URPH". So attacker is not able to read the message if he intercepts the message [3].

If in case it is known that a given ciphertext is Caesar cipher, then brute force cryptanalysis is easily performed: Try all the 25 keys. There are some weak points about Caesar cipher which enables us to use brute force attack [4].
1. The encryption and decryption algorithm is known.
2. Only 25 keys are to try.
3. The language of the plaintext is known and easily recognizable.

5. PROPOSED TECHNIQUE

This problem can be sloved using multi level Row Transposition cipher. it can used with either same key at each level or different key at each level . both method successfully resolve the problem of security and the cipher text produced by these methods will be more secure it would be difficult to perform brute force cryptanalysis.

5.1 SIMPLE ROW TRANSPOSITION CIPHERS

- Write the plaintext in a rectangle, row by row
- If there is any blank place fill it with the random alphabet of symbols.
- Reorder the columns according to the key before reading off.
- Read the message off column by column top to bottom.

Key: **4312567**
Column Out:

4	3	1	2	5	6	7

Plaintext:

text:	a	t	t	A	c	k	P
	o	s	t	P	o	n	E
	d	u	n	T	i	l	T
	w	o	a	M	x	y	Z

Cipher text:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

We can significantly more secure by performing more than one stage transposition.

The result will be more complex permutation that is not easily reconstructed.

To do so we will re-encrypt the cipher text (obtained after applying the above algorithm) using the same algorithm.
Now I am going to discuss two more algorithms which generate more complex permutation
That cannot be easily reconstructed and much more difficult to cryptanalysis

5.2 MULTI LEVEL ROW TRANSPOSITION CIPHERS

Method -1

Encryption algorithm-

- Apply row Transposition Cipher
- Write the cipher text in a rectangle, row by row.
- Reorder the columns according to the key before reading off.
- Using the key of first level encryption , Read the message as follows
- First column top to bottom.
- Then next column bottom to top.
- And so on

EXAMPES---

1ST LEVEL ENCRYPTION

Plaintext: Attack postponed until two am
Key: **4312567**

Column Out	4	3	1	2	5	6	7
Plaintext:	A	t	t	A	C	k	P
	O	s	t	P	O	n	E
	D	u	n	T	I	l	T
	W	o	a	M	X	y	Z

Cipher text:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

2ND LEVEL ENCRYPTION

Plaintext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
Key: **4312567**

Column Out	4	3	1	2	5	6	7
Plaintext:	T	t	n	A	A	p	T
	m	t	s	U	O	a	O
	D	w	c	O	I	x	K
	N	l	y	P	E	t	Z

Cipher text:
NSCYPOUATTWLNDMTAOIETXAPTOKZ
The generated ciphertext is more secure, cannot be easily reconstructed and much more difficult to cryptanalyze.

In above example we have used the same key at both level of encryption but if we use different keys at each level then we can get more secure and complex permutation.

It will be cleared from following example.

1ST LEVEL ENCRYPTION

Plaintext: Attack postponed until two am
Key: **4312567**

Column Out	4	3	1	2	5	6	7
Plaintext:	A	t	t	A	c	k	P
	O	s	t	P	o	n	E
	D	u	n	T	i	l	T
	W	o	a	M	X	y	Z

Ciphertext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

2ND LEVEL ENCRYPTION

Plaintext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ
Key: **5146327**

Column Out	5	1	4	6	3	2	7
Plaintext:							
text:	T	t	n	A	a	p	T
	M	t	s	U	o	a	O
	D	w	c	O	i	x	K
	N	l	y	P	E	t	Z

Ciphertext:
TTWLTXAPAOIEYCSNTMDNPOUATOKZ

Decryption

Decryption Algorithm-

- Using the key Write the cipher text as follows.
- First column bottom to top.
- Next column top to bottom. And so on.
- Read the message row by row.
- First level of decryption is complete now we will start next level of decryption
- Write the message using same decryption key (used at first level) column by column.
- Read the message row by row.

Decryption Example with Different Keys

1ST LEVEL DECRYPTION

Ciphertext:
TTWLTXAPAOIEYCSNTMDNPOUATOKZ
Key: **5146327**
Column Out 5 1 5 6 3 2 7
Plaintext:

P	t	T	n	a	A	p	T
	m	T	s	u	O	a	O
	d	W	c	o	I	x	K
	n	L	y	p	E	t	Z

Plaintext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

2ND LEVEL DECRYPTION

Ciphertext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ
Key: **4312567**
ColumnOut 4 3 1 2 5 6 7
Ciphertext:

a	T	T	a	C	K	P
o	S	T	p	O	N	E
d	U	N	t	I	L	T
w	O	A	m	X	Y	Z

Plaintext: ATTACK POSTPONED UNTI TWO AM.

Decryption Example with Same Keys

1ST LEVEL DECRYPTION

Ciphertext: NSCYPOUATTWLNDMTAOIETXAPTOKZ
Key: **4312567**
Column Out 4 3 1 2 5 6 7
Plaintext:

ıtext:	T	t	n	A	A	p	T
	M	t	s	U	O	a	O
	D	w	c	O	I	x	K
	N	l	y	P	E	t	Z

Plaintext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

2ND LEVEL DECRYPTION

Ciphertext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ
Key: **4312567**
Column Out 4 3 1 2 5 6 7

Plaintext:	a	t	t	A	C	k	P
	o	s	t	p	O	n	E
	d	u	n	t	I	l	T
	w	o	a	m	X	y	Z

Plaintext: ATTACK POSTPONED UNTI TWO AM.

Method-2

Encryption Algorithm-

- Write the plaintext in a rectangle, row by row.
- Reorder the columns according to the key before reading off.
- Read the message off column by column to bottom.
- At the next level of encryption use following key to cipher the encrypted text.
  Key→ N↔ (N+2)
- Exchange the letter of Nth position with latter of N+1s position from left to right.
- Write the respective alphabetic number for each latter in cipher text

Decryption Algorithm

- At the first level of decryption to decrypt cipher text the key will be same but it will be apply from opposite direction
  Key → N↔ (N+2)
- In cipher text stream Exchange the letter of Nth position with latter of N+1s position from right to left.
- First level of decryption is complete now we will start next level of decryption
- Write the plaintext in a rectangle, column by column using the key of first level encryption.
- Reorder the columns according to the key before reading off.

Read the message off Row by Row top to bottom.

EXAMPLE
1ST LEVEL ENCRYPTION

Key: **4312567**
ColumnOut 4 3 1 2 5 6 7
Plaintext:

a	t	t	a	c	k	P
o	s	t	p	o	n	E
d	u	n	t	i	l	T
w	o	a	m	x	y	Z

Cipher text:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

2ND LEVEL ENCRYPTION

Plaintext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

At the second level of encryption we will use the key (Exchange the element of nth position with the element of n+2s position)

T T N A A P T M T S U O A O D W C O I X K N L Y P E T Z
N T T A A P T M T S U O A O D W C O I X K N L Y P E T Z
N A T T A P T M T S U O A O D W C O I X K N L Y P E T Z
N A A T T P T M T S U O A O D W C O I X K N L Y P E T Z
N A A P T T T M T S U O A O D W C O I X K N L Y P E T Z
N A A P T T T M T S U O A O D W C O I X K N L Y P E T Z
N A A P T M T T T S U O A O D W C O I X K N L Y P E T Z
N A A P T M T T T S U O A O D W C O I X K N L Y P E T Z
N A A P T M T S T T U O A O D W C O I X K N L Y P E T Z
N A A P T M T S U T T O A O D W C O I X K N L Y P E T Z
N A A P T M T S U O T T A O D W C O I X K N L Y P E T Z
N A A P T M T S U O A T T O D W C O I X K N L Y P E T Z
N A A P T M T S U O A O T T D W C O I X K N L Y P E T Z
N A A P T M T S U O A O D T T W C O I X K N L Y P E T Z
N A A P T M T S U O A O D W T T C O I X K N L Y P E T Z
N A A P T M T S U O A O D W C T T O I X K N L Y P E T Z
N A A P T M T S U O A O D W C O T T I X K N L Y P E T Z
N A A P T M T S U O A O D W C O I T T X K N L Y P E T Z
N A A P T M T S U O A O D W C O I X T T K N L Y P E T Z
N A A P T M T S U O A O D W C O I X K T T N L Y P E T Z
N A A P T M T S U O A O D W C O I X K N T T L Y P E T Z
N A A P T M T S U O A O D W C O I X K N L T T Y P E T Z
N A A P T M T S U O A O D W C O I X K N L Y T T P E T Z
N A A P T M T S U O A O D W C O I X K N L Y P T T E T Z
N A A P T M T S U O A O D W C O I X K N L Y P E T T Z
\N A A P T M T S U O A O D W C O I X K N L Y P E T T Z
N A A P T M T S U O A O D W C O I X K N L Y P E T Z T T

Cipher text:
NAAPTMTSUOAODWCOIXKNLYPETZTT

1ST LEVEL DECRYPTION

At the first level of decryption exchange element of nth location with the element of n+2th location

N A A P T M T S U O A O D W C O I X K N L Y P E T Z T T
N A A P T M T S U O A O D W C O I X K N L Y P E T T T Z
N A A P T M T S U O A O D W C O I X K N L Y P E T T T Z
N A A P T M T S U O A O D W C O I X K N L Y P T T E T Z
N A A P T M T S U O A O D W C O I X K N L Y T T P E T Z
N A A P T M T S U O A O D W C O I X K N L T T Y P E T Z
N A A P T M T S U O A O D W C O I X K N T T L Y P E T Z
N A A P T M T S U O A O D W C O I X K T T N L Y P E T Z
N A A P T M T S U O A O D W C O I X T T K N L Y P E T Z
N A A P T M T S U O A O D W C O I I T T X K N L Y P E T Z
N A A P T M T S U O A O D W C O O T T I X K N L Y P E T Z
N A A P T M T S U O A O D W C T T C O I X K N L Y P E T Z
N A A P T M T S U O A O D W T T C O I X K N L Y P E T Z
N A A P T M T S U O A O D W C T T O I X K N L Y P E T Z
N A A P T M T S U O A O D W C O T T I X K N L Y P E T Z
N A A P T M T S U O A O D W C O I T T X K N L Y P E T Z
N A A P T M T S U O A O D W C O I X T T K N L Y P E T Z
N A A P T M T S U O A O D W C O I X K T T N L Y P E T Z
N A A P T M T S U O A O D W C O I X K N T T L Y P E T Z
N A A P T M T S U O A O D W C O I X K N L T T Y P E T Z
N A A P T M T S U O A O D W C O I X K N L Y T T P E T Z
N A A P T M T S U O A O D W C O I X K N L Y P T T E T Z
N A A P T M T S U O A O D W C O I X K N L Y P E T T Z
N A A P T M T S U O A O D W C O I X K N L Y P E T Z T T
T T N A A P T M T S U O A O D W C O I X K N L Y P E T Z

Now the first level of decryption is over and we will move to second level of decryption

2ND LEVEL DECRYPTION

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
Key: **4312567**

ColumnOut	4	3	1	2	5	6	7
Plaintext:	a	t	T	a	c	k	P
	o	s	T	p	o	n	E
	d	U	N	t	i	l	T
	w	O	A	m	x	y	Z

Plaintext: attack postponed until two am.

6. APPLICATION

This Caesar cipher which is secured by “Multilevel Row Transposition with same and different keys” has various advantages over simple Caesar cipher.

- In this double transposition method is applied which provide much less structured permutation.
- It is more difficult to crypt analyze.
- The result is not easily reconstructed.
- Brute force attack is not possible.
- Overcome all the limitations of Caesar cipher.

CONCLUSIONS

Caesar cipher is simplest type of cipher and mostly used. Transposition method is mostly combined with other techniques. Both substitution method and transposition method encryption are easily performed with the power of computers. The combination of these two classic techniques provides more secure and strong cipher. The final cipher text is so strong that is very difficult to break. Substitution method only replace the letter with any other letter and transposition method only change position of characters. The above described second method(algorithm) is the combination of both the transposition and substitution method which provides much more secure cipher.

REFERENCES

[1]William Stalling”Network Security Essentials(Applications and Standards)”,Pearson Education,2004
[2] Atul Kahate (2009), *Cryptography and Network Security*, 2nd edition, McGraw-Hill.
[3] Stallings W (1999), *Cryptography and Network Security*, 2nd edition, Prentice Hall.
[4] William Stallings (2003), *Cryptography and Network Security*, 3rd edition, Pearson Education
[5] V. Umakanta Sastry1, N. Ravi Shankar2, and S. Durga Bhavan “A Modified Hill Cipher Involving Interweaving and Iteration” International Journal of Network Security, Vol.11, No.1, PP.11{16, July 2010
[6] M. S. Hwang and C. Y. Liu, \Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.
[7]M. H. Ibrahim, \A method for obtaining deniable publickey encryption," International Journal of Network Security, vol. 8, no. 1, pp. 1-9, 2009

[8] M. H. Ibrahim, \Receiver-deniable public-key encryption," International Journal of Network Security, vol. 8, no. 2, pp. 159-165, 2009
[9] Results of Comparing Tens of Encryption Algorithms Using Di®erent Settings- Crypto++ Benchmark, Retrieved Oct. 1, 2008. (http://www.eskimo.com/ weDai/benchmarks.html)
[10] Y. C. Hu, A. Perrig, and D. B. Johnson, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” Proceeding of IEEE Workshop on Mobile Computing Systems and Applications, 2003.
[11] International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 10, October 2012 ISSN: 2277 128X “Enhancing Security of Caesar Cipher by Double Columnar Transposition Method” Mr. Vinod Saroha ,Suman Mor, Anurag Dagar