CCET JOURNAL OF SCIENCE AND ENGINEERING EDUCATION
(ISSN 2455-5061) *Vol. - 3, Page-60-65, Year-2018*

Substitution Technique Based Noble Approach Towards Base64 Crypting System Incorporating Rail Fence Cipher

Ujjwal Barman[*], Suchismita Gupta[**], Sudipta Sahana[***]

[*]*B.Tech, Department of CSE, JIS College of Engineering, West Bengal, India,* ***ubarman262@gmail.com***
[**]*B.Tech, Department of CSE, JIS College of Engineering, West Bengal, India,* ***guptasuchismita96@gmail.com***
[***]*Asst. Prof., Department of CSE, JIS College of Engineering, West Bengal, India,* ***ss.jisce@gmail.com***

Abstract

Network security is a very important aspect of the digital world. Cryptography provides authentication, integrity, non-repudiation and confidentiality to the global data. It stores and transmits data in a particular form so that only the authorized user can access it. Cryptology and Cryptanalysis are the disciplines to which Cryptography is linked. Techniques such as microdots, merging words with images, and other ways to hide information in storage or transit are included in cryptography. However, in the computer-centric world of today, cryptography is most often associated with scrambling plain text into cipher text, then back again. Cryptographers are the individuals who practice this field. In this paper we have proposed a cryptographic algorithm based on techniques like Rail Fencing cipher and Substitution thus accomplishing the goal of security. Proper encryption and decryption methods have been used in the algorithm, thus assuring security at its best possible way.

Index Terms: *Encryption, Decryption, Rail Fencing Cipher, Substitution Technique, Base64 conversion.*

1. Introduction

Cryptography can be defined as the process of converting ordinary plain text into garbled text and vice-versa. In this method the data is stored and transmitted in a particular form, so that only the authorised people can access it. Cryptography has gone through a change of phase. At the beginning it was effectively synonymous with encryption but now it is mainly based on mathematical theory and computer science practice.

Primary goals of cryptography are confidentiality, integrity, non-repudiation and authentication. Confidentiality is very important. It ensures that information is not understood by any unauthorised person. Integrity refers to protecting information from being modified or altered by the unauthorized parties. Non-repudiation confirms that the sender cannot deny his/her intentions in the transmission of the information after completion of the task. Authentication implies the confirmation of the sender and the receiver in any transmission. A wide range application of cryptography can be viewed in authentication/digital signatures, time stamping, electronic money, secure network communications and anonymous remailers.

In general, cryptographic techniques can be categorised into three types, Symmetric-key cryptography, Public-key cryptography and Hash functions.In Symmetric-Key Cryptography a single key is shared by both the sender and the receiver. The key is used by the sender to encrypt the plain text and then the cipher text is send to the receiver. Further the same key is applied by the receiver to decrypt the message and the plain text is thus recovered. In Public-Key Cryptography two related keys are used. One is called public key which may be freely distributed, and the other is private key which remains a secret. The process of encryption can be done using the public key and the process of decryption can be done by the private key. In Hash Functions no key is used. The recovery of the contents of the plain text is hindered by a fixed-length hash value which is computed as per the plain text. These are also applied by many operating systems to encrypt passwords.

Substitution is a technique in which units of plaintext are replaced with ciphertext, according to a fixed system. The text is deciphered by the receiver by performing the inverse substitution. On the other hand, Transposition cipher is a method in which the positions held by units of plaintext are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. The Rail Fence Cipher is a form of transposition cipher used in the paper. In this the plaintext is written downwards on successive

"rails" of an imaginary fence, then moving up when the bottom is obtained. The message is then the Rail Fence Cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows.

2. Related Works

Anupam Mondal et al. [1] introduced a new approach to encrypt secret information based on the concept of triangularization. Since the encryption and decryption is done on a binary file by means of XOR operation it is effective on any type of data such as text or multimedia files.

Sudipta Sahana et al. [2] altered the plain text to a cipher text using cryptography process. Some Boolean algebraic operations are used. Further supressing the cipher text inside a cover media of image. Cryptoanalysis and Steganalysis methods of recovering data at receiver side is also exposed.

Monalisa Dey et al. [3] have proposed an algorithm considering encryption as a critical security measure for protecting data privacy. The entire process is achieved by considering binary data to cover all kinds of data in the field of Computer Science thus ensuring data security irrespective of what information is being transmitted.

Soupayan Dutta et al. [4] focused primarily on the idea wherein the location of data is encrypted along with the data itself by means of a single Location Encryption Algorithm. The security is further boosted using the Confirmation Code.

A Nag et al. [5] proposed a process of embedding to accomplish data hiding under the transformation (DWT and IDWT) of cover image and to obtain privacy by using Huffman encoding.

Ajit Singh et al. [6] introduced a technique where Caesar cipher and Rail Fence cipher technique are combined to eliminate their respective fundamental weaknesses, and produce a cipher text that is hard to crack. When Caesar cipher substitution and Rail fence transposition techniques are used individually, cipher text obtained is easy to crack. This talk will present a perspective on combination of techniques substitution and transposition. Combining Caesar cipher with Rail fence technique can eliminate their fundamental weakness and produce a cipher text that is hard to crack.

3. Proposed Work

In this section we have proposed our encryption & decryption algorithm.

A. Encryption Algorithm-

Step1. Input a string from user.
Step2. Replace each letter in the plaintext by a right shifted letter where shift value is 3.
Step3. Substitution of each character using mapping table for encryption.
Step4. Perform Rail Fence Cipher.
Step5. Convert plaintext to its corresponding 8-bit ASCII value.
Step6. Perform 1's Complement operation on 8-bit ASCII value.
Step7. Convert 8-bit ASCII values to Hexa-Decimal form.
Step8. Merging all the Hexa-Decimal Values.
Step9. Obtain Base64 value of the obtained plaintext.

B. Decryption Algorithm -

Step1. Take encrypted text as input.
Step2. Convert encrypted text from Base64 to Text.
Step3. Perform two-character segment grouping.
Step4. Convert each segment from Hexa-Decimal to 8-bit Binary form.
Step5. Perform 1's Complement operation on 8-bit Binary value.
Step6. Convert 8-bit binary to ASCII Character.
Step7. Perform Backtracking Rail Fence Cipher.
Step8. Substitution of each character using mapping table for decryption.
Step9. Replace each letter in the plaintext by a left shifted letter where shift value is 3.

Mapping table for Encryption:

!	**“**	**#**	**$**	**%**	**&**	**‘**	**(**	**)**	*****	**+**	**,**	**-**	**.**	**/**
&	(	+	.	)	“	*	%	-	,	$	‘	/	!	#

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

:	**;**	**<**	**=**	**>**	**?**	**@**
;	=	?	:	@	>	<

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

[	****	**]**	**^**	**_**	**`**
`	^	_	]	\	[

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**
d	k	v	q	f	i	b	j	w	p	e	s	c	x	h	t	m	y	a	u	o	l	r	g	z	n

{	**|**	**}**	**~**
|	}	~	{

Mapping table for decryption:

&	**(**	**+**	**.**	**)**	**“**	*****	**%**	**-**	**,**	**$**	**‘**	**/**	**!**	**#**
!	“	#	$	%	&	‘	(	)	*	+	,	-	.	/

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

;	**=**	**?**	**:**	**@**	**>**	**<**
:	;	<	=	>	?	@

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

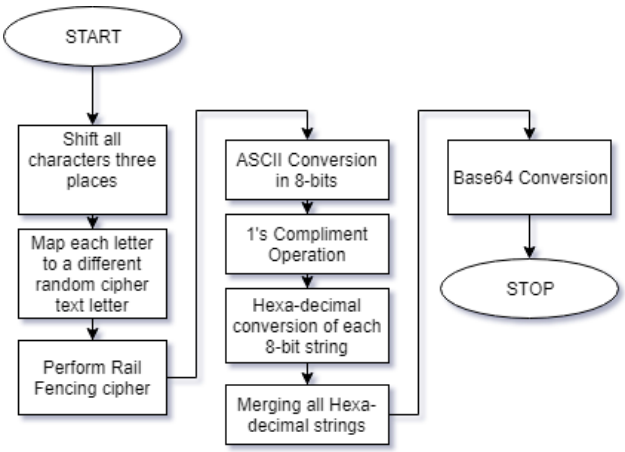
`	**^**	**_**	**]**	****	**[**
[	\	]	^	_	`

d	**k**	**v**	**q**	**f**	**i**	**b**	**j**	**w**	**p**	**e**	**s**	**c**	**x**	**h**	**t**	**m**	**y**	**a**	**u**	**o**	**l**	**r**	**g**	**z**	**n**
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

|	**}**	**~**	**{**
{	|	}	~

CCET JOURNAL OF SCIENCE AND ENGINEERING EDUCATION
(ISSN 2455-5061) *Vol. - 3, Page-60-65, Year-2018*

Flow Chart for the Encryption



4.Example

A. Encryption –

Consider the plain text to be "Hello@123"

Step1. Replacing each letter in the plaintext by a right shifted letter where shift value is 3.
Each character has its own shifting table. Each shifting table is in looped form.
So, the message "Hello@123" becomes: Khoor<456

Step2. Substitution of each character obtained from the previous step.Each plaintext letter maps to a different cipher text letter according to the mapping table(s).

So, the message "Khoor<456" becomes: Ejhhy?721

Step3. Performing Rail Fence Cipher on the newly obtained plaintext.

Ejhh?721 →

E	h	y	7	1
j	h	?	2	

← String 1
← String 2

Using Rail Fence Cipher, we divide the string into two parts as shown above.
We then merge String 1 with String 2.
So, the message "Ejhhy?721" becomes: Ehy71jh?2

Step4. Plaintext letter is converted to its corresponding 8-bit ASCII Value.

Character	ASCII Value
E	01000101
h	01101000
y	01111001
7	00110111
1	00110001
j	01101010
h	01101000
?	00111111
2	00110010

Step5. 8-bit ASCII Value is operated with 1's Complement operation.

ASCII Value	1's Complement
01000101	10111010
01101000	10010111
01111001	10000110
00110111	11001000
00110001	11001110
01101010	10010101
01101000	10010111
00111111	11000000
00110010	11001101

Step6. Convert all the newly obtained 8-bit values to Hexa-Decimal form.

8-bit Value	Hexa-Decimal
10111010	BA
10010111	97
10000110	86
11001000	C8
11001110	CE
10010101	95
10010111	97
11000000	C0
11001101	CD

Step7. Merging all the Hexa-Decimal Values.
We get Cipher text as:

BA9786C8CE9597C0CD

Step8. Obtaining Base64 value of the obtained plaintext.

So, the message "BA9786C8CE9597C0CD" becomes: QkE5Nzg2QzhDRTk1OTdDMENE

Finally, the plaintext "Hello@123" becomes QkE5Nzg2QzhDRTk1OTdDMENE

B. Decryption –

Our encrypted message is "QkE5Nzg2QzhDRTk1OTdDMENE"

Step1. Convert the encrypted text from Base64 to Text.

Base64	Text
QkE5Nzg2QzhDRTk1OTdDMENE	BA9786C8CE9597C0CD

Step2. Grouping in two-character segments.

2-Character Segment Grouping								
BA	97	86	C8	CE	95	97	C0	CD

Step3. Converting each segment from Hexa-Decimal to 8-bit Binary form.

Hexa-Decimal	8-bit Value
BA	10111010
97	10010111
86	10000110
C8	11001000
CE	11001110
95	10010101
97	10010111
C0	11000000
CD	11001101

Step4. 8-bit Binary Value is operated with 1's Complement operation.

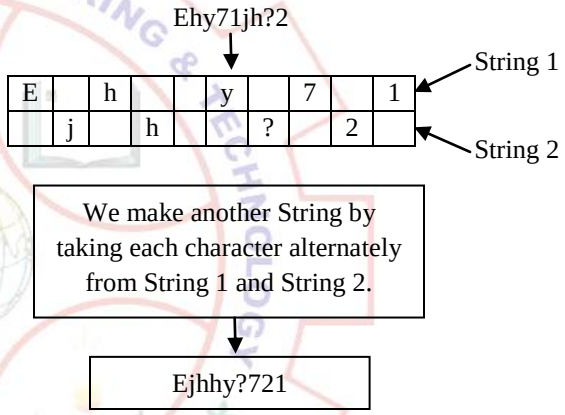
8-bit Value	1's Complement
10111010	01000101
10010111	01101000
10000110	01111001
11001000	00110111
11001110	00110001
10010101	01101010
10010111	01101000
11000000	00111111
11001101	00110010

Step5. Convert8-bit binary to ASCII Character.

ASCII Value	Character
01000101	E
01101000	h
01111001	y
00110111	7
00110001	1
01101010	j
01101000	h
00111111	?
00110010	2

We obtain plaintext: Ehy71jh?2

Step6. Perform Backtracking Rail Fence Cipher.



So, the message "Ehy71jh?2" becomes: Ejhhy?721

Step7. Substitution of each character using mapping table(s).
So, the message "Ejhhy?721" becomes: Khoor<456

Step8. Replacing each letter in the plaintext by a left shifted letter where shift value is 3.
So, the message "Khoor<456" becomes: Hello@123

So, we finally obtain our decrypted message which is: Hello@123

5. Conclusion

Cryptography is a particularly interesting field because of the amount of work that is done in secret. But the secrecy is not the key component which defines the effectiveness of the cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied! In our proposed work we have used methods like substitution, character mapping which provides a basic

level of encryption to the message. The uses of Rail Fence Cipher technique to provide a second layer of encryption to the message without increasing the size. Using conversion techniques like ASCII to 8-bit binary, 1's complement, 8-bit binary to hexa-decimal which provides more security. Base64 conversion technique has been incorporated in our algorithm to make it more secure.by using this approach safe and sound data can be transmitted.

Acknowledgement

We would like to thank the Department of Computer Science and Engineering for providing us necessary information regarding the project. We would like to express our humble gratitude and thanks to the authors of the publications we have taken as a reference.

References

[1] Anupam Mondal, Joy Samadder, Ivy Mondal, Neha Majumder, SudiptaSahana, "Asymmetric Key based Secure Data Transfer Technique", International Conference on Computing, Communication and Sensor Network (CCSN) 2012.

[2] SudiptaSahana, Abhipsa Kundu, "Diagonal Block Steganography Based Enhanced Auxiliary Key Crypting for Secure Data Transfer", International Journal of Advanced Research in Computer Engineering & Technology(IJARCET) Volume 3 Issue 10, October 2014.

[3]MonalisaDey, Dhirendra Prasad Yadav, Sanik Kumar Mahata, Anupam Mondal, SudiptaSahana, "An Improved Approach of Cryptography using Triangulation and MSBIteration Technique" Special Issue of International Journal of Computer Applications (0975 – 8887) International Conference on Computing, Communication and Sensor Network (CCSN) 2012.

[4] Soupayan Dutta, Soumya KantaDey, SudiptaSahana, "Implementation of Location Encryption Algorithm for Data Flow in Database Systems Ensuring Enhanced Security Management", International Journal of Innovations in Engineering and Technology(IJIET), Volume 6, Issue 4 April 2016, ISSN:2319-1058.

[5] A. Nag, S. Biswas, D. Sarkar, P. P.Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding," International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6),pp. 497-610,2011.

[6] Ajit Singh, Aarti Nandal, swati Malik, "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012, ISSN: 2277 128X.