International Research Journal of Computer Science (IRJCS)
Issue 04, Volume 3 (April 2016)
ISSN: 2393-9842
www.irjcs.com

A Novel Approach for Cryptography using Modified Substitution Cipher and Triangulation

Sainik Kumar Mahata*
CSE Dept. JIS College of Engineering

Monalisa Dey
CSE Dept, JIS College of Engineering

Abstract— In this paper a novel approach to encryption and decryption is presented, which will include two new techniques, namely, Rounded Cipher, a modified version of the substitution cipher, and Triangulation. This approach also uses a random primary key and a secondary key that is derived from the primary key, for the process of encryption and decryption, thus making the proposed work more secure.

Keywords— Cipher, Decryption, Encryption, Key, Triangulation

I. INTRODUCTION

Information exchange over the internet is gaining more and more importance with each passing day [1]. The need to securely transfer data from one computer to another has gained utmost significance [2]. And with it, the demand for data security is also increasing exponentially. So, for protecting the data from unauthorized access while in transit, an efficient security mechanism is required. Cryptography is the science of making communications unintelligible to everyone except the intended receiver(s) [3]. A cryptosystem usually consists of three elements, an encryption algorithm, a decryption algorithm and a key which work together to help protect the integrity of the data.

In the current work, a novel approach for data security is proposed which incorporates two techniques, viz., Rounded Cipher Technique and Triangulation. The techniques are presented in the sections 2 and 3. The encryption and decryption algorithms are presented in section 4 and 5 respectively, followed by an example depicting the proposed scheme in section 6.

II. MODIFIED SUBSTITUTION CIPHER

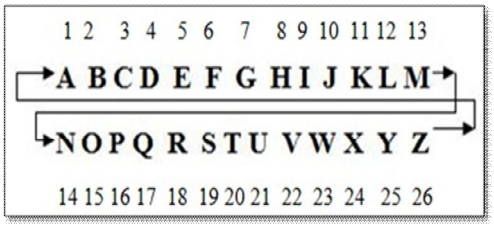

Fig. 1 Working of the modified substitution cipher

In this approach, positionional weights of individual letters of a word are taken (eg. A=1, B=2, C=3 and so on), shown in Figure 1, and a value, that is obtained from the key, is added to those weights. The resultant weights obtained are converted to their corresponding letters.

For eg.

Plain Text = **SAINIK**
Let us take a random number that is not prime, 5021988.
Key = 5021988
R = 5021988 % 26 = **10**

So,
S=19+10=**29**
A=1+10=**11**
I=9+10=**19**
N=14+10=**24**
I=9+10=**19**
K=11+11=**22**

Therefore,
A will be replaced by **K**
I will be replaced by **S**
N will be replaced by **X**
K will be replaced by **V**

© 2014-16, IRJCS- All Rights Reserved

If the positional weight exceeds 26 then we subtract 26 from that number. For S, we get 29. So we subtract 26 from 29 and we get 3 (29-26=3).

S will be replaced by **C**
The immediate ciphertext will be **CKSXSV**.

III. TRIANGULATION

Initially an n bit binary data string is taken. After this, the steps given below are performed.

- The data string initialized is taken as it is.
- Bit wise XOR operation is performed of all the bits; however, the MSB is not kept constant .This step is considered as the 1st iteration.
- The iteration process is continued until the data string is reduced to a single bit.
- The MSB's from the data string obtained from each of the iterations and are then joined together and taken as the new output.
- If we take the new output as the data string, and perform the above mentioned steps, i.e, step1-4, we get the original input.

The implementation of the above algorithm is shown using the following data string example. The data string taken is 1001110.

1	001110
1	01001
1	1101
0	011
0	10
1	1
0	

So, the Ciphertext is 1110010.

Now, we take the same ciphertext, apply triangulation, to get the original plaintext.

1	110010
0	01011
0	1110
1	001
1	01
1	1
0	

The plaintext is 1001110.

IV. ENCRYPTION PROCESS

An algorithm for the encryption process is given below.

- Take out every letter of the plaintext and determine their positional weights.
- Take a random number, which is not prime, and determine it as a Primary Key K.
- Take out a Secondary Key which is found out by dividing the Primary Key with 26, and taking out the remainder. Name this as R.
- Add the Secondary Key R to each letter positions.
- Take the ASCII equivalent of ach of the resultant letters.
- Take out the binary equivalent of each result.
- Name the results as **EIC1, EIC2, EIC3** and so on.
- Apply Triangulation method to each result to get **EFC1,EFC2, EFC3** and so on.
- We convert **EFCn** to its equivalent decimal.
- Convert the decimal numbers to equivalent letters w.r.t ASCII notation.

© 2014-16, IRJCS- All Rights Reserved

V. DECRYPTION PROCESS

An algorithm for the decryption process is given below.

- Take each letter of the ciphertext and convert it to ASCII notation.
- Convert the ASCII to corresponding binary equivalent.
- Name the results as DIC1, DIC2, DIC3 and so on.
- To DICn, apply the method of triangulation.
- After triangulation, name the results as DFC1, DFC2, DFC3 and so on.
- Convert DFCn to corresponding decimal equivalent.
- Taking the decimal numbers in ASCII form, convert them to corresponding alphabets.
- Apply the process of rounded cipher to the alphabets to get the plaintext.

VI. EXAMPLE

A. Encryption Process

Plaintext = **SAINIK**
Take a random number which is not prime, **5021988**
Primary Key K = 5021988
Secondary Key R = 5021988 % 26 = 10

S=19+10=**29**
A=1+10=**11**
I=9+10=**19**
N=14+10=**24**
I=9+10=**19**
K=11+11=**22**

Therefore,
S will be replaced by **C**
A will be replaced by **K**
I will be replaced by **S**
N will be replaced by **X**
K will be replaced by **V**

Resultant Ciphertext is CKSXSV

Alphabets	ASCII equivalent
C	67
K	75
S	83
X	88
S	83
V	86

Now, all the ASCII equivalents are converted to Binary equivalents.

67 = **1000011** = **EIC1**
75 = **1001011** = **EIC2**
83 = **1010011** = **EIC3**
88 = **1011000** = **EIC4**
83 = **1010011** = **EIC5**
86 = **1010110** = **EIC6**

Applying Triangulation Method to ICn, we get

© 2014-16, IRJCS- All Rights Reserved

1	000011
1	00010
1	0011
1	010
1	11
0	0
0	

EFC1 = 1111100

1	001011
1	01110
1	1001
0	101
1	11
0	0
0	

EFC2 = 1110100

1	010011
1	11010
0	0111
0	100
1	10
0	1
1	

EFC3 = 1100101

1	011000
1	10100
0	1110
1	001
1	01
1	1
0	

EFC4 = 1101110

1	010011
1	11010
0	0111
0	100
1	10
0	1
1	

EFC5 = 1100101

1	010110
1	11101
0	0011
0	010
0	11
1	0
1	

EFC6 = 1100011

© 2014-16, IRJCS- All Rights Reserved

Now, convert **EFCn** into decimal equivalent.
1111100 = 124
1110100 = 116
1100101 = 101
1101110 = 110
1100101 = 101
1100011 = 99

ASCII	Alphabets Equivalent
124	|
116	T
101	E
110	N
101	E
99	C

Final Ciphertext is **| t e n e c**

*B. **Decryption Process***
Ciphertext: **| t e n e c**

Alphabets Equivalent	ASCII
|	124
t	116
e	101
n	110
e	101
c	99

124 = **1111100 = DIC1**
116 = **1110100 = DIC2**
101 = **1100101 = DIC3**
110 = **1101110 = DIC4**
101 = **1100101 = DIC5**
99 = **1100011 = DIC6**

1 111100
0 00010
0 0011
0 010
0 11
1 0
1

DFC1 = 1000011

1 110100
0 01110
0 1001
1 101
0 11
1 0
1

DFC2 = 1001011

© 2014-16, IRJCS- All Rights Reserved

1	100101
0	10111
1	1100
0	010
0	11
1	0
1	

DFC3 = 1010011

1	101110
0	11001
1	0101
1	111
0	00
0	0
0	

DFC4 = 1011000

1	100101
0	10111
1	1100
0	010
0	11
1	0
1	

DFC5 = 1010011

1	100011
0	10010
1	1011
0	110
1	01
1	1
0	

DFC6 = 1010110

1000011 = 67
1001011 = 75
1010011 = 83
1011000 = 88
1010011 = 83
1010110 = 86

ASCII	Alphabets Equivalent
67	C
75	K
83	S
88	X
83	S
86	V

Immediate plaintext is **CKSXSV**.

Primary Key K = 5021988
Secondary Key R = 5021988 % 26 = 10

© 2014-16, IRJCS- All Rights Reserved

C = 3+26 = 29-10 =19
K = 11-10 = 1
S = 19 -10= 9
X = 24-10 = 14
S = 19-10 = 9
V = 22-10 = 11

C will be replaced by **S**
K will be replaced by **A**
S will be replaced by **I**
X will be replaced by **N**
S will be replaced by **I**
V will be replaced by **K**

Final Plaintext is **SAINIK**

VII. CONCLUSIONS

The proposed work incorporates two levels of encryption and decryption as well as two keys, one primary and a secondary, which is derived from the primary key, which are ransom in nature, thus increase the security features of the process. A future work in this approach would likely include, encryption of a binary plaintext, as because if binary number system is covered, every type of data will be covered.

REFERENCES

[1] M. Dey, D. P. Yadav, S. K. Mahata, A. Mondal, S. Sahana, "An Improved Approach of Cryptography using Triangulation and MSB Iteration Technique", International Journal of Computer Applications, Special Issue of 1st International Conference on Computing, Communication and Sensor Networks, February, 2012, pp. 16-18.
[2] S. K. Mahata, M. Dey, Dr. S. Som, "A Novel Approach For Block-Based Data Encryption", International Journal Of Computer Applications In Engineering Sciences, Vol III, Special Issue On CCSN 2012, May 2013. pp. 90-94. **[**ISSN: 2231-4946**]**
[3] Dr. S. Som, M. Banerjee, "Cryptographic Technique using Substitution through Circular Path Followed by Genetic Function", International Journal of Computer Applications, Special Issue of 1st International Conference on Computing, Communication and Sensor Networks, February, 2012, pp. 1-5 .
[4] William Stallings, *Cryptography and Network Security*, 2005, 4th Edition, Prentice Hall.
[5] Atul Kahate, *Cryptography and Network Security*, 2005, 4th reprint, Tata McGraw-Hill.

© 2014-16, IRJCS- All Rights Reserved