A Novel Approach to Cryptography using Modified Substitution Cipher and Hybrid Crossover Technique

Sainik Kumar Mahata[1], Shikha Nogaja[2], Smita Srivastava[3], Monalisa Dey[4], Subhranil Som[5]

[1,4]: Assistant Professor, Dept. of CSE, JIS College of Engineering, West Bengal
[5]: Assistant Professor, Dept of Computer Application, JIS College of Engineering, West Bengal
[2,3]: B.Tech student, Dept. of CSE, JIS College of Engineering, West Bengal

ABSTRACT

In the modern globally connected world, with the internet growing continually, the exchange of information over the web has made the data quite vulnerable. The need for data security is thus increasing exponentially day by day. Cryptography is a scientific measure used for the protection of sensitive communications. In this paper, a novel approach for information security is introduced. The encryption technique is incorporated using two methods namely, a modified approach to substitution cipher and a two step hybrid crossover technique. The devised algorithm uses two keys, thereby, increasing the security aspect. Moreover the entire process is done on alphabetical data thus increasing the scope of its implementation.

Index Terms

Crossover, Cryptography, Data security, Encryption, Substitution technique.

1. INTRODUCTION

In the present world, there is a rapid increase in globalization, resulting in an extreme rise in the use of wireless media to exchange information. The demand for effective internet security is increasing exponentially day by day [1]. As the internet is an insecure channel, while the data is in transit, it may be intercepted and modified by an eavesdropper. Thus, a highly developed system is required to protect the data privacy as well as integrity.

Cryptography is the science of making communication unintelligible to everyone except the intended user(s) [2]. It helps in protecting information from being eavesdropped by using various encryption algorithms. A cryptosystem is a set of algorithms, indexed by some key(s), for encoding messages into cipher text and decoding them back into plain text [3][4].

In the present work, we have introduced two such algorithms, namely, Modified Substitution Cipher and Hybrid Crossover Technique, derived from the concept of Genetic Algorithms. The algorithm is based on the process of substitution and genetic function [5]. Brute Force attack has the disadvantage of high computational complexity. In order to overcome this complexity, the Meta heuristic search techniques like Genetic Algorithm are used [6]. So the use of GA in the proposed approach makes it less vulnerable.

The first approach is discussed in section II. The flowchart representation of the second approach is discussed in section III. Examples of encryption and decryption are illustrated in section IV, followed by conclusion in section V.

2. MODIFIED SUBSTITUTION CIPHER APPROACH

A. Encryption

In the proposed model, we consider the co-ordinate axes and a clockwise spiral line which starts from Positive X- Axis. The characters of an input stream are placed on the intersection points of the clockwise spiral line and the axes. Consider **Figure 1**.

A random number, which is not a prime number, is chosen as the first key and is modulated by 256. The ASCII value of each character is calculated. Substitution is made according to the sign of the axis on which the character is. There are two cases:

- Case 1: If the axis is positive, the modulated random number is added to the ASCII value of the character on the axis.
- Case 2: If the axis is negative, the modulated random number is subtracted from the ASCII value of the character on the axis.

The modulated random number is incremented by 1 for each subsequent character. If the result of substitution is greater than 255 or less than 0, then the result is modulated by 256.

In the case of 2nd spiral round and more, the ASCII value of character on the inner spiral line is also added to the ASCII value of character on the outer spiral line and then the same procedure is conducted for the incremented value of modulated random number.

By this way, substitution of all the characters of the input stream will generate the intermediate cipher text. After this the genetic function is followed which gives us the final cipher text.

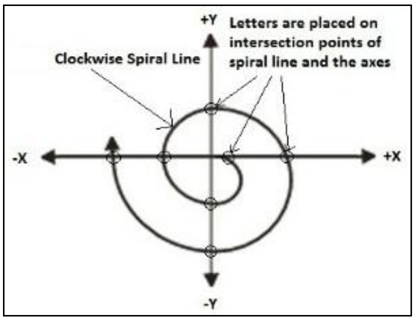
+Y
Letters are placed on intersection points of spiral line and the axes
Clockwise Spiral Line
-X
+X
-Y

Figure 1: Spiral co-ordinate for Encryption

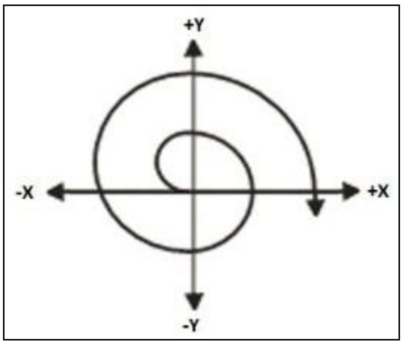

Figure 2: Spiral co-ordinate for Decryption

B. Decryption

In decryption the same co-ordinate axes and clockwise spiral line is considered, the only difference is that the spiral line has a 180 degree shift, i.e. it starts from the Negative X- Axis. Consider Figure 2.

The decryption procedure is same as that used for encryption. The difference is that in the 2nd or more spiral line the ASCII value of plain text of character on inner spiral line is subtracted from the ASCII value of Intermediate cipher of character on the outer spiral line, and then the same procedure is conducted for the incremented value of modulated random number to get the plain text.

3. FLOWCHART REPRESENTATION OF HYBRID CROSSOVER TECHNIQUE

A. Encryption

The detailed flowchart of the 2- stage Hybrid Crossover for encryption is given in the **Figure 3 (A)**. Each set of bits in a block is denoted by a number such as 1, 2, etc. '**X**' is indicating 1- Point crossover between two blocks of bits, and '**XX**' is indicating 2- Point crossover between the blocks of bits.

The first stage is a 1- Point crossover. The 8- bit binary data of two characters, represented by blocks **1** and **2** is divided into 4 blocks of 4 bits each, represented by blocks **1.a**, **1.b**, **2.a** and **2.b**. A pivot 'n' is selected, where n is a whole number from 0 to 3 as the block size is 4 here. A 1- Point crossover is done between blocks **1.a** and **2.b**, resulting in the children blocks **1.1.a** and **2.1.b**; and blocks **1.b** and **2.a**, resulting in children blocks **1.1.b** and **2.1.a**. The 4- bit blocks **1.1.a** and **1.1.b** are combined together to form an 8- bit block **1.1** and blocks **2.1.a** and **2.1.b** are combined to form block **2.1**.

The second stage is a 2- Point crossover between 2 blocks of 8-bit binary data each, represented by blocks **1.1** and **2.1**, and there are two pivots here, 'n' and 'n+4'. This crossover results in the children blocks **1.2** and **2.2**. The ASCII values of 8-bit are then converted to characters. Thus, by following this procedure we get the final cipher text.

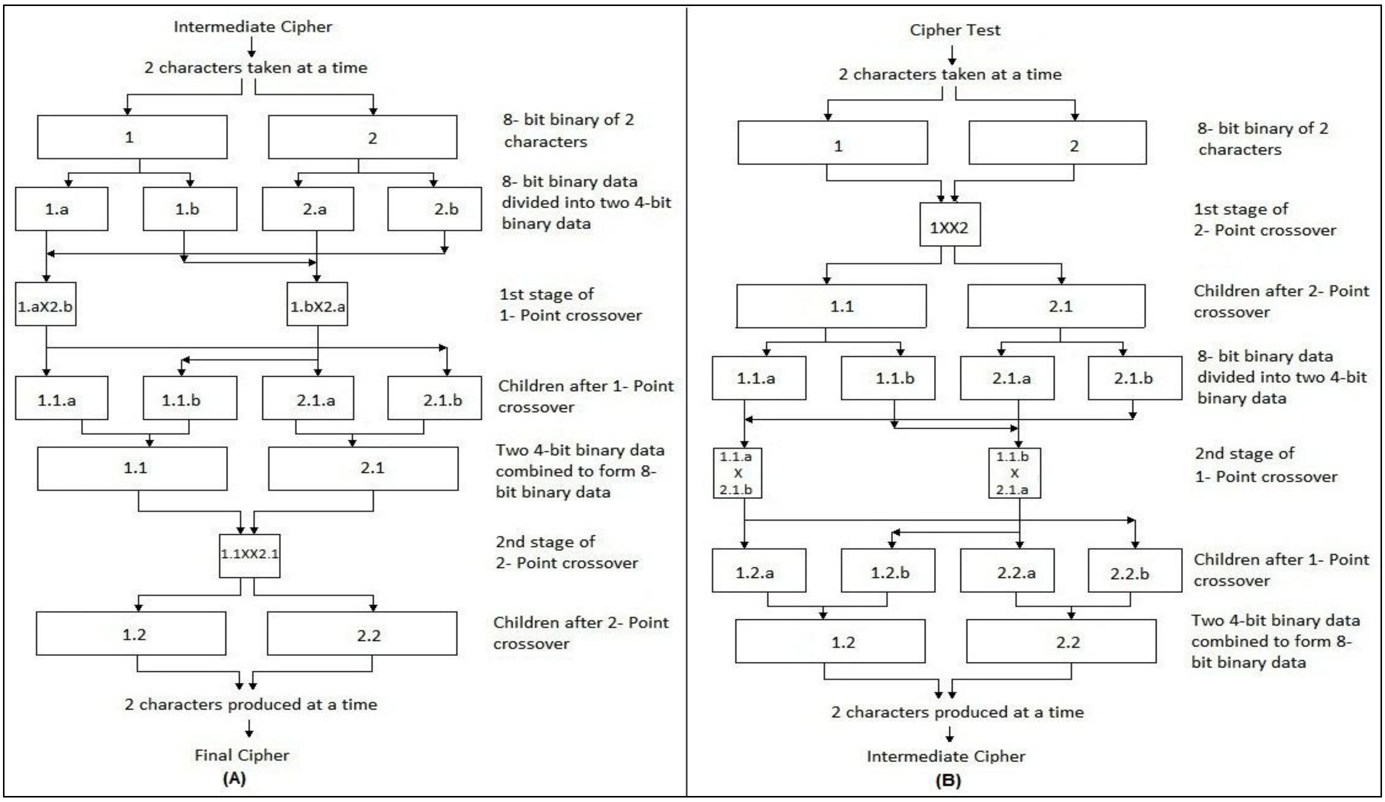
Intermediate Cipher
2 characters taken at a time
1
2
8- bit binary of 2 characters
1.a
1.b
2.a
2.b
8- bit binary data divided into two 4-bit binary data
1.aX2.b
1.bX2.a
1st stage of 1- Point crossover
1.1.a
1.1.b
2.1.a
2.1.b
Children after 1- Point crossover
1.1
2.1
Two 4-bit binary data combined to form 8-bit binary data
1.1XX2.1
2nd stage of 2- Point crossover
1.2
2.2
Children after 2- Point crossover
2 characters produced at a time
Final Cipher
(A)
Cipher Test
2 characters taken at a time
1
2
8- bit binary of 2 characters
1XX2
1st stage of 2- Point crossover
1.1
2.1
Children after 2- Point crossover
1.1.a
1.1.b
2.1.a
2.1.b
8- bit binary data divided into two 4-bit binary data
1.1.a X 2.1.b
1.1.b X 2.1.a
2nd stage of 1- Point crossover
1.2.a
1.2.b
2.2.a
2.2.b
Children after 1- Point crossover
1.2
2.2
Two 4-bit binary data combined to form 8-bit binary data
2 characters produced at a time
Intermediate Cipher
(B)

Figure 3: Hybrid Crossover for (A) Encryption and (B) Decryption

B. Decryption

Decryption is done in the reverse way. The detailed flowchart of the Hybrid Crossover for decryption is given in the Figure 3 (B). The pivots remain the same in decryption technique.

In the first stage, 2 characters of the cipher text are taken at a time, converted to 8- bit binary, represented by blocks **1** and **2;**.and a 2- Point crossover is done between these two blocks resulting in the blocks **1.1** and **2.1.** Block **1.1** is divided into 2 blocks **1.1.a** and **1.1.b** and block **2.1** is divided into 2 blocks **2.1.a** and **2.1.b** of 4 bits each.

In the second stage, a 1- Point crossover is done between blocks **1.1.a** and **2.1.b** resulting in blocks **1.2.a** and **2.2.b**, and between blocks **1.1.b** and **2.1.a** resulting in blocks **1.2.b** and **2.2.a**. The blocks **1.2.a** and **1.2.b** are combined to form an 8-Bit block **1.2** and the blocks **2.2.a** and **2.2.b** are combined to form block **2.2**. Then the blocks **1.2** and **2.2** are converted to the respective characters. Thus, by following this procedure we get the entire intermediate cipher text.

Further we would take an example to make the encryption technique clear.

4. EXAMPLE

A. Encryption

Let, for example, the plain text is **World'14**

We consider the co-ordinate axes here. Each character is placed on the clockwise spiral line which starts from Positive X- Axis, as shown below in **Figure 4**.

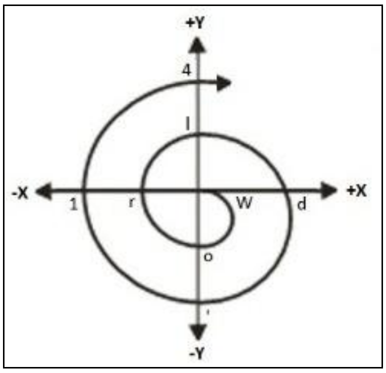

Figure 4: Encryption Example

Any non-prime random number is taken as the first key,
Let, First Key = **3160420**
Therefore, R = 3160420 % 256 = **100**

The substitution for the characters of plain test is given below:

In the 1st round of spiral path, substitutions for 'W', 'o', 'r' and 'l' are given below.

W = 87 = 87 + 100 = 187 = ╖
o = 111 = 111 – 101 = 10 = ◙
r = 114 = 114 – 102 = 12 = ♀
l = 108 = 108 + 103 = 211 = ╙

In the 2nd round of spiral path, substitutions for 'd', ' ' ', '1' and '4' are given below.

d = 100 = 100 + 104 + W = 204 + 87 = 291 = 35 = #
' = 39 = 39 – 105 + o = – 66 + 111 = 45 = -
1 = 49 = 49 – 106 + r = – 57 + 114 = 57 = 9
4 = 52 = 52 + 107 + l = 159 + 108 = 267 = 11 = ♂

Therefore, Intermediate Cipher text is ╖◙♀ ╙**#-9**♂

Now, in **Table 1**, the ASCII value of intermediate cipher text is represented by 8- bit binary.

TABLE 1: INTERMEDIATE CIPHER TEXT TO 8- BIT BINARY

CHARACTER	ASCII VALUE	8- BIT BINARY	BLOCK NUMBER
╖	187	10111011	1
◙	10	00001010	2
♀	12	00001100	3
╙	211	11010011	4
#	35	00100011	5
-	45	00101101	6
9	57	00111001	7
♂	11	00001011	8

We will take 2 blocks at a time and the Hybrid Crossover technique for encryption, as explained before, is applied on those 16- bits. Let **pivot (Second Key) be 2** and '**X**' sign represent 1-Point crossover and '**XX**' sign represent 2-Point Crossover.

[The pivot element is highlighted and the underlined bits are the bits that gets changed during crossover]

1) *Hybrid Crossover between Block 1 and Block 2*
10111011 X 00001010

a) *1-Point Crossover*

1011 **X** 1010   1011 **X** 0000
Result: 1010 1011   Result: 1000 0011

b) *2-Point Crossover*

10101000 **XX** 00111011
Result: 10111000 00101011

2) *Hybrid Crossover between Block 3 and Block 4*
00001100 X 11010011

a) *1-Point Crossover*

0000 **X** 0011   1100 **X** 1101
Result: 0011 0000   Result: 1101 1100

b) *2-Point Crossover*

00111101 **XX** 11000000
Result: 00000001 11111100

3) *Hybrid Crossover between Block 5 and Block 6*
00100011 X 00101101

a) *1-Point Crossover*

0010 X 1101   0011 X 0010
Result: 0001 1110   Result: 0010 0011

b) *2-Point Crossover*

00010010 **XX** 00111110
Result: 00111110 00010010

4) *Hybrid Crossover between Block 7 and Block 8*
00111001 X 00001011

a) *1-Point Crossover*

0011 X 1011   1001 X 0000
Result: 0011 1011   Result: 1000 0001

b) *2-Point Crossover*

10101000 **XX** 00111011
Result: 10111000 00101011

TABLE 2: 8- BIT BINARY TO FINAL CIPHER TEXT

FINAL RESULT	ASCII	CHARACTER
10111000 00101011	184 43	╕ +
00000001 11111100	01 252	☺ η
00111110 00010010	62 18	> ↕
10111000	24	↑

00101011	59	;

Therefore, Final Cipher Text is **╕+☺η>↕↑;**

B. Decryption

Cipher Text is **╕+☺η>↕↑;**

The ASCII value of the cipher text is now converted to its 8- bit binary equivalent in **Table 3.**

TABLE 3: FINAL CIPHER TEXT TO 8- BIT BINARY

CHARACTER	ASCII VALUE	8- BIT BINARY	BLOCK NUMBER
╕	184	10111000	1
+	43	00101011	2
☺	01	00000001	3
η	252	11111100	4
>	62	00111110	5
↕	18	00010010	6
↑	24	00011000	7
;	59	00111011	8

We will take 2 blocks at a time and the Hybrid Crossover technique for decryption, as explained before, is applied on those 16- bits. The **pivot (Second Key)** remains the same, i.e**.** **2**.

1) *Hybrid Crossover between Block 1 and Block 2*

10111011 X 00001010

a) *2-Point Crossover*

10111000 **XX** 00101011
Result: 10101000 00111011

b) *1-Point Crossover*

1010 **X** 1011 1000 **X** 0011
Result: 1011 1010 Result: 1011 0000
Final Result: 10111011 00001010

2) *Hybrid Crossover between Block 3 and Block 4*

00000001 X 11111100

a) *2-Point Crossover*

00000001 **XX** 11111100
Result: 00111101 11000000

b) *1-Point Crossover*

0011 **X** 0000 1101 **X** 1100
Result: 0000 0011 Result: 1100 1101
Final Result: 00001100 11010011

3) *Hybrid Crossover between Block 5 and Block 6*

00111110 X 00010010

a) *2-Point Crossover*

00111110 **XX** 00010010
Result: 00010010 00111110

b) *1-Point Crossover*

0001 **X** 1110 0010 **X** 0011
Result: 0010 1101 Result: 0011 0010
Final Result: 00100011 00101101

4) *Hybrid Crossover between Block 7 and Block 8*

00011000 X 00111011

a) *2-Point Crossover*

00011000 **XX** 00111011
Result: 00111000 00011011

b) *1-Point Crossover*

0011 **X** 1011 1000 **X** 0001
Result: 0011 1011 Result: 1001 0000
Final Result: 00111001 00001011

TABLE 4: BIT BINARY TO INTERMEDIATE CIPHER TEXT

FINAL RESULT	ASCII	CHARACTER
10111011 00001010	187 10	╗ ◙
00001100 11010011	12 211	♀ ╙
00100011 00101101	35 45	# -
00111001 00001011	57 11	9 ♂

Therefore, Intermediate Cipher Text is **╗◙♀╙#-9♂**

Next, we consider the co-ordinate axes here. Each character is placed on the clockwise spiral line which starts from Negative X- Axis, as shown below in **Figure 5.**

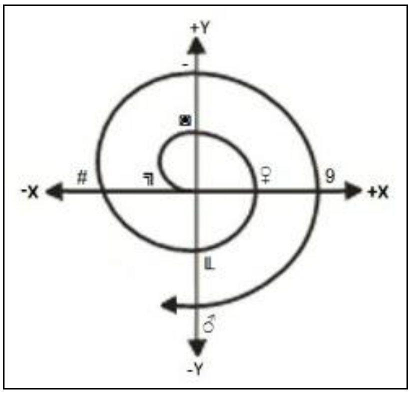

Figure 5: Decryption Example

The same non-prime random number has to been taken as the first key,

First Key = **3160420**

Therefore, R = 3160420 % 256 = **100**

The substitution for the characters of intermediate cipher test is given below:

In the 1st round of spiral path, substitutions for '╗', '◙', '♀' and '╙' are given below.

╗ = 187 = 187 – 100 = 87 = W
◙ = 10 = 10 + 101 = 111 = o
♀ = 12 = 12 + 102 = 114 = r
╙ = 211 = 211 – 103 = 108 = l

In the 2nd round of spiral path, substitutions for '#', '-', '9' and '♂' are given below.

# = 35 = 35 – 104 – W = – 69 – 87 = – 156 = 100 = d
- = 45 = 45 + 105 – o = 160 – 111 = 39 = '
9 = 57 = 57 + 106 – r = 163 – 114 = 49 = 1
♂ = 11 = 11 – 107 – l = – 96 – 108 = – 204 = 52 = 4

Therefore, Plain Text is **World'14**

5. CONCLUSION

The algorithm has been implemented and designed on ASCII data. This type of data can be easily converted to binary data. If only binary data is taken, the second approach only can be used to implement security. The key taken are random, thus enhancing security. Last but not the least, the run time of the proposed scheme is very low thus making it more feasible.

6. REFERENCES

[1] Poonam Garg, "Genetic algorithms and simulated annealing: a comparison between three approaches for the crypto analysis of transposition cipher", Journal of Theoretical and Applied Information Technology, Volume 5No4, pp.387-392, 2004

[2] Dr. G. Raghavendra Rao, Nalini .N, "A New Encryption and Decryption Algorithm Combining the Features of Genetic Algorithm (GA) And Cryptography", International Conference on Cognitive Systems, pp.1-5, New Delhi, December 14-15, 2004.

[3] A.J. Bagnall, "the application of genetic algorithms in cryptanalysis" School of Information System, University of East Anglia, 1996.

[4] N. Koblitz, "A Course in Number Theory and Cryptography", 2nd Edition, Springer- Verlag, New York, 1994

[5] S. Som, M. Banerjee, "Cryptographic Technique using Substitution through Circular Path Followed by Genetic Function", International Journal of Computer Applications, Special Issue, CCSN 2012, pp. 1-5, March, 2013.

[6] R. Toeneh, S. Arumugam, "Breaking Transposition cipher with genetic algorithm", ELEKTRONIKA IR ELEKTROTECHNIKA**,** The College of Information Sciences and Technology**,** The Pennsylvania State University, Volume 7(79), 2007.

[7] Atul Kahate, "Cryptography and Network Security" 2nd Edition, TATA McGRAW HILL Publications.

[8] Melanie Mitchell, "An introduction to Genetic Algorithms". A Bradford Book The MIT Press, Fifth Printing, 1999.