Cryptosystem using Crossover Function and Logical Operators

B. Reddaiah

Abstract: ***As technology is growing faster and exchanging of data is mostly carried through internet different mechanisms are being developed to counter unwanted access to the data. By introducing the web and pay out programs, it becomes very difficult to protect the data even with more mechanisms. It is becoming a big concern and worry in securing individuals data. These types of problems can be solved with cryptography and data can be secured in the network. In developing security systems Genetic algorithms are playing important role. In this proposed work crossover function from Genetic algorithms along with bitwise logical operations are used together to build a hybrid cryptosystem.***

Keywords: Security mechanisms, Security attack, Encryption, Decryption, Genetic algorithms, Crossover Function.

I. INTRODUCTION

In present days using of web services becomes essential for individuals and groups. With internet services from the past 25 years, communication is made possible and easy to communicate to all parts of the world. E-business is one area that picked with significant advantage that is provided by the internet. In this scenario securing confidential data becomes very important. As the electronic business field is growing more, a variety of secured applications that provides security are required. For providing better security, cryptography is the science that plays a vital role and one of the best methodologies. This science is having a huge and pretty good history in securing data [7]. It is more significant modem systems too [5]. This science provides absolute and reliable security by considering scientific functions that strengthen the security services along with mathematical operations.

Cryptography is followed from 1900 BC which is a scientific approach for encoding and decoding. This process was initialized and used when a scribe in Egypt initially utilized the customary techniques to communicate [3]. Earlier Julius Ceaser too used techniques to hide data and to communicate with his military officers [2]. By using cryptographic science data can be hidden so that it cannot be revealed to unauthorized individuals. It is seen as a strategy that changes the text from original form to another form that cannot be understood and thus to maintain and transmit the data safely [8]. The safety transmission is made possible by developing a mechanism that protects data and the process is known as encryption. When this process is used on any kind of data, it is impossible to bring the originality of data by not involving decryption process [6].

Revised Manuscript Received on December 08, 2019

Reddaiah Buduri*, Yogi Vemana University, Kadapa, Andhra Pradesh, India.

The hiding and un-hiding processes are execute by means of one important ingredient namely key. The privacy of information is based on calculations performed by operations of enciphering and deciphering and keys used [4]. This is considered as a primary element that is used in cryptographic calculations and to intensify overall activity of the system and it is considered as a primary ingredient. If key is compromised and made open to all then it is very easy for the unauthorized people to break the security even though the encryption and decryption algorithms are efficient and stronger in nature. As the key is an important factor in cryptosystems, usage of keys is classified into two forms. First one is single key cryptosystem that uses single key .Here common key is applied for enciphering as well as and deciphering. Another form is asymmetric cryptosystem or public key cryptosystem. Here two keys are used one to hide the information and the other to get back the original form of information.

II. CRYPTOGRAPHY AS BACKGROUND

Method of changing from original text to scrambled form is referred as encryption or enciphering and getting back original text from scrambled form is called decryption or deciphering [1]. The output of each algorithm demonstrates processing of text in encryption and decryption algorithms. In general two encryption techniques are used to process text. The first is the substitution technique by which each element of plain text in any form are replaced with text, that is difficult to understand and will become difficult for unauthorized people. The second is the transposition technique where elements of original text are reorganized into dissimilar way that is not same as original text and it is also difficult to read and understand. Along with this a combined technique called product cipher can be used. It is by combining more than one technique to secure text. When these techniques are used on the original text the primary constraint is that no data from the plaintext is to be lost. The next constraint is that all the text is to be reversible in nature.

III. PROPOSED SCHEME

Crossover is also one of the genetic operators as it generates or reproduces a new child by taking two chromosomes i.e. taking some attributes from first and remaining from second chromosome.

Crossover is divided into three types. They are Single point crossover, Two point crossover and Uniform crossover function. This proposed work is based on single point crossover function with logical operators.

A. Single point crossover Function

In this form of crossover, bare individual point is chosen to reproduce a fresh child as shown in Figure 1 and 2.

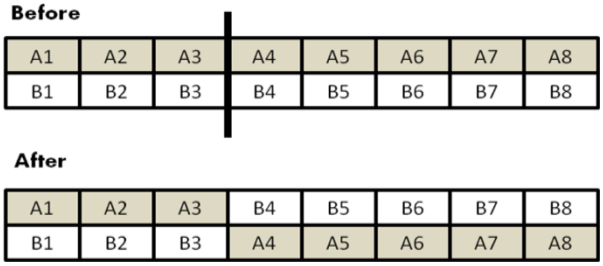

Fig. 1. Model of Single point crossover

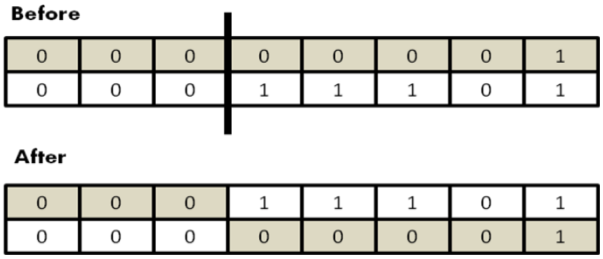

Fig. 2. Illustration of Single point crossover

B. Two-point crossover Function

In this form more than one point is taken to reproduce a new child as shown in Figure 3 and 4.

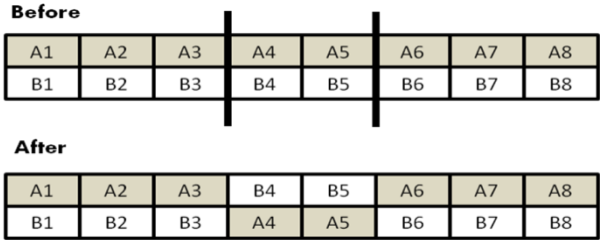

Fig. 3. Model of Two-point crossover

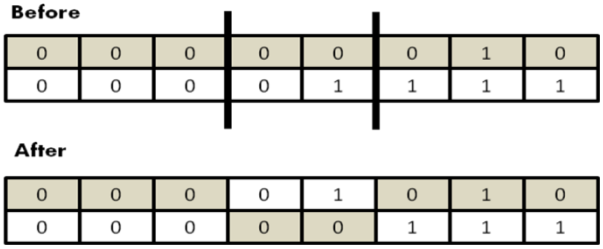

Fig. 4. Illustration of Two-point crossover

C. Uniform crossover Function

Here a bit is taken uniformly from each to reproduce a new child as shown in the Figure 5 and 6.

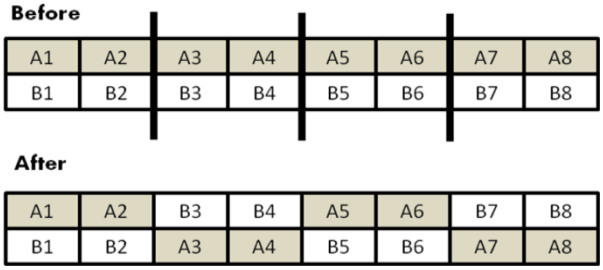

Fig. 5. Model of Uniform crossover

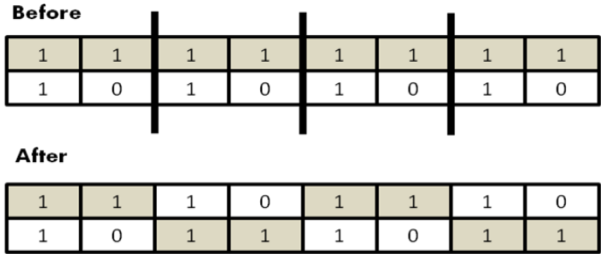

Fig. 6. Illustration of Uniform crossover

IV. PROPOSED CRYPTOSYSTEM

A. Framework for Encryption

Plain text is converted to cipher text by using Single point crossover function and logical operators as shown in Figure 7 and reverse is decryption as shown in Figure 8.

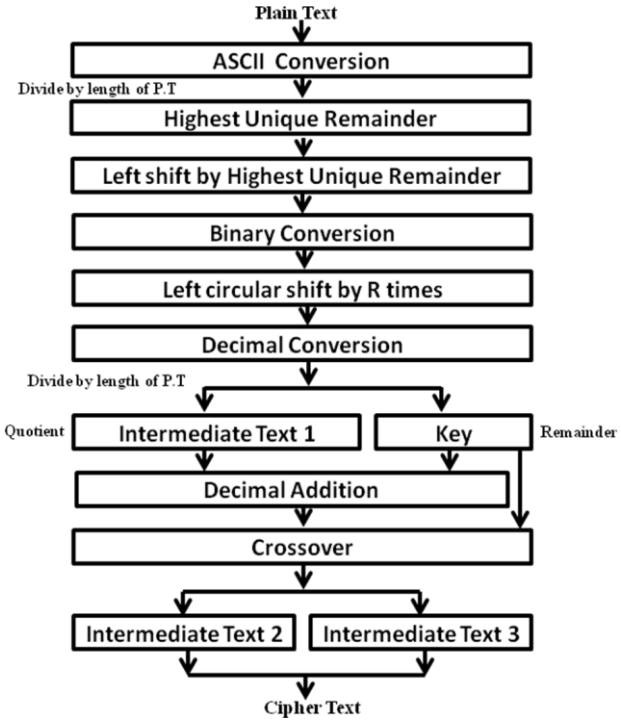

Fig. 7. Block Diagram of Encryption Process

B. Encryption Algorithm

STEP1: Start
STEP2: Read original data
STEP3: Generate ASCII code to original text
STEP4: Divide the ASCII values to the length of original text to get remainders.
STEP5: Identify unique remainder values
STEP6 Select the highest value among remainders (R).
STEP7: Left shift plaintext by highest unique remainder value.
STEP8: Change R values to binary values.
STEP9: Perform left circular shift process by R times.
STEP10: Convert the left circular shifted values into decimal values
STEP11: Divide the plain text by the length of it to get remainders and quotient values.

STEP12: Perform addition operation between quotient values and remainder value.
STEP13: Perform Crossover operation with addition resulted values and remainder values.
STEP14: Append those values by taking cipher 1 and cipher text 2.
STEP15: Stop

C. Framework for Decryption

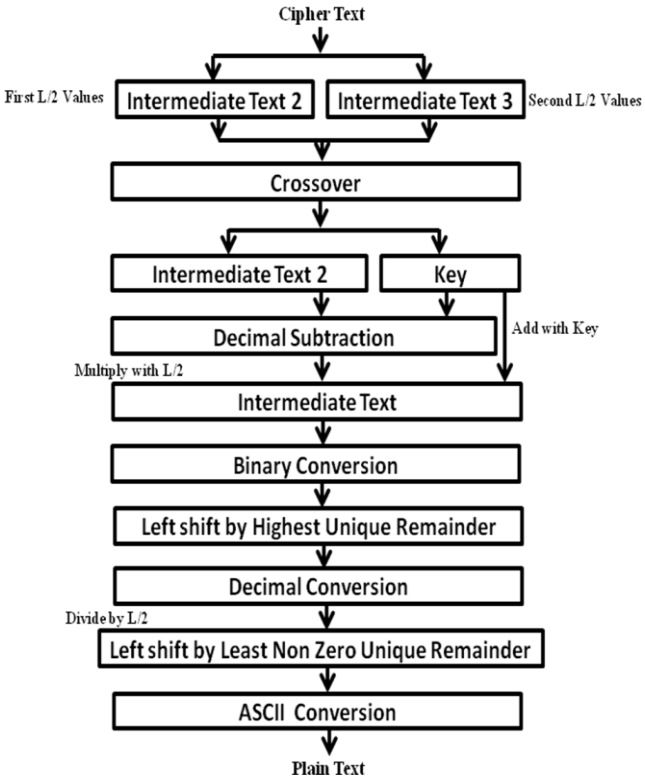

Fig. 8. Block Diagram of Decryption Process

D. Decryption Algorithm

STEP1: Start
STEP2: Read scrambled text.
STEP3: Split the scrambled text to two parts by its length.
STEP4: Consider the first part as Text3 and next part as Key.
STEP5: Perform crossover operation between Text3 and Key.
STEP6: Subtract key from Text3.
STEP7: Multiply subtraction result with length of first part and add key.
STEP8: Convert the output to decimal and then binary form.
STEP9: Perform right circular shift by R times
STEP10: Generate decimal values to shifted values
STEP11: Find unique remainders by dividing shifted values with length of plain text.
STEP12: Shift them by least non-zero unique remainder.
STEP13: Convert them to ASCII values
STEP14: Convert ASCII values to text
STEP15: Converted text is original text.
STEP16: Stop

V. RESULTS

After processing encryption and decryption algorithms by using Single point Crossover function with logical operators used on word 'GowthAm' the following data shown in Table I, Table II, Table III and Table IV are derived.

A. *Encryption*

The encryption algorithm used on the example word 'GowthAm' and results are shown in Table I followed by Table II.

Table –I: Outcome of Encryption process

Original Text	ASCII values	Length of text =L	Divide ASCII values by L to get remainders	Finding Unique remainders	Highest unique remainder (R)	Shift text to left by R times	Generate Binary values	Left circular shifting by R times
G	71	7	1	1	6	111	01101111	11011011
o	111		6	6		119	01110111	11011101
w	119		0	0		116	01110100	00011101
t	116		4	4		104	01101000	00011010
h	104		6			65	01000001	01010000
A	65		2	2		109	01001101	01011011
m	109		4			71	01000111	11010001

Table-II: Results of Encryption continued

Change to Decimal	Text 1 (Dividing by L to get quotients)	Key (Dividing by L to get remainders)	Decimal Addition (Text1, Key)	Crossover Cipher text 1 (CT-1)	Crossover Cipher text 2 (CT-2)
219	31	2	33	34	1
221	31	4	35	36	3
29	4	1	5	1	5

26	3	5	8	13	0
48	6	6	12	14	4
59	8	3	11	11	3
177	25	2	27	26	3

Plain text 'GowthAm' of size 7 characters is taken as input for encryption function and cipher text is generated as two parts namely CT-1and CT-2. The final cipher text is 34 36 1 13 14 11 26 1 3 5 0 4 3 3 after combining CT-1and CT-2.

B. *Decryption*

The encryption algorithm results for the example word 'GowthAm' are shown in Table I and Table II. The cipher text is 34 36 1 13 14 11 26 1 3 5 0 4 3 3 for decryption

Table-III: Outcome of Decryption

Cipher scrambled text length (L)	L/2 Initial values as CT-1	L/2 values as CT-2	Crossover for 1, 2		Decimal Subtraction (Text 3, Key)	((L/2)* Sub)+key Intermediate Text	Binary Form
			Text 3	Key			
14	34	1	33	2	31	219	11011011
	36	3	35	4	31	221	11011101
	1	5	5	1	4	29	00011101
	13	0	8	5	3	26	00011010
	14	4	12	6	6	48	01010000
	11	3	11	3	8	59	01011011
	26	3	27	2	25	177	11010001

Table-IV: Decryption Results Continued

Right circular shift by R	Decimal conversion as Text 4	(L/2) on Text 4 to get remainders	Unique remainders	Select least non-zero unique remainder	Rotate text 4 by least unique remainders	Plain text
01101111	111	6	6	1	71	G
01110111	119	0	0		111	o
01110100	116	4	4		119	w
01101000	104	6			116	t
01000001	65	2	2		104	h
01101101	109	4			65	A
01000111	71	1	1		109	m

The Cipher text with length 14 (34 36 1 13 14 11 26 1 3 5 0 4 3 3) when decrypted gets back the original plain text message word 'GowthAm' as shown in Table III, followed by Table IV.

VI. ADVANTAGES OF PROPOSED ALGORITHM

This work is carried out by using single point crossover function. This function has the capacity to process large dimensional values. Along with this simple logical operators are used that shows less complexity. Here there are no key transmission problems because separate key development and management is not essential, because it is a part of text itself.

VII. CONCLUSION

Different algorithms from the past are being used in building cryptosystems like paring functions. Functions like paring are purely mathematical that takes more time as the complexity increase and they are standard functions that may derive values in a standard way. The genetic algorithm used in this work is different in nature. In these algorithms data that comes out of these functions follows absolutely the property of 'Diffusion'. New data will evolve from the parent data that is very difficult to interpret. In this work single point crossover function. This is one of the versatile operations that are used in other traditional algorithms. By using the genetic algorithm we can provide more strength to entire process. In this process we used symmetric key that is generated from the text itself.

REFERENCES

1. Reddaiah, R Pradeep kumar Reddy, S. Hari Krishna "Enciphering using Bit–wise logical operators and paring function with text generated hidden key," IJCA (0975-8887), Vol. 121, No. 8, July 2015: pp. 30-35.
2. S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.
3. S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html
4. Behrouz A. Forouzan, Cryptography and Network Security, Special Indian Edition, TATA McGraw Hill.
5. *S. Tanenbaum, "Modern Operating Systems", Prentice Hall, 2003.*
6. Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.html#Algorithms
7. KHAN, "The Codebreakers", Macmillan Publishing Company, New York, 1967.
8. P. P Charles & P. L. Shari, "Security in Computing: 4th edition", Prentice-Hall, Inc., 2008.

AUTHORS PROFILE

Reddaiah is presently working in Department of Computer Applications, Yogivemana University. He completed his Ph.D in 2015 from Acharya Nagarjuna University, Guntur under the esteemed guidance of Dr R.Satya Prasad. He Published 25 International papers and attended 8 National and International conferences. The areas of research are Software Engineering, Security