ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Implementing a Cryptographic Protocol based on movement of Coin in Carom

Anupam Monda[1], Prof. Dr Pranam Paul[2]

MCA Final Year Student, Narula Institute of Technology, Agarpara, Kolkata, West Bengal, India[1]

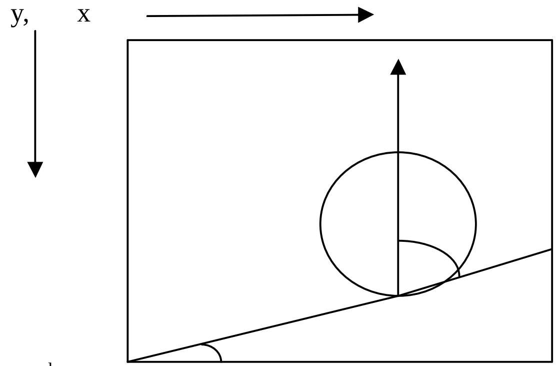
HOD, Department of Computer Application, Narula Institute of Technology, Agarpara, Kolkata, West Bengal, India[2]

ABSTRACT: Cryptography is a Greek word that's means is Hidden Secret. In any communication, security is the most important issue in today's world. Lots of data security and data hiding algorithms have been developed in the last decade, which worked as motivation for the research. The scenario of present day of information security system includes confidentiality, authenticity, integrity, non-repudiation. This present work focus is enlightening the technique to secure data or message with authenticity and integrity. With the growth of internet and network, the need for secure data transmission become more and more essential and important, as security is a major concern in the internet world. Data likely to be kept hide from all people except from the authorized user cannot be sent in plain text. So the plain text should be codified by the process of encryption. Each type of data has its own features; therefore different techniques should be used to protect confidential data from unauthorized access. Here we introduced a new algorithm which is based on simple mathematical operation. In this algorithm encryption is done on binary file so it can be applicable for any type of data such a text as well as multimedia data. Here the same idea of cryptography is working (i.e. using key, conversion of plain text into cipher text called encryption and the reverse, means cipher text to plain text called decryption).

KEYWORDS: Cipher Text, Cryptography, Encryption, Decryption, Plain Text, Symmetric Key.

I. INTRODUCTION

In our childhood when a playing ball dropped into a pond, we had thrown some stone such a manner that the ball comes towards us. But there was some problem then we come into carom board concept.
In this concept when we hit the carom's coin, the carom's coin will move any direction depending on the hitting point.
This concept is being implemented in our proposed algorithm for encryption and decryption. Here hitting a carom's coin, which is displaced a given unit of length, is formed by three consecutive blocks value.



Let's 1st block and 2nd block treated as the position of the carom's coin whereas 3rd block of the plain text will be treated as the radius of the coin. After the displacement of hitting the coin, the new position of the coin, the angle of the hitting force and the angle of the displacement is treated as encrypted blocks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

II. RELATED WORK

In [18] the author used perfect square number to calculate the difference between two numbers and calculated the number of bits required to represent them. In [17] the author emphasized on division method where how many times division method will be applied is calculated. In [7] author used primer number from where basic concept of this algorithm is obtained. Each author has shown different ways of strengthening security to data. . In this algorithm encryption and decryption process are performed on binary data. All data which is under stable by the computer is finally converted into binary bits. So it can be implemented for any data type encryption process. Therefore that encryption technique can be used for text encryption, image encryption etc

III. EXAMPLE

3.1 Key: Block Size (e.g. n), moving unit (e.g. f).

3.2 Encryption:

Step:-1Pick three blocks from the binary stream of ASCII value of plain text file. The each block size is equal to the block size of key file.

Step:-2 1st block of plain text we consider as x,2nd block is consider as y,3rd block is consider as r. Where (x, y) is the position of a carom board's dice and r is the radius of the dice.

Step:-3 At first we hit the dice from (0, 0) position, θangle and hit the dice at (x1, y1) position. Then we calculate the path.

Eq-1.1: y1 = $\tan\theta\, x1$=m1x1.

As $tan\theta$ = m1.

And from the following equation we put y1 value.

$$(x - x1)^2 + (y - y1)^2 = r^2$$

$\Rightarrow (x - x1)^2 + (y - mx1)^2 = r^2$

From the above equation we put x, y and r value.

Example-$(2 - x1)^2 + (3 - 1.55740772465 * x1)^2 = r^2$

Step:-4 we get x1 two values from following equation.

X1=$\frac{-b+\sqrt{b^2-4ac}}{2a}$, x1= $\frac{-b-\sqrt{b^2-4ac}}{2a}$

We choose low value of x1 and this value put into Eq-1.1 and get y1.We get the hit point of the dice.

Step:-5 After hitting the dice it will move the hitting point and centre point towards and dice will move the distance that is equal to the moving unit of key file.

Step:-6 we calculate the new position of the carom's coin(x2, y2)

$$(x, y) = \frac{f}{f + r}(x1, y1) + \frac{r}{f + r}(x2, y2)$$

From the above equation we put x, y, m, r, x1, y1 values and get the x2, y2 values.

Step:-7 We convert the x2, y2, θ values to binary number and store in cipher text file.

Step:-8 we calculate the magnitude of the line which is the dice moving.Eq-1.2

$$\frac{y2 - y}{x2 - x} = m2$$

We calculate the angle(θm) of dice movement.

$$\theta m = \tan^{-1}\left\{\frac{m2 - m1}{1 + (m1 * m2)}\right\}$$

We store the binary value of $\theta m$to cipher text file.

Step:-9 we get the cipher text of the plain text file.

3.3 Decryption:

Step:-1Pick three blocks from the binary stream of ASCII value of cipher text file. The each block size is equal to the block size of key file.

Step:-2 1st block of cipher text we consider as x2,2nd block is consider as y2,3rd block is consider as θ and 4th block we consider as θm. Where (x2, y2) is the moved position of a carom board's dice.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Step:-3 We calculate the hitting line of the carom.
Eq-2: y1=tanθx1=mx1.
And we know m= tan $(\theta + \theta m)$ and

$$\frac{(y2 - y1)}{(x2 - x1)} = m$$

Where we put the y2, x2 and y1 value from Eq-2 and calculate the x1 value. Again put the x1 value into Eq-2 and get the (x1, y1) value that is the hitting point of carom.
Step:-4 After that we found the radius(r).

$$(x1 - x2)^2 + (y1 - y2)^2 = (f + r)^2$$

Put the value of x1,x2,y1,y2 and f (from key file) and get the value of radius.
Step:-5 the following equation we put x1, y1, x2, y2, m values and we get the x, y.

$$(x, y) = \frac{f}{f + r}(x1, y1) + \frac{r}{f + r}(x2, y2)$$

Step:-6 we convert the x, y and r value to binary stream and then convert to ASCII value.

IV. EXAMPLE

4.1 Key Generate: Let Block size (n) = 4,
And the distance the carom's coin traversing (f) = 3.
4.2 Encryption:
Let the plain text file content "JI".
Step:-1 pick ascii value of each character and make a binary stream.
010010100100100
Pick block size number binary digit and convert into decimal value. 1st value is treat as x, 2nd is y, and 3rd is r. so x = 4, y = 10, r = 4.
Step:-2
1st we hit the carom coin from 0 degree (θ) to $\tan^{-1}(y/x)$ = 68.19859051
Step:-3 calculate the radian value of the angle from $(\pi * \theta)/180$
And get the magnitude value m1 =$\tan\theta$.
m1=0
Step:-4 calculate the a= 1+ $m1^2$, b= 2* (x+ m1*y), c = $x^2 + y^2 - r^2$
a= 1.00,b=-8.000, c=100.00
Then check $(b^2 - 4 * a * c) > 0$ (1)
Here its value -384 that is not getter than 0.(so the process repeated from step:-3 increase the theta value 5. In this case when θ= 50 then a= 2.422304452, b= -31.852081272, c= 100.0000. and45.63330056 is getter than 0 it will go next step.).
If it is satisfy then we go to next step.
Step:-5 then calculate the hitting point (x1,y1)
X1=$\frac{b+\sqrt{b^2-4*a*c}}{2*a}$,
X1= 7.969131144
x1= $\frac{b-\sqrt{b^2-4*a*c}}{2*a}$
x1=5.180364263
Here we accept the lowest value of x1 i.e. 5.180364263.
Step:-6 after hitting the coin, it will move and we calculate the new position of the coin (x2, y2).
X2=((f-x)+(r*x)-(f*x1))/r
Here x2= 3.114726883
And y2=((f-y)+(r*y)-(f*y1))/r
Here y2=12.866407397
Step:-7 we get the new position of the coin. We calculate the how much move the coin from original position (θm). First we must calculate the magnitude of the line i.e. m2

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

And m2 = (y2-y)/(x2- x)
Here m2= -3.237878891.
Step:-8 we calculate the angle of the coin movement (θm).

$$\theta m = \tan^{-1}\left\{\frac{(m2 - m1)}{1 + (m1 * m2)}\right\}$$

Here θm= 0.997331281.
It's radian value. We convert the value to degree so now value of θm= 57.119882453.
Step:-9 round off the value of x2, y2, $\theta, and\ \theta m$. So now value is
X2 = 3, y2 = 13, θ=50, θm=57
Step:-10 Here some unused bit there so we remain bit are unchanged and store these. How many number of unused bits are there, the value store in key. After that x2, y2, $\theta, and\ \theta m$ values are store. That is our cipher text. Here our cipher text is

"=Œ¤"

4.3 Decryption:
Step:-1 1st pick all ASCII value of the character and covert into binary stream.
Step:-2 we pick the binary bit equal to block size number from key.1st segment as x2= 3, 2ndsegment is y2= 13, θm= 57, θ= 50.
Step:-3 convert the all angel value from degree to radian. So,
θ= (θ*π)/180, = 0.873015873.
θm = (θm*π)/180, = 0.995238095.
Step:-4 then we calculate the magnitude of the hitting line (as m1) and the movement of the coin line (as m2).
The value of m1 =$\tan\theta$, = 1.192604064.
The value of m2=$\tan\ (\theta m + \theta)$=- 3.262082808.
Step:-5 Then we calculate the inter section point and the inter section point is the hitting point of the coin. Hitting point is x1,y1.
Value of x1 =$\frac{y2-(m2*x2)}{m1-m2}$, = 5.115117869.
We know y1= m1* x1.Put the value of m1 and x1 and get the y1 value so y1 =5.976749324.
Step:-6 Then we must calculate the original position of the carom's coin i.e. x, y and radius of the coin (r).
$(r - f)^2$=$(x1 - x2)^2 + (y1 - y2)^2$, put the value in the equation and calculate the r value.
r =4.334832899.
Step:-7 after calculating the radius of coin we calculate the original position of the coin i.e. x, y.
Value of x= $(((f * x1) + (r * x2))/(f + r))$
x =3.865098592
Value of y= $(((f * y1) + (r * y2))/(f + r))$
y =10.1274394
Step:-8 we round off the value of x, y and r value and convert the decimal number to block size equal number binary digit and get a binary stream.
x =4, y =10, r =4.
Step:-9 the binary stream will convert into decimal and get the original text or plain text i.e. "JI",

V. RESULT ANALYSIS

5.1 Algorithm:

- At first when we hit a coin the coin will move towards the line which is from the hitting point through the centre of the coin. When it goes upward then the new position will positive segment. If it goes downward direction then new position will negative segment. So avoid going the negative segment we hit the coin from 0degree to $\tan^{-1}\frac{y}{x}$ where x, y is the original position of the coin.
- When we draw a line from a fixed position. In the line if $(b^2 - (4 * a * c))$ value is negative that's mean there is no touch point with the particular point. If the value is positive then there is a touch point with the particular carom's coin.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

5.2.Size and Time Comparative Report: We analysis the plain text file size, total time for encryption to create encrypted file and in the same way the total time for decryption and the encrypted file size to create a decrypted file. In this section we compare file size with the time for clear observation.

Original File Size	Encrypted File Size	Encryption Time(Sec.)	Encryption Time/Byte
2	4	0	0
38	82	0.054945	0.00067006
380	689	1.043956	0.001515175
151552	328704	4.175824	0.000012703

Table: 5.2.1

The above table shows the original final size that is encrypted and after encryption the encrypted file and how it takes the time to encrypt the file.

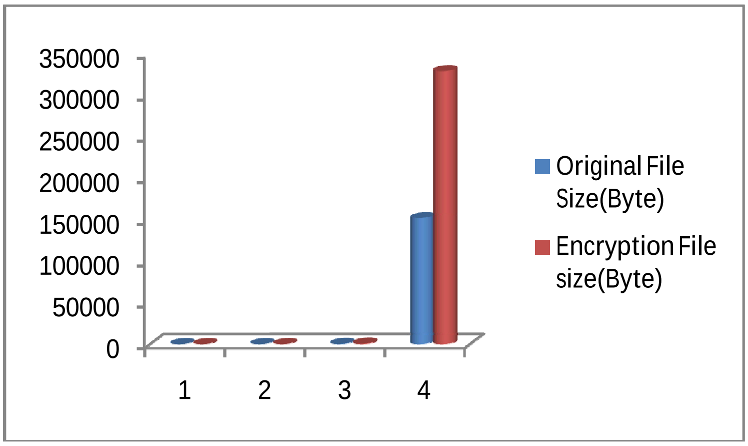


Fig:5.2.1
Original file size vs. encrypted file size

Here we see that after the encryption the file size will increase. We decide to see the fig.

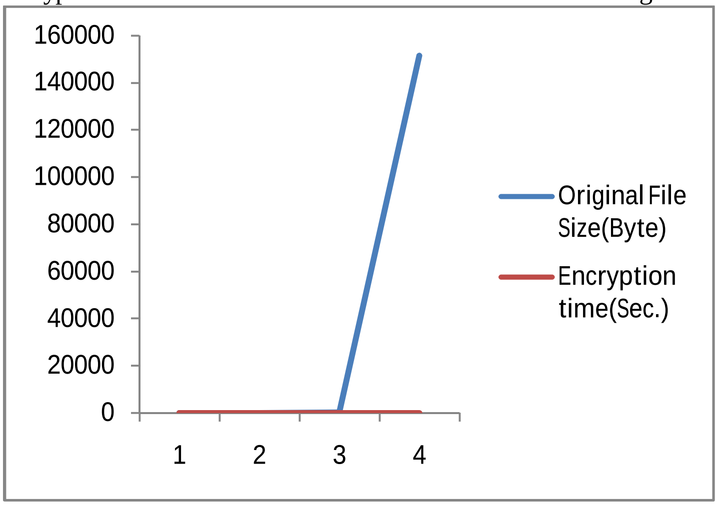


Fig: 5.2.2
Original file size and encryption time.

Here we see that how much time takes for the original file size. In this case we see when the file larger than it takes more time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Original File Size	Decrypted File Size	Decryption Time(Sec.)	Decryption Time/Byte
2	2	0	0
38	38	0.016484	0.000433789
380	380	0.879121	0.002313476
151552	151552	3.791209	0.000025015

Table: 5.2.2

The above table shows the original final size that is decrypted and after decryption the decrypted file and how it takes the time to decrypt the file.

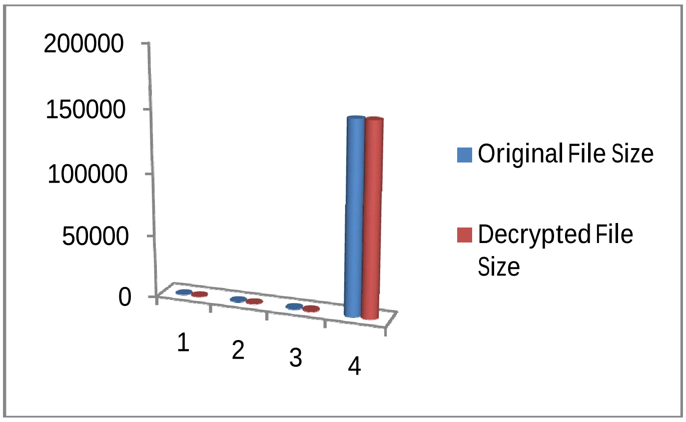


Fig: 5.2.3
Original file size vs. encrypted file size

After decryption we get back the original file size that is the same as the original file size. So, we can tell the decryption process execute in proper way.

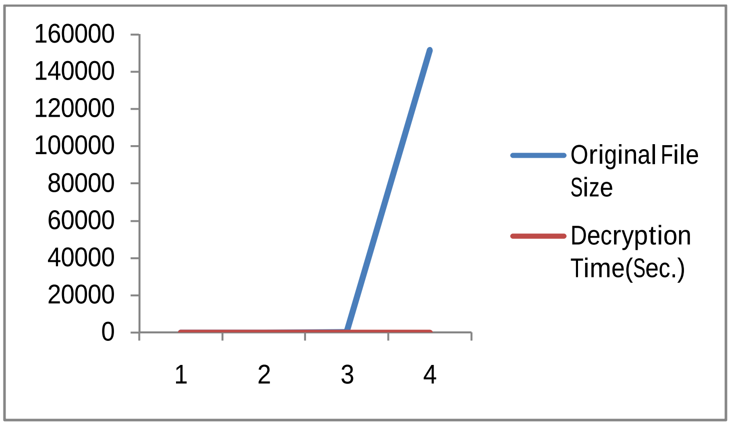


Fig: 5.2.4
Original file size and encryption time.

Here we see that how much time takes for the original file size. In this case we see when the file larger than it takes more time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

VI. CONCLUSION

My conclusion towards this algorithm is that I have tested the implementation of this algorithm and this algorithm worked correctly for the above set of values. From this we can assume that algorithm can correctly be implemented for various type and size of file. It will be secured.

REFERENCES

[1] William Stallings, "Cryptography and network security principles and practices", 4th edition, Pearson Education, Inc. publishing as Prentice Hal, 2006.
[2] Pranam Paul, Saurabh Dutta, A K Bhattacharjee, "An Approach to ensure Security through Bit-level Encryption with Possible Lossless Compression", International Journal of Computer Science and Network Security", Vol. 08, No. 2, pp.291 – 299, 2008.
[3] Sanjit Mazumdar, Sujay Dasgupta, Prof.(Dr) Pranam Paul, "Implementation of Block based Encryption at Bit-Level", International journal of Computer Science and Network Security, Vol. 11, No.2, pp. 18-23, 2011.
[4] Sujay Dasgupta, Sanjit Mazumdar, Prof.(Dr) Pranam Paul, "Implementation of Information Security based on Common Division", International journal of Computer Science and Network Security, Vol. 11, No.2,pp. 51-53, 2011.
[5] http://en.wikipedia.org/wiki/Symmetric-key_algorithm
[6] Asoke Nath, Saima Ghosh, Meheboob Alam Mallik, "Symmetric Key Cryptography using Random key Generator", Proceeding of International conference on security and management (SAM'10" held at Las Vegas, USA Jull 12-15,2010), P-Vol-2, pp. 239-244,2010.
[7] Pranam Paul, Saurabh Dutta, "An Enhancement of Information Security using Substitution of Bits Through Prime Detection in Blocks", Proceeding of National Conference on Recent Trends in information Systems(ReTIS-06), Organized by IEEE Gold Affinity Group, IEEE Calcutta Section,Computer Science & Engineering Department, CMATER &SRUVM Project-Jadavpur University and Computer Jagat.
[8] Oded Goldreich, "Foundation of Cryptography (A primer)", July 2004.
[10] Denise Sutherland, Mark Koltko-Rivera "Cracking Codes and Cryptograms For Dummies"; ISBN: 978-0-470-59100-0;October 2009 [11] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone "Handbook of Applied Cryptography"; CRC Press; ISBN: 0-8493-8523-7
[12] WILLIAM 'F. FRIEDMAN; "MILITARY CRYPTANALYSIS, Part I, MONOALPHABETIC SUBSTITUTION SYSTEMS"
[13] Wenbo Mao; "Modern Cryptograph"..
[14] Wels Chenbach; "Cryptography in C and C++".
[15]Ayan Banrjee, Prof. Dr.Pranam Paul, "Bock Based Encryption and Decryption", International journal of Computer Science and Network Security, ISSN: 0974 – 9616 vol-7,No.2,2015.
[16]Shibaranjan Bhattacharyya, Prof. Dr.Pranam Paul, "An Approach to Block Ciphering using Root of Perfect Square Number", International journal of Computer Science and Network Security ISSN: 0974 – 9616 vol-7,No.2,2015.
[16] Anupam Mondal, Prof. Dr.Pranam Paul, "Implementing Cryptography on the Concept of Returning Back Its Own Nest of a Bird", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,ISSN (Print): 2320-9798 vol-4,Issue-2,2016.
[17]Subir Sharma, Prof. Dr. Pramnam Paul," An Approach to Block Based Ciphering Using Bit Wise Calculation for Representation of A Number Using Its Corresponding Perfect Square Number and Position of Prime Number", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,ISSN (Print): 2320-9798 vol-4,Issue-2,2016.
[18] Sukanya Chakravarty, , Prof. Dr. Pramnam Paul," Approach Based on Finding the Difference between Consecutive Numbers", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,ISSN (Print): 2320-9798 vol-4,Issue-2,2016.

BIOGRAPHY

Anupam Mondal, he is a student of MCA from Narula Institute of Technology and former student of BCA from B.P.Poddar Institute of Management & Technology under WBUT.

Dr Pranam Paul, Assistant Professor and Departmental Head, CA Department, Narula Institute of Technology (NIT), Agarpara had completed MCA in 2005. Then his carrier had been started as an academician from MCKV Institute of Technology, Liluah. Parallel, At the same time, he continued his research work. At October, 2006, National Institute of Technology (NIT), Durgapur had agreed to enroll his name as a registered Ph.D. scholar. Then he had joined Bengal College of Engineering and Technology, Durgapur. After that Dr. B. C. Roy Engineering College hired him in the MCA department at 2007. At the age of 30, he had got

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Ph.D. from National Institute of Technology, Durgapur, and West Bengal. He had submitted his Ph.D. thesis only within 2 Years and 5 Months. After completing the Ph.D., he had joined Narula Institute of Technology in Computer Application Department. Parallel he continues his research work. For that, he has 39 International Journal Publications among 54 accepted papers in different areas. He also reviewer of International Journal of Network Security (IJNS), Taiwan and International Journal of Computer Science Issue (IJCSI); Republic of Mauritius.