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 Data Security with an Approach Based On the Transformation of a Matrix with Rows and Columns

Sukanya Chakravarty[1], Prof. (Dr.) Pranam Paul[2]

Final Year Student of MCA, Narula Institute of Technology, Agarpara, Westbengal, India[1]

HOD, Department of Computer Application, Narula Institute of Technoloy, Agarpara, Westbengal, India[2]

ABSTRACT:-In recent days, for secure information transmission through internet, Cryptography is used. Here for secure data communication the plain text would be encrypted into cipher text using encryption process. This encrypted text along with the key or information would be send by the sender at receiver's end. Then using the key or information, the receiver would able to decrypt the encrypted text. Using this base idea there exist different algorithm for encryption and decryption and for key generation. Here our basic idea is basedonswapping the rows and column of a matrix. The strength of the technique is analyzed in this paper. This is a block based private key cryptographic technique. From the bit level corresponding decimal value is obtained , after this certain decimal value is selected and stored in a matrix column-wise . These stored values from matrix is subtracted from each other and new value is obtained that would be our encrypted value .The process is later discussed in details in this paper.

KEYWORDS: Cryptography, Encryption, Decryption, Cipher, Private key, Symmetric key, Plain Text.

I. INTRODUCTION

For secure information transmission through internet, as the complexity of the threats increases, so the security measures required to protect networks. In order to protect data from unauthorized intruder data must be transmitted in encrypted form. To achieve this goal, network security and cryptography has now become an emerging research area to develop encryption algorithm, decryption algorithm, key generation algorithm and key matching algorithm for proper secure transaction from sender to receiver, avoiding any middle attacker. To be secured, information needs to hidden from unauthorized access (middle attack), protected from unauthorized change, and available only to the sender and receiver. Cryptography, not only protects data from hacking or alteration, but can also be used for userauthentication. The scenario of present day of information security system includes confidentiality, authenticity, integrity, and non-repudiation . Security breaches can often be easily prevented. How? This guide provides you with a general overview of the most common network security threats and the steps you and your organization can take to protect yourselves from threats and ensure that the data travelling across your networks is safe . Each type of data has its own features; therefore different techniques should be used to protect confidential data from unauthorized access. Here the same idea of cryptography is working. After encryption the encrypted file size can be decreases or increases based on some component related to the algorithm and the file on which the encryption process will apply and also for encrypted file size decrease, it results possible lossless compression. In section III , the algorithm is described. Section IV describes the whole process with an example. In sectionV, a result analysis is done executing the technique on some real files. An analysis has been done in section VIalong with conclusion.

II. RELATED WORK

The author used perfect square number to calculate the difference between two numbers and calculated the number of bits required to represent them [15]. The author emphasized on division method where how many times division method will be applied is calculated [14]. Depending on the primer number, basic concept of this algorithm is obtained [7]. 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

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

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. ALGORITHM

In this section, key structure is discussed in section 1 and encryption and decryption process is discussed in section 2 and 3.

1. KEY STRUCTURE

Segment	Description
1	Block Size(bs)
2	Any two digit number.(10-99)
3	Unused Block(ub)
4	The no. of extra bit(u_blk)

2. ALGORITHM OF ENCRYPTION:-

Step 1- At first we need to convert the plain text into its binary form thus creating a bit stream.
Step 2- A Block Size(bs) is taken and defined it in the 1st segment of the key. As per the block size the decimal is calculated from the binary bit stream.
Step 3- Now take any two digit random number from the user which is stored in the 2nd segment of the key.
Step 5- Separate this two digit number and calculate in how many ways we can get that digit by adding two digits. we avoid repetition and if n is the maximum digit in the number then we avoid (0+n) also because in n*n matrix there is no option for 0th row or nth column.
Step 6- Now find which digit is maximum from that number. Suppose n is the maximum number among them so n*n matrix is created.
Step 7- Now depending upon the Block size(bs) the decimal values are placed into the n*n matrix.
Step 8- Now at first we have to interchange the row with column depending upon the adding numbers. Suppose here (0+(n-1)) is selected so the 0th row is interchanging with (n-1)th column. In three places like rr, cc and rc the value is changing after the process. In rc position two values are appearing so we add that two values and putting in that place like rc=rr+cc. rr and cc position hold same value so we apply the below process to that positions
rr = rc +cc and cc = rc + rr
Step 9- step 7 is repeated for another combination.
Step 10-There is another matrix created which hold the block size after the above application. The block size of those particular position rr,cc,rc will be increased after the process.
Step 11- Now one by one store the value of elements of 1st matrix's with the bit stream reflected in the corresponding cell in the 2nd matrix.
Step 12- After completing step 10 we got a binary bit stream named as bt_strm which is actual bit stream generated after encryption.
Step 13- Now the same process will be continue with creating of the next matrix with n*n number of element from the source bit stream.
Step 14-During the formation of the n*n number of the source bit stream in each step may be at last step there are no sufficient bit stream to form n*n matrix. In that case we collect all the bit stream at u_blk.
Step 15- After the entire process which is define just above, there may be also p number of bits are remaining where p<bs. This p no. of bits are named as unused bit(ub) has been stored into the 3rd segment of key. This p no. of unused bit has been stored into the ub segment.
Step 16- Now to create the entire encrypted bit stream or target bit stream by appending in following sequence ub, u_blk, bt_strm. Now it is converted into the encrypted text.

3. ALGORITHM OF DECRYPTION:-

Step 1-Convert the encrypted form into its binary form.
Step 2- As per the 3rd and 4th segment of key we subtract the number of unused bit(ub) and u_blk from the total number of binary bit stream and continue the further decryption process depending on the resultant binary stream.

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-From the 2nd segment of the key take that two digit number for further process.
Step 4- Separate this two digit number and calculate in how many ways we can get that digit by adding two digits. we avoid repetition and if n is the maximum digit in the number then we avoid (0+n) also because in n*n matrix there is no option for 0th row or nth column.
Step 5- Now find which digit is maximum from that number. Suppose n is the maximum number among them so n*n matrix is created.
Step 6- Considering Block Size of the bit size matrix of the corresponding cell we take binary values which is converted into its decimal form and place it into the above mention n*n matrix.
Step 7- Considering the step 4 we get some combinations. At the time of decryption we follow just the reverse order mentioned in the encryption. From here we get the cell rr, cc, rc by which we do the further work.
Step 8- we have three equation rc= rr+cc, rr=rc+cc and cc=rc+rr. After solving this three equation the primary matrix is created. From this matrix we get the decimal values that isdc_strm.
Step 9- Now from the 4th segment of key we take the bits of u_blk and convert the bits of u_blk into their decimal form and append this numbers after the above mention decimal numbers like dc_strm, u_blk. Now convert this whole decimal numbers into the binary bit stream.
Step 10- Now from the 3rd segment we get ub if any and append this with the above mention binary bit stream.
Step 11- Now in the final step the entire binary stream is converted into the normal file according to the ASCII value.

IV. EXAMPLE

To illustrate this algorithm an example has been shown. Let consider a small plain text “SUKANYA”.

1. KEY STRUCTURE

The key structure for this example is shown below in the table 1.1

Table 1.1
Key Structure

Segment	Description	Value of the segment
1	Block Size(bs)	4
2	Any two digit no.	31
3	Unused Block(ub)	0
4	No. of extra bit(u_blk)	5

EXAMPLE OF ENCRYPTION:
S–> 83→ 01010011
U → 85 → 01010101
K→ 75→ 01001011
A→ 65 → 01000001
N→78 → 01001110
Y→ 89 →01011001
A→ 65 → 01000001
Block Size= 4
Separate this binary values depending upon the Block Size.
0101 0011 0101 0101 0100 1011 0100 0001 0100 1110 0101 1001 0100 0001
Convert this binary stream into its decimal value we get
5 3 5 5 4 11 4 1 4 14 5 9 4 1
A two digit number which is the 2nd segment of key = 31
3 is the maximum digit among the no. 31. As per algorithm here 3*3 matrix is used.

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

	0	**1**	**2**
0	5	3	5
1	5	4	11
2	4	1	4

Now 31→3 1
3= (0+3),(1+2),(2+1),(3+0)
1=(0+1),(1+0)

As per the algorithm (1+2) and (0+1) is selected. So first Row= 1 is interchanging with Column= 2 .After the process we get,

	0	**1**	**2**
0	5	3	5
1	5	11+4=15	4+4=8
2	4	1	11+4=15

After this application the another matrix is holding the block size like

4	4	4
4	5	5
4	4	5

Now Row= 0 is interchanging with Column=1 .After the process we get,

	0	**1**	**2**
0	3+15=18	5+15=20	1
1	5	3+5=8	8
2	4	5	15

After this application the another matrix is holding the block size like

5	5	4
4	6	5
4	4	5

As per the algorithm we get this binary stream
10010101000001010100100001000010001010111 1
And for this extra 5 decimal values 14 5 9 4 1 as per the algorithm we get this binary stream
11100101100101000001100101010000010101001000010000100010101111
å”PT„"¼
This is the encrypted form of the plain text.

2. EXAMPLE OF DECRYPTION:

The encrypted form is **å”PT„"¼**
Converting the ASCII value into its binary form we get
11100101100101000001100101010000010101001000010000100010101111
There are 5 extra bit of block size that is 5*4=20 bit. So 1st we have to subtract 20 bit from this binary stream. Applying this process we get 10010101000001010100100001000010001010111 1
Now as per the 2nd matrix's value which are block size this binary stream is converted into its decimal form.Place this decimal values into the matrix we get,

	0	**1**	**2**
0	18	20	1
1	5	8	8
2	4	5	15

Now as per the algorithm
First we work with 0 Row and 1 Column.

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

rc = rr+cc …….(1) rr = rc+cc……(2) cc= rc+rr ……..(3)
Solving this three equation we get;

	0	**1**	**2**
0	5	3	5
1	5	15	8
2	4	1	15

Now we work with 0 Row and 1 Column.
Applying the same process on this matrix we get,

	0	**1**	**2**
0	5	3	5
1	5	4	11
2	4	1	4

From this matrix we get this decimal values
5 3 5 5 4 11 4 1 4
Converting this decimal values into its binary form and the above mention 20 bits of binary values we get,
0101 0011 0101 0101 0100 1011 0100 0001 0100 1110 0101 1001 0100 0001
Entire decrypted binary stream is converted into the normal file according to the ASCII value which is the plain text "SUKANYA".

V. RESULT ANALYSIS

In this algorithm encryption is perform on binary data. All data is finally converted into binary bits. So it can be implemented for any data type. Therefore that encryption technique can be used for text encryption, image encryption i.e., multimedia encryption process.

Size and Time Comparative Report

This algorithm has been implemented on number of data files varying types of content and sizes of wide range, shown in Table-1 and Table-2. Here we compare between the plain text file size, encrypted file size, encryption time, encryption time/byte. And also the comparison between the encrypted file size, decrypted file size, decryption time and decryption time/byte.

TABLE -1
Size and Time Comparative Table of encryption

FileName	**FileSize (in Kb)**	**Encrypted File (in Kb)**	**Encryption Time(in sec)**	**Encryption Time/ Byte**
Msg a.txt	1	1	3.24175824	3.24175824
Msg q.txt	1	1	30.32967033	30.32967033
Msg r.txt	1	1	17.47252747	17.47252747
Msg s.txt	6	6	28.32978034	4.7216350
Msg e.txt	1	1	12.6923069	12.6923069

Now from the above table it is visible that the result of encrypted file size is same as the plain text file size. The graphical representations associated with the table 1 are shown below.

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

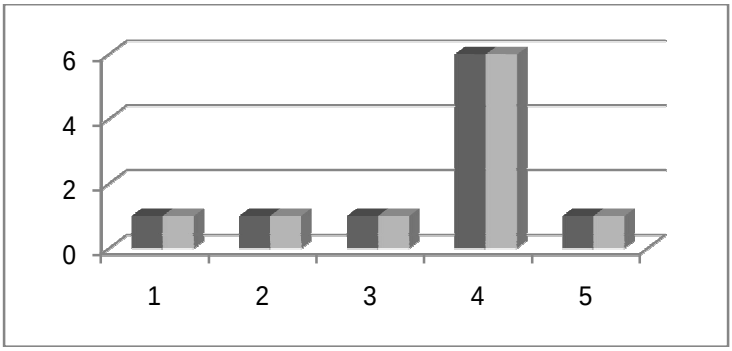

Fig 1

Figure of original file size and encrypted file size

- Black line indicates the file size in bytes.
- Grey line indicates the encrypted file size in byte.

In this fig-1 we compare the original file size with the encrypted file size which is remain same after encryption.

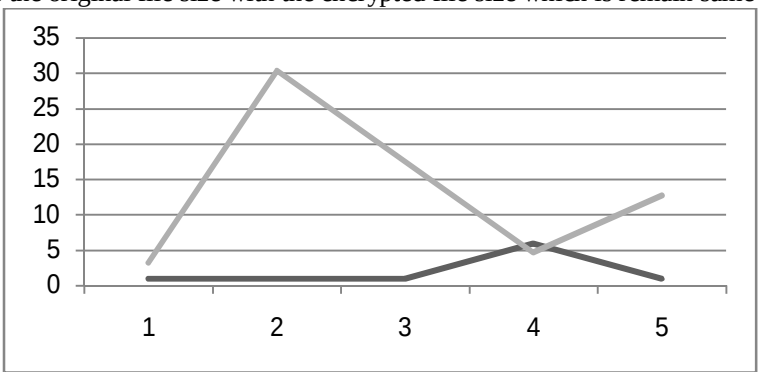

Fig 2

Figure of original file size and encryption time/ byte

- Blue line indicates the file size in byte.
- Red line indicates the encryption time /byte.

In this fig-2 we compare the original file size with the encryption time /byte.
In Table 2 we show the decryption time with decrypted file size.

Table 2
Decryption time with Decrypted file size

FileName	FileSize(in KB)	Decrypted File Size(in Kb)	Decryption Time(in sec)	Decryption Time/ Byte
Msg b.txt	1	1	3.07692308	3.07692308
Msg d.txt	1	1	9.39560440	9.39560440
Msg f.txt	1	1	7.63736264	7.63736264
Msg h.txt	6	6	8.34780380	1.391300633
Msg j.txt	1	1	18.68131868	18.68131868

Now from the above table-2 it is visible that file size is remain same and we get the original file size after decryption. The graphical representations associated with the table 2 are shown below.

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

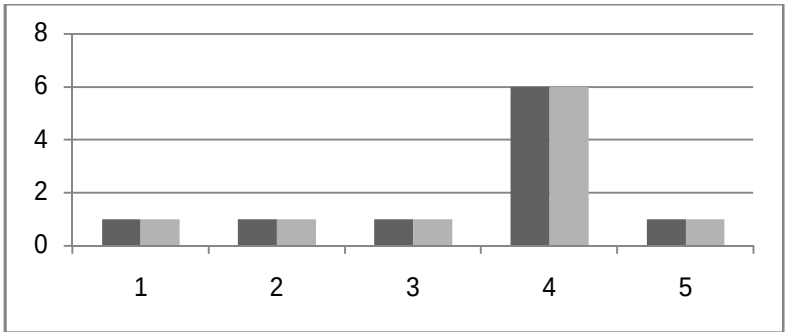

Fig 3

Encrypted file size and Decrypted File Size Comparative Table of decryption

- Black line indicates the file size in byte.
- Grey line indicates the decrypted file size in byte.

In this fig-3 we compare the encrypted file size with the decrypted file size which is remain same after decryption.

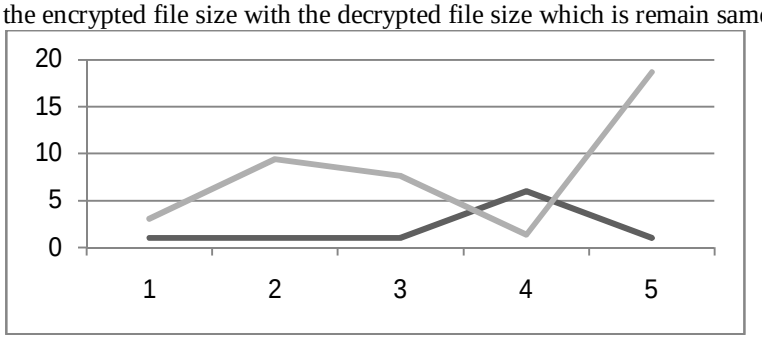

Fig 4

Encrypted file size and Decryption Time/byte Comparative Table of decryption

- Blue line indicates the file size in byte.
- Red line indicates the decryption time/byte.

In this fig-4 we compare the encrypted file size with the decryption time/byte which is remain same after decryption.
So from the result it is clear that after encryption the encrypted file size can be increases or remain same. It is practically impossible to understand in which case the encrypted file size will increase or remain same before the encryption process starts.

VI. CONCLUSION

In this algorithm encryption and decryption are performed on binary bits. 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 textencryption, image encryption i.e., multimedia encryption process. The length of the plain text is not restricted in this algorithm, so it can be applicable for any larger file. Random number can be any number. The random number (which is the block size) kept in key and use of thisrandom number will help several operations related to the technique. Here block size which is the key, can be any number. But for bigger block size more security will be achievable. The encrypted file size is equal after encryption. It is practically impossible to understand whetherthe encrypted file size will increase before the encryption process starts. So these are the main advantages of the algorithm. In this algorithm basically depending upon the key the matrix is created and whole process is done. Whole process is impossible except the 2^{nd} segment of key. After that as per the algorithm all represented values are converted to its binary form. These calculations are responsible for the encrypted file. Here we implemented a new technique for secure message transmission which gives us more security. In future we also try our best to develop more complex technique for better security.

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

REFERENCES

[1] A. Kahate,"Cryptography and Network Security", (2nd ed.). New Delhi: Tata McGraw Hill, 2008.
[2] Zirra Peter Buba, Gregory MakshaWajiga– "Cryptographic Algorithms for Secure Data Communication" ,International Journal of Computer Science and Security, Vol. 5, Issue 2, 2011.
[3] Prof. (Dr.) Pranam Paul, SaurabhDutta, A.K.Bhattacharjee, "Enhancement of Security through an Efficient Substitution based Block Cipher of Bit-level Implementation with Possible Lossless Compression", International Journal of Computer Science and Network Security, Vol. 8, No. 4, April 2008.
[4] Tamisrakundu, Sananda Bhattacharyya, Prof. (Dr.) PranamPaul,"Block Based Cryptographic Protocol Depending on G.C.D. for Secured Transmission", International Journal of Computational Intelligence and Information Security, Vol. 3 No. 3, 2012.
[5] Prof. (Dr.) PranamPaul,"An Application to ensure Security through Bit-level Encryption", International Journal of Computer Science and Network Security, Vol. 9, No. 11, 2009.
[6] Prof. (Dr.) PranamPaul,"Implementation of Information Security based on Common Division", International Journal of Computer Science and Network Security, Vol.11, No. 2, 2011.
[7] John C. Bowman,"Math 422 Coding Theory & Cryptography", University of Alberta, Edmonton, Canada.
[8] Pranam Paul, SaurabhDutta,"An Enhancement of Information Security Using Substitution of Bits Through Prime Detection in Blocks", Proceedings of National Conference on Recent Trends in Information Systems (ReTIS-06), Organized by
IEEE Gold Affinity Group, IEEE Calcutta Section, Computer Science & Engineering Dept., CMATER & SRUVM Project- Jadavpur Univ. and Computer Jagat. July 14-15, 2006.
[9] Koblitz, N.,"A Course in Number Theory and Cryptography, 2nd ed. New York: Springer-Verlag, 1994.
[10] A. Menezes, P. Van Oorschot, S. Vanstone,"Handbook of Applied Cryptography", CRC Press, 1996.
[11] Mark Adler, Jean-Loup Gailly,"An Introduction to Cryptography", released June 8, 2004. [Online] Available: http://www.pgp.com.
[12] PrakashKuppuswamy, Dr. C.Chandrasekar, "ENRICHMENT OF SECURITY THROUGH CRYPTOGRAPHIC PUBLIC KEY ALGORITHM BASED ON BLOCK CIPHER" Indian Journal of Computer Science and Engineering, Vol. 2, No. 3 2011.
[13] Newton's forward Method for initial idea
[14]AyanBanrjee, Prof. Dr.Pranam Paul, "Bock Based Encryption and Decryption", International journal of Computer Science andNetwork Security, ISSN: 0974 – 9616 vol-7,No.2,2015.
[15]Shibaranjan Bhattacharyya, Prof. Dr.Pranam Paul, "An Approach to Block Ciphering using Root of Perfect Square Number", International journal of Computer Science andNetworkSecurity,ISSN: 0974 – 9616 vol-7,No.2,2015.
[16] Swaping the rows and columns of a matrix is the initial idea.
[17] SukanyaChakravarty,ProfDrPranam Paul," Finding the difference between consecutive numbers",International Journal of Inovative Research is Computer and Communication Engineering,ISSN(Online): 2320-9801,Vol-4 Issue-2 2016.
[18]Anupam Mondal,,Prof DrPranam Paul," Returning Back its Own Nest of a Bird",International Journal of Inovative Research is Computer and Communication Engineering,ISSN(Online): 2320-9801,Vol-4 Issue-2 2016.
[19]Subir Sharma,,Prof DrPranam Paul," Block Based Ciphering Using Bit Wise Calculation for Representing of a Number Using Its Corresponding Perfect Square Number and Position of Prime Number",International Journal of Inovative Research is Computer and Communication Engineering,ISSN(Online): 2320-9801,Vol-4 Issue-2 2016.

BIOGRAPHY

Sukanya Chakravarty she is a student of MCA, NarulaInstitue of Technology under WBUT. She is a former student of Calcutta University. She is interested to work on information security.

DrPranam 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. Parallely, At the same time, he continued his research work. At October, 2006, National Institute of Technology (NIT),Drgapur 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 Ph.D. from National Institute of Technology, Durgapur, 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. Parallely he continue his research work. For that, he have 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.**