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 2, February 2016

Approach Based on Finding the Difference between Consecutive Numbers

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 base on consecutive difference between two numbers. 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.

KEY WORDS: 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 unauthorised access (middle attack), protected from unauthorised change, and available only to the sender and receiver. Cryptography, not only protects data from hacking or alteration, but can also be used for user authentication. 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 II the algorithm is described. Section III describes the whole process with an example. In section IV a test report is done executing the technique on some real files. An analysis has been done in section V along 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 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.

DOI: 10.15680/IJIRCCE.2016. 0402086

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	Segment	Description
1	Random number (Block Size)	3	The number of dummy bit.
2	Number of Block	4	A random number is generated using 1,2,3,4

2. ALGORITHM OF ENCRYPTION:-

STEP 1- At first we need to convert the plain text into its binary form thus creating a bit stream.
For example, after conversion of plain text, binary bit stream is assumed as 011000010.

STEP 2- A Block Size 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.
Here suppose the Block Size is 3. calculating the decimal value of the binary bit stream depending upon the Block size we get 3 0 2.

STEP 3- Now from the obtained decimal values, how many decimal values is to be selected for further operation is stored in the 2nd segment of the key i.e. number of blocks.
Suppose the Number of Block is 3.
3 0 2

STEP 4 - At the beginning of the binary bit stream we will first append the dummy bits and the information about the number of dummy bits is present in the 3rd segment of the key. From now onward encrypted bit stream will be as it is.

STEP 5- The decimal values depending on the Key Size will be placed on the 1st column of a matrix. For example

3
0
2

STEP 6- Now considering this column row wise, the 1st value of the column that is the 1st row of the column is subtracted from the 2nd row value that is the 2nd value of the column and the subtracted result is stored in 2nd column of the matrix, this process is repeated until we get a single value in a column .This process will repeat till all the decimal numbers are operated as per STEP 5. For example

3	-3	5
0	2	
2		

STEP 7- Convert the decimal values of the matrix into its binary form .If the decimal number in the matrix is –ve then put 1 before the converted binary form and the rest of the binary value stored in the form (Block size +2) bits .If the decimal number is +ve then put 0 before the converted binary form from the represented value. This process would repeat until all the decimal values are converted into its binary form.

STEP 8- Now store the value of 1st row in the sequence a[0][0] to a[0][n] named as 1 and in the sequence a[0][n] to a[0][0] named as 2. The diagonal value in the sequence a[0][n] to a[n][0] named as 3 and in the sequence a[n][0] to a[0][n] named as 4.
For example for sequence 4 2→ 00010 2→00010 5→00101 this is the output.

STEP 9- A random no. is generated with the numbers 1,2,3,4 like 4321 or 1432 etc. This is the 4th segment of the key. Each set of decimal numbers that we got as per the key size is stored in matrix and for each set of numbers a single matrix is created as per our earlier steps. Now using these random set numbers that we select in our key the that has some functions as mentioned earlier, on the1st matrix the operation as per the first number is performed, on the 2nd matrix operation as per the 2nd number is performed and this process repeats for all the matrix, If the random number has 4 numbers and we have 6 matrix then from the 5th matrix the random numbers would repeat from the beginning for rest of the matrix.
Suppose here 4 as a random number is generated. So we get 2→ 00010 2→00010 5→00101

STEP 10 – After completing STEP 9 we got a binary bit stream which is converted into its ASCII form. This is the encrypted form of the plain text.

For example the final binary bit stream we get is 000100001000101. The ASCII form of this binary bit stream is the encrypted value of the plain text.

3. ALGORITHM OF DECRYPTION:-

STEP 1-Convert the encrypted form into its binary form.

For example 000100001000101 this binary bit stream we get from the encrypted file.

STEP 2- As per the 3rd segment of key we subtract the number of dummy bit from the total number of binary bit stream and continue the further decryption process depending on the resultant binary stream.

STEP 3- Considering Block Size + 2 we take binary values and check whether the 1st bit is 0 or1.If the 1st bit is 0 then it is a +ve number else the number is –ve number and rest of the binary value is converted into its decimal form.

STEP 4 -Now as per the 2nd segment of the key, the Number of Block we take n number values (say no. Of block size =n) and place it in the 1st row from left to right for the random number 1, right to left for the random number 2 and place it diagonally in a matrix from right to left downward for the random number 3 and left to right upward for the random number 4.

Suppose here 4 as a random number is generated. Here the Number of Block is 3.

5
2
2

STEP 5 –Now if 1 or 2 is generated as random number then the value of a[0][0] is added with a[0][1] and the resultant value is stored in a[1][0].For 1 and 2 using the above process the whole matrix is created. Now if 3 or 4 is generated as random number then the value of a[n-1][1] is subtracted from the value a[n][0] and the resultant value is stored in a[n-1][0] . For 3 and 4 by applying this process on every block we get the whole matrix. For example

3 -3 5
0 2
2

STEP 6 –Thus STEP 4 and STEP 5 is repeated for the rest of the decimal numbers. Thus the other matrix is created in the same way.

STEP 7- After getting the all values of the matrix takes the values of the 1st column. For example 3 0 2.

STEP 8-Convert the decimal values into its binary form. Entire decrypted binary stream is converted into the normal file according to the ASCII value.

III. EXAMPLE

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

1. Key Structure

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

Segment	Description	Value of the segment	Segment	Description	Value of the segment
1	Block Size	4	3	No. of Dummy bit	0
2	No. of Block	4	4	Random number	4

2. EXAMPLE OF ENCRYPTION :-

e –> 101 → 01100101
n → 110 → 01101110
c → 99 → 01100011
r → 114 → 01110010
y →121 → 01111001
p → 112 →01110000
t → 116 → 01110100

Block Size= 4

Separate this binary values depending upon the Block Size.

0110 0101 0110 1110 0110 0011 0111 0010 0111 1001 0111 0000 0111 0100

Convert the 4digit binary values into its decimal form.

6 5 6 14 6 3 7 2 7 9 7 0 7 4

As Number of Block = 4, Now take 1st four values depending upon the Number of Block and calculate the subtracted result of the consecutive decimal value and then repeat the process for the rest of the decimal numbers.
Here the example that we have shown is done by taking 4 as random number. And the operation that 4 indicate is stated in step7 on encryption algorithm. And the 4th segment of the key holds this information that which method is selected by the sender.

6

-1

5 2

1 5

6 7

8

14

In the next step following the step 7 we get,

000100

100001

000101 000010

000001 000101

000110 000111

001000

001110

Now for next 4 decimal numbers depending upon the Number of Block the same process is done and this process will be continued for all the blocks. As the random number is chosen as 4, which is the diagonal value from left to right upward. So finally we get this:-

001110 001000 000111 000101 000010 000101 001001 010000 000000 000111 000101 000001 001010 001010 001110 011111

8 Å

Zpya(£

This is the encrypted form of the plain

3. EXAMPLE OF DECRYPTION:-

The encrypted form is

8 Å

Zpya(£

Converting the ASCII value into its binary form we get

001110 001000 000111 000101 000010 000101 001001 010000 000000 000111 000101 000001 001010 001010 001110 011111

Then we check the 1st bit is 0 or 1. If 1 then it is a -ve number else +ve number. And the rest of the bits are converted into its decimal form. Applying this process we get

14 8 7 5 2 -5 -9 -16 0 -7 -5 -1 10 10 14 15

Considering the Number of Blocks we take 1st 4 values and place it diagonally from left to right and applying the operations to get the rest of the matrix values then again take next 4 values and the process will go on.

5

7

8

14

From this value we get the whole matrix.

6

-1

5 2

1 5

6 7

8

14

Applying this process on the next 4 decimal values and continues this process at the and at the end we get,
6 5 6 14 6 3 7 2 7 9 7 0 7 4 0 10. Then Convert the decimal values into its binary form. Entire decrypted binary stream is converted into the normal file according to the ASCII value which is the plain text “encrypt”.

IV. 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 2 bellow. 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

File Name	File Size (in byte)	Encrypted File Size (in byte)	Encryption Time(in sec)	Encryption Time/ Byte
Msg a.txt	7	12	0.00000000	0.00000000
Msg b.txt	12	16	0.00000000	0.00000000
Msg c.txt	21	29	0.05494505	0.0025997383
Msg d.txt	13	16	0.00000000	0.00000000
Msg e.txt	10	16	0.32967033	

Now from the above table it is visible that
for the file c.txt file size is 21 bytes,
the result of encrypted file size is increased. The encrypted file size is 29 bytes.
Four graphical representations associated
with the table 1 are shown below.

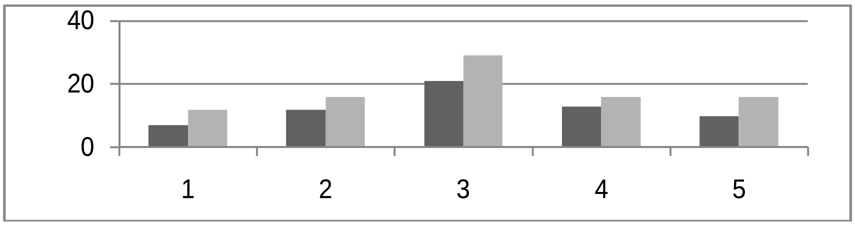

Fig 1
Figure of original file size and encrypted file size

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

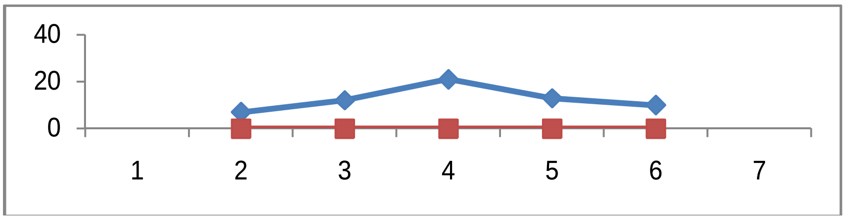

Fig 2
Figure of original file size and encryption time/ byte

DOI: 10.15680/IJIRCCE.2016. 0402086

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 2, February 2016

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

In table 5.2 we show the decryption time with decrypted file size

TABLE – 2
Size and Time Comparative Table of decryption

File Name	File Size (in byte)	Decrypted File Size (in byte)	Decryption Time (in sec)	Decryption Time/ Byte
Msg j.txt	12	7	0.00000000	0.00000000
Msg z.txt	16	12	0.00000000	0.00000000
Msg y.txt	29	21	0.00000000	0.00000000
Msg x.txt	16	13	0.00000000	0.00000000
Msg w.txt	16	10	0.32887055	0.205544093

Now from the above table it is visible that for the file w.txt file size is 16 bytes, the result of encrypted file size is reduced. The decrypted file size is 10 bytes. Four graphical representations associated with the table 2 are shown below.

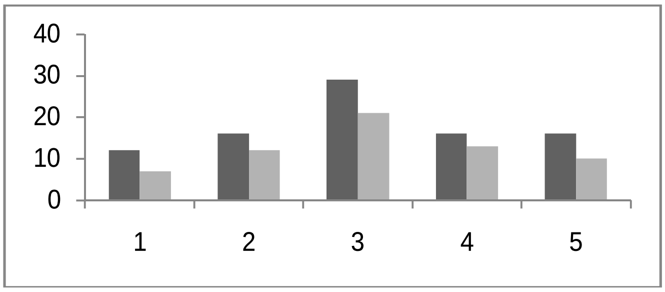

Fig 3
Figure of original file size and decrypted file size

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

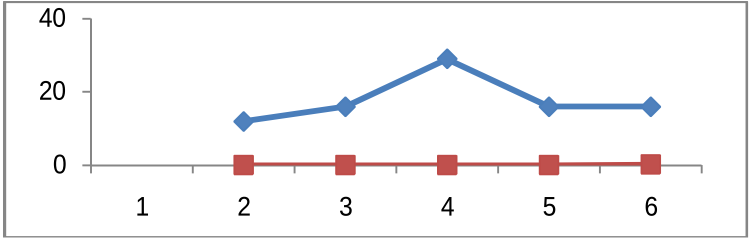

Fig 4
Encrypted file size and Time/byte Comparative Table of decryption

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

So from the result it is clear that after encryption the encrypted file size can be increases. It is practically impossible to understand in which case the encrypted file size will increase or remain same before the encryption process starts.

V. 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 for encryption process. Therefore that encryption technique can be used for text encryption, 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 of any number. The random number (which is the block size) kept in key and use of this random number will perform 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 achieved. The encrypted file size increases after encryption in some cases. It is practically impossible to understand whether the encrypted file size will increase or not, before the encryption process starts. So these are the main advantages of the algorithm. In this algorithm we first calculate the difference between two consecutive numbers using a technique which is described in the algorithm section and using this technique a matrix is created. Here we implemented a new technique for secure message transmission which may give us more security. In future we also try our best to develop more complex technique for better security and to reduce the file size eventually.

REFERENCES

[1] A. Kahate,"Cryptography and Network Security", (2nd ed.). New Delhi: Tata McGraw Hill, 2008.
[2] Zirra Peter Buba, Gregory Maksha Wajiga– “Cryptographic Algorithms for Secure Data Communication” ,International Journal of Computer Science and Security, Vol. 5, Issue 2, 2011.
[3] Prof. (Dr.) Pranam Paul, Saurabh Dutta, 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] Tamisra kundu, Sananda Bhattacharyya, Prof. (Dr.) Pranam Paul,“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.) Pranam Paul,“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.) Pranam Paul,“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, Saurabh Dutta,“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] Prakash Kuppuswamy, 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]Ayan Banrjee, 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 andNetwork Security,ISSN: 0974 – 9616 vol-7,No.2,2015.

BIOGRAPHY

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

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. 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.

DOI: 10.15680/IJIRCCE.2016. 0402086