www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 11906-11909

Various Bit-Rotation Technique On Key-Symmetric Matrix

Mampa Ghosh[1], Debjani Chakraborty[2]

[1] M.Tech (Scholar) of Narula Institute Of Technology, WBUT,
81,Nilgung Road, Agarpara, Kolkata-700109
ghoshmampa1315@gmail.com

[2] Asst.Professor of Narula Institute Of Technology, WBUT,
81,Nilgung Road, Agarpara, Kolkata-700109
debjani.cse@gmail.com

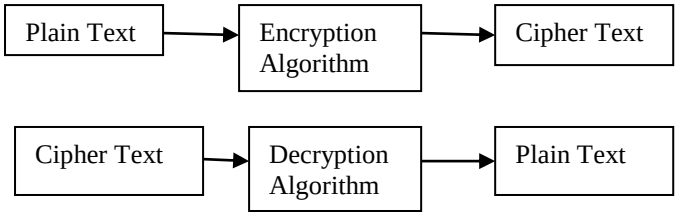
Abstract: Cryptography is one type of very much challenging methods in today's technological world for hiding the secret information. Security is the main purpose of the Cryptography. Actually, the main aim of the Cryptography is protecting the data or informations from unauthorized users or hackers. In cryptography, it has two parts: one is Encryption Algorithm and another one is Decryption Algorithm. In this paper, we have proposed a new Encryption Algorithm to encrypt the plain Text to Cipher Text and the Decryption Algorithm to do the reverse. Here we applied various bit-rotation techniques with complement, shifting and transposing on key-symmetric matrix. These operations are simple and easily to implement.

Keywords: Information hiding, Security, Encryption, Decryption, Key-Symmetric matrix.

1. Introduction

Cryptography comes from the Greek words "Crypto" means "Secret" or "Hidden" and "Graphein" means "Writing". Cryptography is a study of techniques for secure communication.

Thousand of years ago, the concept of Cryptography begins, it changes the format of Plain Text into a Cipher text which is encrypted version of the original Text and it is unrecognizable and also useless to unauthorized party. It is only recognized in between the sender and the intended recipient.



Cryptography is considered not only part of the branch of mathematics but also branch of computer science[1].

There are two basic types of Cryptography: Symmetric Key Cryptography and Asymmetric Key Cryptography. In Symmetric Key Cryptography it uses same key for both Encryption and Decryption. In Asymmetric Key Cryptography, it uses different keys Private key and public key. Another category of Cryptography which is Hash function, this is one-way function and no key is required[2].

The issues of Cryptography: 1) Confidentiality: sender and intended recipient only understand the secret information-sender encrypts the information and recipient decrypts this.

2) End-Point Authentication: in this method, sender and receiver confirm their identity of each other.

3) Message Integrity: sender, receiver want to ensure information not altered without detection.

4) Non- Repudiation: The final order is accepted.

5) Access Control: prevent misuse of resources.

6) Availability: It is permanent,not erasure.[3].

Cryptology embraces both Cryptography and Cryptanalysis. Cryptography is the art and science of using mathematics to encrypt and decrypt data. Cryptanalysis is the science of analyzing and breaking secure communication. Classical Cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination and luck. Cryptanalysts are also called attackers.

The main purpose of the Cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation.

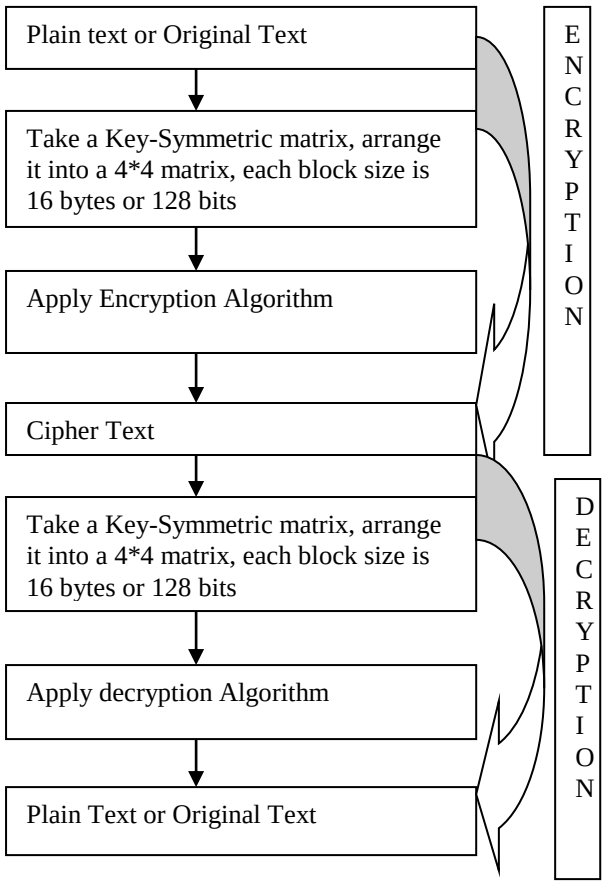
The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If anyone is protecting confidential information then cryptography provides high level of privacy of individuals and groups.

Limitation of Cryptography is that the third party is always aware of the communication because of the unintelligeible nature of the text. To overcome this problem we can also implement Steganography.

In this paper, we have proposed a new method which is Key-Symmetric block cipher algorithm. Here we have used 4*4 matrix. Each block size is 16 bytes or 128 bits. Various Bit-Rotation techniques are applied with shifting, complement (one's and two's) and transposing processes and we also analysis the algorithm. In this paper, we have also applied

ASCII values of the corresponding characters. Here we are generating the private key using a method and we also applied here bit-xor method. Since, it is Symmetric Key Encryption and Decryption method, so we applied here same key operation for both.

2. Flowchart of Encryption and Decryption Method:



3. Algorithm for Encryption with Equations

1) First, we take an Original Text or Plain Text "I SHALL GO TO SCHOOL". This text will arrange into a 4*4 matrix, each block size is 16 bytes or 128 bits.

2) Then we will find the corresponding ASCII value of these characters using the equation:De=uint8(Ce); (1)

3) Bit-wise complement(2's) method will be applied on the above resultant matrix by:

   Ee=bitcmp(resultant matrix of step 2); (2)

4) Now, we draw a matrix which contains odd number of random values, the range of the values is in between 0 to 255. After taking it, we have applied modulus method with 2 and we get a new matrix which contains all 1 value. He=mod(random number,2); (3)

5) Bit-wise XOR method has applied between step 3 resultant matrix and step 4 resultant matrix and we will get a new resultant matrix using this:

   Ie=bitxor(resultant matrix of step 3,resultant matrix step 4); (4)

6) Transpose the above matrix. Je=(Ie)'; (5)

7) After that we have rotated the step 6 matrix in 90 degree position using 'rot90' function.

8) 'fi' function is applied here:fi(value,bit-wise rotation by right shift,word length,fraction length); (6)
   from this method, we get the binary value and we apply 'bin2dec' method to convert the binary value to decimal value.

9) Circularshift method is applied on above matrix.

10) Thus we get the Cipher Text or Encrypted information.

Key generation

1) After getting the resultant matrix of circularshift method, suppose, this matrix is denoted by 'b'.

2) 'a', new matrix is taken. Now we can write a=b;// 'a' matrix contains the value of 'b' matrix.

3) 'ned', this new matrix contains the value of private key. ned=a %10;// from here we take the remainder and store it 'ned' matrix.

4) After that, we will do the 'minus' operation between 'a' matrix and 'ned' matrix and also store the value into 'a' matrix. a= a- ned;

Algorithm for Decryption

The reverse process of Encryption Algorithm is applied.

1) We take an encrypted version or Cipher Text and put it into a 4*4 matrix, each block size is 16 bytes or 128 bits. Then we apply the 'uint8' method on the character of the matrix and we will get the corresponding ASCII value.

2) Circularshift method is used on the matrix which is getting from step 1.

3) 'fi' function is used:fi(value,bit-wise rotation by left shift,word length,fraction length); from this we will get the binary value and same way, we will convert the values from binary to decimal using 'bin2dec' method.

4) 'rot90' function is applied on the above getting matrix and then apply the transpose method and we will get the new resultant matrix.

5) Now, we take odd numbers of random values and put those into a 4*4 matrix. The range of the values between 0 to 255. Same way, we apply modulus operation on those value and we get the resultant matrix which contains value 1.

6) Bit-wise XOR method is applied between step 4 resultant matrix and step 5 resultant matrix.

7) Bit-wise complement (2's) method is applied on the above matrix.

   Thus, we will get back the Original or Plain text.

4. Result

From Encryption Algorithm, we take an Original Text:

Be=('I SHALL GO TO SCHOOL');

Then we arrange all the characters of this text into a $*4 matrix:

Ce=

I	S	H	A
L	L	G	O
T	O	S	C
H	O	O	L

Using equation (1). We get the corresponding ASCII value:

De=

73	83	72	65
76	76	71	79
84	79	83	67
72	79	79	76

From equation (2)..

Ee=

183	173	184	191
180	180	185	177
172	170	173	189
184	170	177	180

Now we draw a 4*4 matrix which contains odd number of random values:

Ge=

99	101	131	93
193	85	235	35
67	89	199	97
77	177	7	79

Using equation (3)..

He=

1	1	1	1
1	1	1	1
1	1	1	1
1	1	1	1

From equation(4)..

Ie=

182	172	185	190
181	181	184	176
173	176	172	188
185	176	176	181

Transpose the matrix by equation (5)..

Je=

182	181	173	185
172	181	176	176
185	184	172	176
190	176	188	181

After operating step 7 we get this new matrix:

Le=

11011010	01011110	01011000	01011111
01011000	01010110	01011100	11011100
01011000	01011000	11011010	01010110
11011100	11010110	11011010	01011011

Using 'bin2dec' method, we get..

Me=

218	94	88	95
88	86	92	220
88	88	218	86
220	214	218	91

From step 9, we get..

Ne=

220	214	218	91
218	94	88	95
88	86	92	220
88	88	218	86

Then we apply Key generation method and we will get the new resultant matrix:

Oe=

220	210	210	90
210	90	80	90
80	80	90	220
80	80	210	80

At last, we will get the Cipher block..

Pe=

Ü	Ò	Ò	Z
Ò	Z	P	Z
P	P	Z	Ü
P	P	Ò	P

Corresponding Cipher text is:

Qe=(' Ü ÒÒZÒZ PZ PP ZÜPPÒP');

5. Conclusion

From the above result its clear that our "Proposed technique" is better than other Cryptographic algorithm for hiding the datas.Here we have applied different types of bit rotation with shifting, complement, XORing, transposing methods and also have taken a key symmetric matrix with block size 128 bits or 16 bytes.This algorithm is very simple, efficient and easy to implement.

The future work should be focused on the application of this method is applicable in key symmetric matrix but some how this method may not be applicable in key asymmetric matrix.

6. Acknowledgment

I am giving thanks to all of the CSE faculties at Narula Institute Of Technology.Last but not the least I am giving thanks to my college Narula Institute Of Technology for giving me the opportunity to present this project.

References

[1] Sunita Bhati, Anita Bhati and S. K. Sharma, "A New Approach towards Encryption Schemes: Byte-Rotation Encryption Algorithm", proceedings of the World Congress on Engineering and Computer Science 2012 Vol II, October 24-26, 2012, San Francisco, USA.

[2] Ayushi, "A Symmetric Key Cryptographic Algorithm", proceedings of 2010 International Journal of Computer Applications (0975-8887) Volume 1-No.15.

[3] Vishwa Gupta, Gajendra Singh and Ravindra Gupta, "A Hyper Modern cryptography Algorithm to Improved Data Security: HMCA", proceedings of the International Journal of Computer Science & Communication Networks, Vol 1(3), 258-263, ISSN: 2249-5789.

[4] Suyash Verma, Rajnish Choubey and Roopali Soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security", proceedings of the International journal of Emerging technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 7, July 2012.

[5] Sudhakar Kumar Singh, "Design and Implementation of Cipher Algorithm using Randomized Alphanumeric characters", proceedings of the International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012, ISSN 2250-3153.

[6] Dr. Dilbag Singh, Pooja Rani and Dr. Rajesh Kumar, "To design a Genetic Algorithm for Cryptography to Enhance the Security", proceedings of the International Journal of Innovations in Engineering and Technology, Vol.2, Issue 2, April 2013, ISSN: 2319-1058.

[7] Anju, Babita, Reena an Ayushi Agarwal, "An Approach to Improve the Data Security using Encryption and Decryption Technique", proceeding of the International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 3(2013), pp. 125-130 © International Research Publications House.

[8] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[9] P. Gutmann, ―Cryptographic Security Architecture: Design and Verification‖. Springer-Verlag,2004.

Author Profile

Mampa Ghosh, M.Tech in Computer Science and Engineering at Narula Institute of Technology, Agarpara, Kol-700109, under West Bengal University Of Technology. Now I am persuaing in M.Tech. I have interest on Network Security basically Cryptography and Steganography. I want to further study and research on these subject.

Debjani Chakraborty,Asst. Professor of Narula Institute of Technology.Agarpara., Kol-700109, under West Bengal University Of Technology .M-Tech in computer Science and Engineering from Netaji Subhash Engineering College,Garia.