An Integrated Cryptography Approach Using Msa Symmetric Key

Thanapal P
Assistant Professor (Senior)
VIT University, India

Muthamil Selvan T
Assistant Professor (Senior)
VIT University, India

Pratheeba T
Assistant Professor
Kanchi Pallavan Engineering College, India

Abstract

*The piracy protection of any software is a very big problem. We are in the situation of creating a new technique to overcome the problem. The symmetric key encryption is very much suitable for this environment. So we have to create a very robust symmetric key cryptography system which is helpful for safeguard licensee software. Hence Symmetric key cryptography plays important role. From long past there is lot of research works carried out for the improvement of symmetric key cryptography. The current work treats with the symmetric key method for multiple encryption and decryption of files. In this paper we will extend DJSSA algorithm (1) which is extended from the very familiar algorithm MSA. The current work uses a randomized key of size 16777216*256 which contains all possible 4 lettered words. In our proposed method the difficulty of finding actual key matrix is 4294967296! Trials which is not possible to break by any brute force method. The current method will be best for encryption of small size file. For encryption of big size files we have to divide the file into reasonable numbers and then execute our encryption code parallel in another system and after we have to combine those file to obtain final encrypted file*.

1. Introduction

In cryptography for encryption and decryption of data we use many algorithms. These algorithms are divided in two major category-symmetric and asymmetric key algorithms. In asymmetric key algorithm there are two keys are used for encryption and decryption .one key is used for encrypt the data and other key is used for reverse the encryption that is to decrypt the data but in this asymmetric key technique there are some difficulties occurred such as – sometimes computing the encrypted information from simple text takes much time so power consumption is more, difficulty to remember the different- different keys for encryption and decryption. in asymmetric key another problem is we have to make private key secrete . In asymmetric algorithm if the key size is long enough then the best known attack algorithm take so much time to break the code. Symmetric key method is simple because in this we have to maintain only one key. In symmetric key algorithm same key is used for encryption and decryption of data. In symmetric algorithm there are different methods such as- playfair method, DES method are popular. The problem in symmetric key approach is that key must be confidentially distributed. For security improvement there are many algorithms developed but main problem is that, now today it is not difficult for intruders to find the original key. so for securing the key we use multiple encryption and decryption. Using this approach we increased the difficulty for finding the actual key.

2. Related works:

Meheboob Alam Mallick, Saima Ghosh and Asoke Nath et ele.[1] says this cryptography method , for generating the symmetric key matrix which are randomly choose to encrypt data and decrypt the cipher data .In this approach encrypt the plain text multiple times . This procedure takes the key given by user , the key length must be less than or equal to sixteen character long . so the number of total matrices are 16*16 is !256. Which are difficult to break.

Asoke Nath, Dripto Chatterjee and Joyshree Nath et al.[2] says For generating the original key matrix ,we take secret key from user and the size of key matrix with 256*256 and in this we store two character in each cell . So the difficulty of finding the real key is 65536! Samples in this. Now today it's not impossible to give the 65536! Trial .In this method also used several times encryption for securing the data .In this randomization is performed by using the method proposed in Nath et.al.[1].the length of the text key entered by the user should be less than or equal to 16 characters long.

Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath et al. [3] says Proposed method is use the new randomization method for create randomized key matrix to the encrypt the several times any kind of data and to decrypt the cipher data. This method is fully dependent on the text key given by user. It may be include the any character (ASCII value 0 to 255). In this randomized and encrypted number will be computed from the text key which is given by the user. In this method size of key matrix will be 65536*256 that enclose three letter terms and randomization procedure is used to construct arbitrary key matrix. The difficulty of finding the real key matrix is !1677726 trails that is very difficult for the intruders.

Packirisamy Murali and Gandhidoss Senthilkumar et. al.[4] says In this playfair cipher depends on poly-alphabetic cipher. Playfair arrange the plain text in table based on key value .This paper tries to improve playfair cipher using linear feedback shift register .In this for mapping random numbers to secret key of playfair cipher ,related numbers will be sent to receiver in the place of alphabetical letter .This approach quickly increases the security of transmission over an unsecured channel. A LFSR is a shift register in which input state is a linear function of its previous state. This method is based on key stream value only.

Asoke Nath, Sankar Das, Amlan Chakrabarti and A.K.Chaudhuri et.al[5] says a new method to hide any encrypted message inside a cover file. The new randomization method is used to generate a randomized key matrix to encrypt a plain text file and to decrypt a cipher text file. A new algorithm has also been introduced to encrypt the file multiple number of times. Randomization numbers and encryption numbers are calculated using this algorithm from the given text key. A password mechanism is also introduced for hiding the data in the cover file. Here we propose that our new method could be most appropriate for hiding any kind of file in any standard cover files such as image, audio, video files.

A.K.Chaudhuri, Asoke Nath et.al [6] says Steganography is a Greek word. Steganography is a special method. It is used for writing secret message. It includes the embedding of digital information within computer file. Now we are try to include the embed sound file in image file , text file within a word file excel file or within a pdf file and embed any file into another cover file. The cover should be at least 10-20 bigger than the embedded file. This is only constraint that should be taken care of.

3. Comprehensive Approach

The piracy protection of any software task the decryption is not the critical problems but the breaking the key and copying the software is the very big problem. So our aim is to not to increase the speed, to give the robust technique for encryption and decryption. There should be a approach which can not be break by brute force method even for a long time. Existing MSA Algorithm for encryption and decryption of data used 16*16 random key. But in MSA algorithm if Brute force method is applied on this then only 256! Trial needed to find the original key and it is not impossible to give 256! Sample. To get the rid of these new algorithm DJSSA proposed and it increase the difficulty of finding the original key 256*256! Trial and in each cell it hold the two character. But it is also not difficult so the new scheme proposed which is extended algorithm of MSA named DJSSA. In this the difficulty of finding the original key matrix increased to 65536*256! Samples. It is difficult but not more difficult to break because now today it is possible to give 65536*256! Sample. For finding the original key, we want to such algorithm which is not possible to break the original key that is increased the more and more difficulty to finding the original key so we extended the MSA algorithm in which for finding the original key matrix difficulty is 16777256*256! Samples .so it is not possible to finding the original key**.**

For generating the random key of size (429496*4)! We give any text key which is confidential and size should be maximum 16 character can be any of 256 characters. In this method the character and position of the character is main point in the method for the finding the

randomization number and encrypted number. There is following process to apply to calculate the randomization number and encrypted number[1],[3]..
Choose the following table for calculating the place value and the power of characters of the incoming key

Key Length (n)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Base Value (b)	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2

User enters the PQ as text key. Here key length is two.
Step-1: Sum=Σ ASCII value * b^m ---(1)
m=1
So sum =80*16+81*16^2 = 1280+20736
sum= 22016
Now we try to find En and Rn
Where En = encrypted number and
Rn = randomization number
For calculation Rn---: we find the sum of product of each digit in sum and the place value
number1=2*1+2*2+0*3+1*4+6*5
=40
Rn=40-64
= 24
Now,
En=mod (sum, number1) =mod (22016, 40)
=16;
If, Rn=0, Rn=number1 and if Rn<64 then put Rn=Rn-64
For En, find the product of each digit in sum by its position in sum reverse order.
Number2=6*1+ 1*2+0*3+2*4+2*5=26
En=mod (sum, number2)
=mod (22016, 26) =20
if En=0, put E2=num2 and if En>64 then we put, En=En-64

In our method if we vary the text key slightly then the randomization number and the encryption number will changed. Now we show the procedure of making random key of size 16777216*256*4 . Generated random key is used for encrypting and decrypting the data. We store the random key in a file by following some steps. We partition the whole key in 16 blocks and in these blocks, every block hold 64*64 words and per word store 2 characters. These blocks are formed in the RAM and we do randomization method, one at a time on it and note down on external file in some arbitrary order. we want to make random key fully random so finding the pattern of encryption[5] is difficult. Following is the main key matrix which stores 1024x4 blocks per block of size 64x64x4 characters:

Block 1 (64*64*4)	Block 2 (64*64*4)	→	Block 1024(64*64*4)
Block 1025 (64*64*4)	Block1026 (64*64*4)	→	Block2048 (64*64*4)
Block 2049 (64*64*4)	Block2050 (64*64*4)	→	Block3072 (64*64*4)
Block 3073 (64*64*4)	**B**lock 3074 (64*64*4)	→	Block4096 (64*64*4)

Here we try to make each cell in array of size (64x64x4) where we hold 4 lettered words beginning from a word 0000 to word 255255255 255in random orders. To make the randomization more randon we may use some technique that is inter change of words. That is every first word with every fifth word of a page or reversing the letters of each word ect. Like this we can apply any type of technique to increase randomization.

These randomization works applied for Rn times and for making more random we alter the order of function.

4. Result

How our encryption method works shows on a sample text file. Here we are giving simple text file named sample.txt and the resultant encrypted file named sampleout.txt .for the decryption we apply decryption method on encrypted file.

Here for encryption we take the
Text key- pq
Randomization no- 8 times
Encryption no- 16

4.1 Input file (sample.txt)

I find a solace in the holy book that I miss even in the Sermon on the Mount. When disappointment stares me in the face and all alone I see not one ray of light, I go back to the holy book. I find a verse here and a verse there, and I immediately begin to smile in the midst of overwhelming tragedies--- and my life has been full of external tragedies--- and if they have left no visible, no indelible scar on me, I owe it all to the teaching of the holy book". Holy is universally acknowledged as one of the world's great scriptures

4.2 Resultant encrypted file (sampleOut.txt)

**♀╥>♀·Γ?ñ♀.%>m?%♀~>║?Γ♀>╧♀?╧╥|♀?>║║╘
█╥|>╧♀~>║?Γ♀>╧♀?╧╥|░?>║║╘╥█|>╧???Γ╧╥
║?%♀┘|
.|%?╧?Γ♀?>!!|┬┬|>╧Γ║♀█║?ñΓΓ█♀■╘!?║♀'|%
%♀·Γ?ñ♀?♀°♫░!Γ!mΓ║??.%>m?%♀╥?┬■♀~>║
?Γ♀╥>♀█
%?╧♀?♀■╧>'%?ñ.Γ♀!?╧?.!Γ╧╥♀┬·┬╥Γ!♀╥>♀█
║>!>╥Γ♀.%>m?%♀???╧ñ♀■ΓΓ█♀?♀?·Γ?■♀>╧
♀m%??■♀&
·Γ♀ñΓ?|┬|>╧♀╥>♀?┬┬|.╧♀╥·Γ♀║>%Γ♀>~♀·Γ?
ñ|╧.♀╥·Γ♀??╥?┬■♀~>║?Γ♀╥>♀╥·Γ♀█║>m|╥·♀'
?╥?·ñ
>.♀'?┬♀╥?■Γ╧♀║Γ?Γ╧╥%·♀m·♀|╧╥Γ║╧?╥|>╧?
%??╓┬┬>?|?╥|>╧♀>~♀╓╧╥|░?>║║╘█╥|>╧♀??╓
╘╥·>║|
╥|Γ┬♀?╧♀|╧ñΓ█ΓñΓ╧╥♀?╧╥|░?>║║╘█╥|>╧♀>
║.?╧|+?╥|>╧«♀♀??x**

5. Conclusion and Future work

From the result analysis we conclude that it will take much more time to decrypt if the file size is large. So that this technique is very suitable for encrypting software CDs. It increases the complexity of the key matrix to 4294967296! That is impractical to break the code by any one and find the actual key. Here we use greatest encryption time 64 and greatest number of randomization is 64. In this method if the size of the given file is too big and number of encryption is also big so it takes the more time this is the main weakness of this method. This method is more suitable for the sector where data privacy is more important than the time. In future we try to improve the speed of the approach and try to increase the complexity more.

6. References

1. A.Nath, S.Ghosh, M.A.Mallik, Symmetric key cryptography using random key generator, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-24
2. Dripto Chatterjee, Joyshree Nath, Suvodeep Dasgupta and Asoke Nath, A new Symmetric key Cryptography Algorithm using extended MSA method :DJSA symmetric key algorithm , communicated for publication at IEEE conference to held at Singapore from 14/06/2011 to 17/06/2011
3. Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm
4. P. Murali and Gandhidoss Senthilkumar, Modified Version of Playfair Cipher using Linear Feedback Shift Register, UCSNS International journal of Computer Science and Network Security, Vol-8 No.12, Dec 2008
5. A.Nath, S.Das, A.Chakrabarti, Data Hiding and Retrieval, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.
6. Cryptography and Network, William Stallings, Prentice Hall of India