INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

A NEW ENCRYPTION ALGORITHM TO INCREASE PERFORMANCE & SECURITY THROUGH BLOCK CIPHER TECHNIQUE

Neha Joshi*[1], Megha Singh*[2], Surabhi shah*[3]
CSE RGPV Bhopal

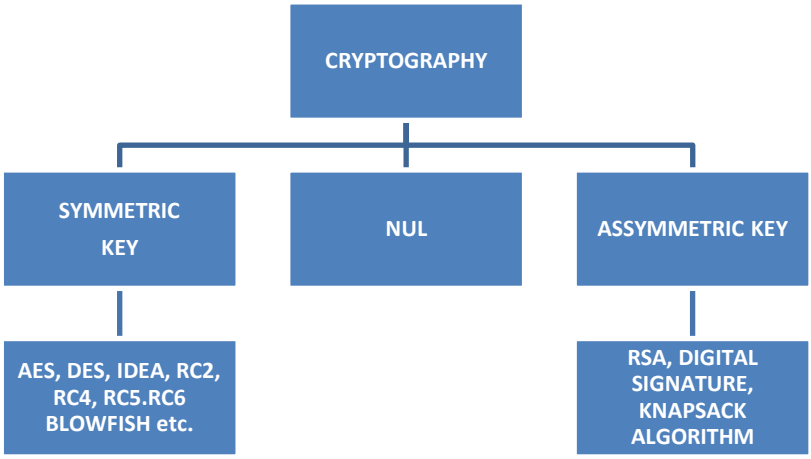
ABSTRACT

In this paper we represent a new approach for data encryption trough symmetric key based algorithm for data transmission in open network and also we represent a new design of Implementation of symmetric key encryption by which sender can easily communicate with receiver, the propose technique not on the restricted to purely making data unreadable but it also aims to provide user authentication and confidently ,which ensure the recipient that the encrypted message oriented, from a trusted source , in this propose technique we represent a new design approach for encrypting the file such as text file,.exe,binary ,audio, PDF ,2d and 3d images. This technique is not only implemented but it also compares its performance, efficiency, security and also it's complexity other presents existing block cipher algorithm of same categories.

[KEY WORDS]: - Data Security Block cipher, plain text, cipher text, text file, audio file, 3D-images]

I. INTRODUCTION

Cryptography is the technique for encrypt and decrypt data for securely transmits the information on the insecure network. The cryptography is divided into two categories Symmetric key and Asymmetric key. Symmetric key – Symmetric key is also called "secret key". Cryptography and it is the type of cryptography technique which we have to use single key or same key for encrypt and decrypt the data. This is very simple and very easy algorithm, but some drawback is present here like Unauthorized user intercepts the key and they could be. Decrypt the massage. DES- The word DES is representing to "Data Encryption Standard" and it is also known as "Data Encryption Algorithm". It is developed in 1997 by National Bureau of Standards (NBS), and now the NBS known as National institute of Standards and Technology (NIST). It is a block cipher algorithm that means it divides plaintext into fixed length block. It is encrypt the each data in 64bit size of blocks. These 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. In DES the plain text is 64bit and key size is 56 bit. Blowfish Algorithm – The blowfish is the technique of symmetric key algorithm in which we are use the common key for encryption and decryption the message. It was designed by Bruce Schneider in 1993. It is a block cipher algorithm that means it divides plaintext into fixed length block during encryption and decryption. And in which block length is 64bits for Blowfish and variable key length is from 32 bits up to 448 bits. AES Data Encryption – The data encryption standard was old technology for the data encryption, so that, the unauthorized user could be able to read the information, because the DES algorithm might break by use of some methods. So that's way it was not using for securing the top secret information. At that movement the DES algorithm has replaced by a new algorithm which is known as AES (Advanced Encryption Standard). The AES is the best technique for the data encryption now is. It is still egregious for any type of cracking techniques which is provides good security for top secret information. The AES (Advanced Encryption Standard) is proposed by Rijndael in April 2000. It is a block cipher it means that, it is divides information into fixed block during encryption and decryption. In AES algorithm the block size is 128 and it is fixed but the key size is in three flavors like 128, 192 and 256bits. These three flavors of the AES algorithm use for different rounds like. The key size128bit use for 10 rounds, the key size192bit use for 12 rounds, The key size256bit use for 14rounds An AES encryption algorithm consists of many rounds. This is depending on the length of key. And each round made by a set of four basic operation. Like- Key Expansion, Initial Round, and Final Round. And RC2 uses one 64-bit key. Triple DES (3DES) uses three 64-bits keys RC6 uses various (128,192,256) bits keys [2, 11, 18, 19, and 21]. The most common classification of encryption techniques can be shown in Figure 1.1.



(Fig 1.1)

II. RELATED WORK

In past few decades the increased use of internet, demands more security for information. Today, information is need to the transferred safely. Plain text is easily accessible and is prone to hack. The basic need of today's systems is to transfer data to the appropriate user without distortion. As this data has to be send over an open network so this data are subjected to attacks like session hijacking, authentication attacks, and spoofing, sniffing and other network security attacks. Hence a solution is required to protect this data against above mentioned attacks. This method is an effort to secure the data. Today various cryptography algorithms have been proposed or are being used to protect the data but none of the algorithms completely achieves all the security goals. The problem is to overcome the limitations of existing work which was observed during study. The presented the work is our effort, not only to empower a user to hide his secret information but also to enhance the efficiency of an algorithm To restrict the area of research and achieve the quality of work, the presented work is focus to improve the efficiency of algorithm proposed by "*A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm"* and *"Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types".* And According to "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" and other." Effect of Security Increment to Symmetric Data Encryption through AES Methodology". Uses a key for encryption and decryption is generated using large database which results in poor efficiency. In this firstly they are creating large sets of character which are store in file and then they will select key from those sets of character. This complete process is the too much time consuming and it decreases the efficiency by increasing the output time, battery power consumption, execution time and many more. Even the modifications made on the existing techniques of encryption and decryption concentrates mainly to enhance the security level and less on the other parameters like efficiency, response

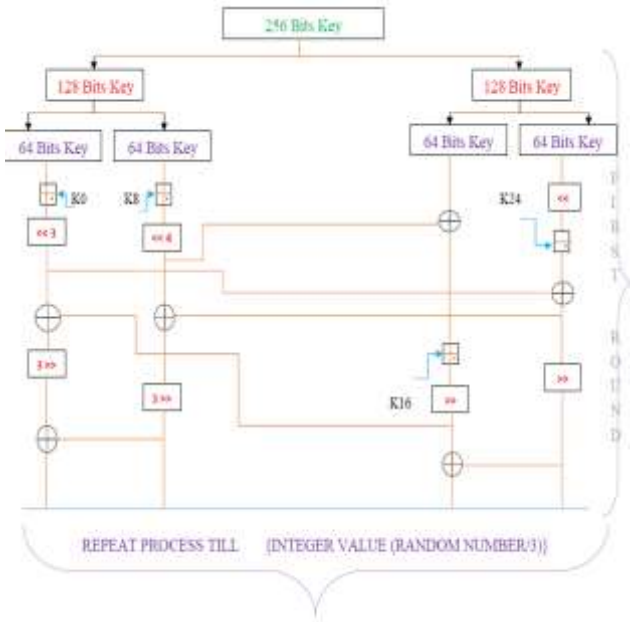
Time, memory utilization, CPU utilization and many more. In software, the cipher and its inverse make use of different code and/or tables. To calculate mixing column functions, existing work are using polynomial equation which increases response time of encryption and decryption

III. PROPOSED WORK

In order to enhance the confidentiality of data and to preserve different dimensions of efficiency like produce output time, battery power consumption, memory utilization etc, a new block based symmetric cryptography algorithm is proposed. This technique uses a random key generator for generating the initial key and this generated key is used for encrypting the given source file. For encrypting the source file basically a block based substitution method will be used. The proposed technique enhances the confidentiality by encrypting the message multiple times. The key value contains all possible words comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. This method will be accept any type of file like .Txt, .PDF, .EXL., .Doc, .JPG, .Bmp, .to be encrypted and return encrypted file with .pa extension that mean that file is encrypted by proposed algorithm. Our Proposed Software will accept input in the form of a file selected from browser by the user. Output of the algorithm will encrypt file on the specified location in the system. The pattern of the key will depend on text key entered by the user. In the proposed algorithm a method is used to obtain randomization number and encryption number from the initial text key. It will be very difficult to match same massages using this parameter. To decrypt any type of file one has to know exactly what the key value is and to find the random matrix theoretically one has to apply 2^{256} trial run and which is intractable This method can adopt on M-S word file, excel file, PDF. Text file.

IV. KEY GENERATION STEPS

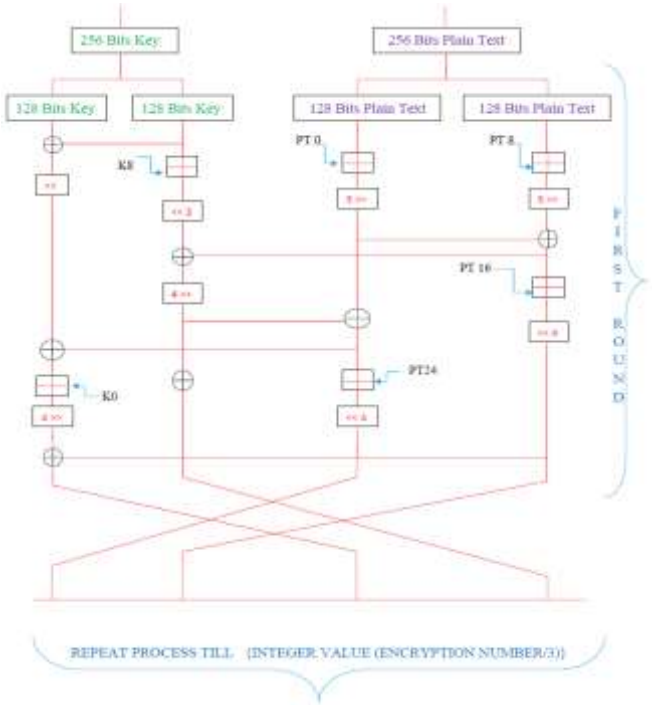
1. first we choose 256 bit key then break this key into two part left key (L.KEY) and right key(R.KEY) and both of each 128 bit.
2. now select one part like L.KEY and again break this L.KEY into two parts left left key1(LLK1) and second is that left right key1, both of each 64bit.similarly rules apply on second part of Right Key.
3. And then we are applying 3 bits on the initial block of 8 bits of Left-Left-Key-1 in shift left circular. And after then output will be Left-Left-Key-2.
4 after then we are applying 4 bits on 8th block of 8 bits of Left-Right-Key-1 by left circular shift. Then Out put will be Left-Right-Key -2.
5. Then the technique of XOR applies between Left-Right-Key -2 and Right-Left-Key-1.and the output of this step will be Right-Left-Key-2.
6. We are applying 2 bits on the 24th block of Right-Right-Key-1 in shift left circular and XOR with Left-Left-Key-2. The out put of this step will be Right-Right-Key-2.
7. After then select 2 bits apply right circular shift on Right-Right-Key -2. And we will be getting the Out put of this step Right-Right-Key -3.
8. Then the technique of XOR applies between Left-Right-Key -2 and Right-Right-Key-2.and the output of this step will be Left-Right-Key-3
9. Then the technique of XOR applies between Left-Right-Key -2 and Right-Right-Key-2.and the output of this step will be Left-Right-Key-3.
10. Now select 3 bits right circular shift apply on Left-Right-Key-3. Then Out put of this step will be Left-Right-Key-4.
11. And then select 2 bits apply on 16 block of Right-Left-Key-2 by right circular shift. Out put of this step will be Right-Left-Key -3
12. Then the technique of XOR applies between Right-Left-Key -3 and Right-Right-Key-3. And the output of this step will be Right-Left-Key-4.
13. Then the technique of XOR applies between Left-Left-Key -2 and Right-Left-Key-3. And the output of this step will be Left-Left-Key-3.
14. After that we are applying 3 bits on Left-Left-Key-3 by right circular shift and XOR with Left-Right-Key-4. Out put of this step will be Left-Left-Key -4.
15. Then in the next round we will use the Left-Left-Key-4, Left-Right-Key-4, Right-Left-Key-4 and Right-Right-Key-3 as input.
16. And we will reuse this entire process till random number divided by 3 is null.
17. And than we will exit.



(Fig.1.2 key generation)

V. ALGORITHM STEPS

1. first we choose 256 bit key and then break this key into two part left key (L.KEY) and right key(R.KEY)and both of key is 128 bit.
2. Again we choose 256 bit key and then break this key into two left plain text (LPT) and right plain text (RPT) and both of each 128 bit.
3. Now we apply XOR operation on both of left key value and right key value and Left key-1 is output of this step.
4. Now we Apply 3 bits right circular shift on first block of 8 bits of left plain text and 3 bits right circular shift on 8^{th} block of 8 bits and XOR with each other. Out put of this step will be RPT-1.
5. We are applying 3 bits on the 8^{th} block of 8bits of Right-Key in shift left circular and XOR with Right Plain Text-1. The out put of this step will be Right-Key-1.
6. Apply 3 bits left circular shit on 8^{th} block of 8 bits of right key and XOR with RPT-1. Out put of this step will RK-1.
7. Apply 4 bit left circular shit on 16^{th} block of 8 bits of RPT-1. Out put of this step will be RPT-2.
8. Apply 4 bits right circular shift on RK-1. Out put of this step will be RK-2.
9. Apply 3 bits right circular shift on first block of 8 bits of left plain text and XOR with RK-2. Out put of this step will LPT-1.
10. Apply 4 bits left circular shift on 24^{th} block of 8 bits of LPT-1. Out put of this step will be LPT-2.
11. Apply 2 bit left circular shift on LK-1 and XOR with LPT-1. Out put of this step will be LK-2.
12. Apply 4 bits right circular shift of first block of 8 bits of LK-2 and XOR with RPT-2. Out of this step will be LK-3.
13. Finally RPT-2 will become RK, LPT-2 will become LK, LK-3 will become LPT and RK-2 will become RPT input for the Next round.
14. Repeat process till encryption number divided by three is null.
15. Exit.



(Fig 1.3 algorithm)

VIII. CONCLUSION

As we know that data security is an important issue and much software based solutions were developed to provide data security but they were not well enough to provide security. Here a new approach for data security using block cipher symmetric key cryptography has been proposed. This new approach uses the concept of encryption number and random

number from paper [1] to enhance the complexity of key. This results in increase efforts for brute force attacks. The proposed approach also uses the logical shift and X-or operations to reduce the CPU utilization and processing time of algorithm. Performance analysis concludes that difference of efficiency between our "proposed algorithm" and existing algorithm is very high. If the security along with efficiency is of primary concern then one can prefer our proposed algorithm. Our proposed algorithm not only enhances the security level but has better efficiency in terms of CPU utilization and encryption time than any of the other comparing algorithms and hence can be incorporated in the process of encryption of any plain text. The proposed encryption algorithm presented above, is a very simple, direct mapping algorithm using some logical operation. The proposed system successfully encrypts and decrypts the files in Text, PDF, xml, image, mp3 format.

VIII. APPLICATION

Proposed Encryption/Decryption algorithm can find its applicability in various sector like banking sector, education sector, medical sector, different type of private organization, and many more sectors. Some more point where proposed algorithm can be used is following proposed encryption algorithm can be suitable for many different type of applications: Proposed encryption algorithm should be efficient in encrypting data files or a continuous data stream. Proposed encryption algorithm should be efficient in producing single random bits. Proposed encryption algorithm should be efficient in encrypting packet-sized data.

IX. FUTURE ENHANCEMENT

I will work on security enhancements of algorithm; I will improve the result of algorithms. Presently our algorithm works on particular format of files like Text, PDF, Audio, word and Excel, but in future I will enhancement works on Mp4 and Video Format also.

REFERENCES

[1] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE
[2] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud *"Evaluating the Effects of Symmetric* Vol 3, Issue 2, Page-66-71,Feb(2011)
[3] Symmetric key Cryptography using modified DJSSA symmetric key algorithm ,Dripto Chatterjee, Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, accepted for publication in WORLDCOMP-2011 to be held in Las Vegas, USA from 18/07/2011 to 21/07/2011.
[4] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm, Neeraj Khanna, Joel James, Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath, accepted for publication CSNT-2011 IEEE International conference to be held at SMVDU, Jammu from 03/06/2011 to 05/06/2011
[5] Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath Advanced Steganographic Approach for Hiding Encrypted Secret Message in LSB, LSB+1, LSB+2 and LSB+3 Bits in Non standard Cover Files" published in International Journal of Computer Applications (0975 – 8887) Volume 14– No.7, February 2011

[6] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.
[7] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept. 2010
[8] Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm, Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, Journal of Computing, Proposed algorithm (1.3)

Books:
[9] Cryptography and Network, William Stallings, Prectice Hall of India.
[10] Onwutalobi Anthony-Claret *"Using Encryption Technique"* Department of Computer Science, University of Wollongong Australia, Anthony.claret@ieee.org.
[11] William Stallings, *"Cryptography and Network Security: Principles & Practices"*, second edition,
[12] Hardjono, "Security in Wireless LANS and MANS," Artech House Publishers.

Web References:

[13] http://informativeprompt.com/2011/02/cryptography-history-and-terms.html
[14] http://www.ibm.com/developerworks/library/s-crypt02/index.html
[15] http://people.csail.mit.edu/rivest/Rc6.pdf
[16] http://www.freetechexams.com/computers- tips/computer-tips/aes-algorithm.html