Using Simple Encryption Technique a TimeLine Approach for Block Cipher Module

Poorva Shukla[1], Alpana Meena[2]

[1]Research Scholar, [2]Assistant Professor
Department of CSE, Department of IT
Indore Institute of Science and Technology, Indore (M.P), India

***Abstract*: Number of aspects related to security like so many applications ranging from E-commerce, payments gateways .But there are so many hackers' tools are available which breaks the security concern. For that purpose our main focus is secures transmission of information that is possible with the help of cryptography. Cryptography is very necessary for secure transmission of our personal data or we can say information. Now cryptography itself is not sufficient for secure for secure transmission of information .our works presents on encryption /Decryption that is we have called cryptography. The Encryption and decryption techniques are able to work publically or privately or with any type of secure file. It can work on image file, text data file, audio/video file, power point presentation file and so on…..**

The Encryption /Decryption technique or cryptography is one of key generation method of randomization .If we want to create a encryption key for any type of information but result for that key is only in binary format. To create a Key we use a simple mathematical operation like matrix and substitution of bits which can be applied on each block of information. The key generation and encryption are very transparent to the user. Now the process is used to decrypt the encrypted binary file.

***Keywords*: Symmetric decimal key, Encryption, Decryption, audio, file**

Introduction

During the age of information, evolution of technology in daily life and social organization is digitized. Today's is the world of digitization or digital information for example -if we talk about the security of our information or data it is totally related to the real life like how we can secure our gold jewellery in our home. We can use our almirah locker or we can use bank locker, so there is a concept of key. The key is available only for authenticated person. Here we use concept of cryptography. In a network there are so many movable mobile nodes are available. If the transmitter wants to send the data, they may pass from one node to another node so that here the security may be a concern, that's why we use the concept of key generation. Data can be transmitted in many forms and this information can openly move around the network. In such cases the security is the main issue so we use a technique of cryptography which can be implemented at both the ends (sender and receiver). There is a mechanism of key generation which should be public and private both according to the information type. [1]
To protect our information we use two distinct problems.

- Security protection :-
  - For security we mean that preventing information from unauthorized or unwanted Access.

- Authentication :-
  - For Authentication we mean that the receiver which receives the data (information) is on the right hand.

Our proposed work is devoted to the first problem. In cryptography there are two type of key generation technique used.

- Symmetric key Generation.

- Asymmetric key Generation.

In cryptography a key is any type of variable value that is applied on an unencrypted text to produce encrypted text. The length of the key depends on how difficult it will be to decrypt the given text. Keys are shared in between the sending device (sender) and receiving device (receiver).[2]
In some cases the keys shared in between sender and receiver is common that is called public key encryption. Now in some cases the key is shared between sender and receiver have their individual encrypted key and decrypted key.[3]
The main purpose to use cryptography is **Confidentiality** it means that cryptography ensure transmission of personal data in a very confidential manner. **Authentication** means that cryptography ensures that the data is sended or received by the reliable person. **Integrity** means that it ensures the quality of audio/video file. **Non- repudiation** means that the sender and the receiver cannot deny the authenticity. **Access control** is also an important aspect of security by which how we can access the information if multiple data can be generated at a time, so for that purpose cryptography ensure the Access control mechanism. **Availability**

means that suppose transmitter wants to send the data but the receiver is not available at that time that's why it ensures the availability also. [4]

Fig 1 key concept [20]

Encryption algorithm uses the two basic principles.

- Substitution method
- Transposition method

In substitution method elements used in plaintext is mapped into another element. And in transposition elements of plaintext are re-arranged in different position.

$$\text{plaintext} \xrightarrow{\text{encryption}} \text{ciphertext} \xrightarrow{\text{decryption}} \text{plaintext}$$

Plaintext: A message in its original form
Cipher text: A message in the transformed, unrecognized form
Encryption: The process for producing cipher text from plaintext
Decryption: the reverse of encryption
Key: a secret value used to control.

Here we use symmetric key cryptography for key generation to address the problem of security protection. If sender and receiver share a single, common key for encryption and decryption at the end of sending device and at the end of receiving device. That process is called symmetric key or symmetric encryption. Based on this phenomenon symmetric encryption are known as ciphers.[5]

Now Symmetric key cryptography is the concept of secret key generation. They use common key at the end of sending device and at the end of receiving device or we can say that for encryption and decryption the share common key or one key. It has been used for traditional days and it is used in some of these situations where same key is used for both to encrypt or to decrypt the data which is some time known as Caesar cipher. [6]

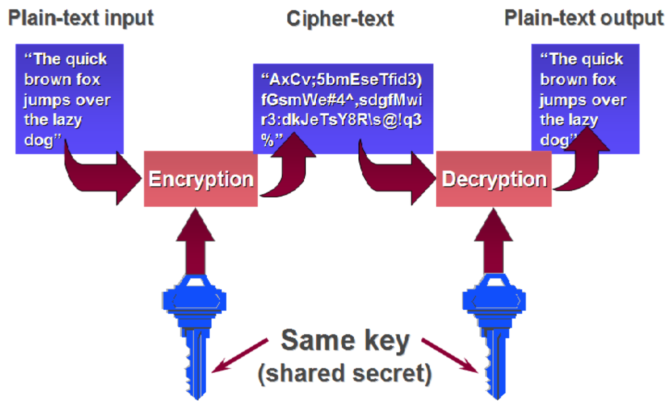
Plain-text input
Cipher-text
Plain-text output
"The quick brown fox jumps over the lazy dog"
"AxCv;5bmEseTfid3) fGsmWe#4^,sdgfMwi r3:dkJeTsY8R\s@!q3 %"
"The quick brown fox jumps over the lazy dog"
Encryption
Decryption
Same key
(shared secret)

Fig 2 symmetric key generation [21]

In asymmetric key cryptography it uses the concept of public key cryptography where two keys are used one for encryption and another for decryption. One is public key which can access publically; it means that everyone can access these keys. Another one is private key which can be accessed privately. It means no one can access these key. Or we can say different keys must be used for encryption and decryption so we almost never shared the private key .It is impossible for the user who views the encrypted data with symmetric cipher.

There are mainly two types of symmetric cipher.

- Block cipher
- Stream cipher.

Stream cipher can be faster than Block cipher but a block cipher and stream cipher are encryption technique that encrypt a fixed size n bit data (packet).It could be 64 bits ,128 bits and 256 bits .[7]
64 bits of data use 64 bits of plain text and it could be encrypt into 64 bits of cipher text .popular block cipher used like DES, Triple DES, AES, IDEA & Blowfish. As we can say that it is faster method of encryption so that stream cipher is also an encryption technique of cryptography. But it can encrypt 1 bit or byte of plaintext at a time .It could be designed to approximate an idealized cipher which is known a onetime pad .That one time pad can be use only one time to encrypt or decrypt the data (information).[8]

Problem Definition

There are number of research paper examines the symmetric encryption of various algorithm likes AES, 3DES, DES, Blowfish Idea and so on……These all are the encryption technique and took a lots of time or we can say these all are the time taken algorithm and it could be measure in term of CPU Time, Throughput, Battery power consumption.[9] Now battery problem is related to the energy consumption now we examine that these all algorithms are very time consuming and energy consuming. Now today's is the world of digitization .digital information is transformed from one end to another end. So that the battery consumption and time consumption is very much important concern in the world of digitization .how fast we can send data or we can perform transaction like money should be transfer from one user to another user or online shopping. Theses all are the main aspects. So we have to make an mechanism which has strong security and their battery backup is good, and fast communication is done in between the sender and the receiver .By which they can communicate as much as faster .Now we suggest an algorithm with the help of that algorithm we reduce all the problems occur in all types symmetric key algorithm.[10]
The algorithm reduces some of the energy consumption problem and so that found after six hundred encryption of five MB file the remaining battery power is about to forty five percent .and more encryption is not possible if battery goes to die.[11]
It can be conclude that AES is as much faster than other encryption standards.[12] A study of another research that all the encryption algorithm AES,DES,3DES,IDEA And Blowfish so on….gives a batter performance but still there is a problem of energy consumption and fastest communication so that our work focus on these problems so we compare these all symmetric key encryption algorithm to our proposed algorithm.[13][14] et all.

Proposed Technique

Key Generation
With the help of generating function we can generate a key at both the end .at the end of sending and at the end of receiving it means that the Encryption and Decryption occur at both the end .Sender may be Receiver some times and Receiver may be sender sometimes. There are following steps which should be performed.

1. Start with new key "M".

2. Choose some eighteen alphabets (character) from any key "M"

3. If M<=18 alphabets (character) the filled character space as one.

4. Cobble up two matrix which is (Three *Three) and the matrix became fill with key values like K1,K2,K3,K4,K5,K6,K7,K8 and K9 and another matrix also became fill with the key values K10,K11,K12,K13,K14,K15,K16,K17 and K18. Respectively.

5. Here we consider B as a block key for Encryption and Decryption.

6. Now we put the ASCII value of each key values like ASCII value of K1, K2, K3, K4………K19.

   B1=(K1+K10)*(K4+K13)*(K7+K16).
   B2=(K2+K11)*(K5+K14)*(K8+K17).
   B3=(K3+K12)*(K6+K15)*(K9+K18).

7. Now finally we consider these Block Key

   B=B1*Y(10^6)+B2*Y(10^3)+B3.
   B=B mod 10^9.
   B={Y1,Y2,Y3,Y4,Y5,Y6.Y7.Y8,Y9}.

Result Comparisons

In the result analysis the time consumption is the main issue in previous algorithm so we make our proposed algorithm with the help of that we can see in this graph clearly.

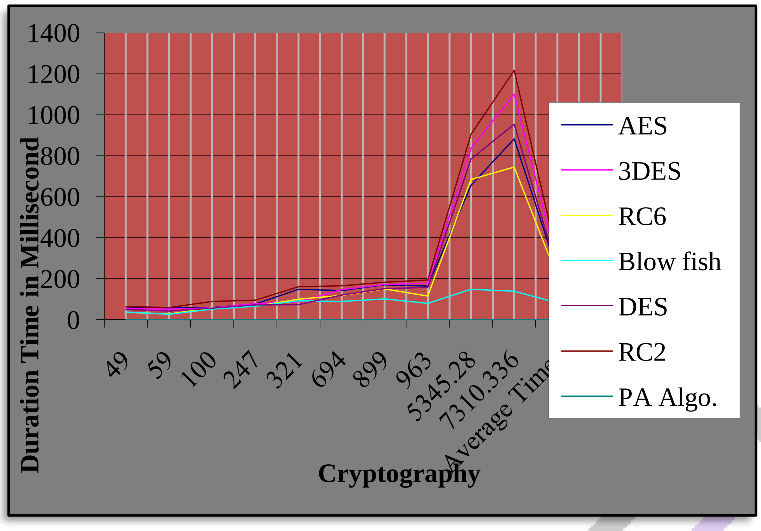

Fig 3 Time consumption graph

Conclusion and Future Enhancement

Now a days there are so many methods and algorithms are available to secure our personal data or information.
Because today's is the world of digitization or we can say cache less world .in this manner security is more concern in the world of digitization or there are so many algorithms like AES,DES 3DES ,IDEA,RC2,RC5,RC6 and our proposed algorithm so on…are help full for secure transmission .
So in future we use hash function to implement this algorithm because hash function takes an arbitrary input but produce a fixed size output. We give a strong security result to protect our data, information .so that the unauthenticated user can't access our personal information.

References

1.R.Chandramouli, "Battery power-aware encryption," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 2, pp. 162-180, May 2006.
2.D. Coppersmith,"The data encryption standard (DES) and its strength against attacks," IBM Journal of Research and Development, pp. 243 -250, May 1994.
3.J. Daemen, and V. Rijmen, "Rijndael: The advanced encryption standard," Dr. Dobb's Journal, pp. 137139, Mar. 2001.
4. P. Ding, "Central manager: A solution to avoid denial of service attacks for wreless LANs," International Journal of Network Security, vol. 4, no. 1, pp. 35-44, 2007.
5. N. E. Fishawy, "Quality of encryption measurement of bitmap images with RC6, MRC6, and rijndael block cipher algorithms," International Journal of Network Security, pp. 241-251, Nov. 2007.
6.Hardjono, Security In Wireless LANS And MANS, Artech House Publishers, 2005. International Journal of Network Security, Vol.10, No.3, PP.213–219, May 2010
7. S. Hirani, Energy Consumption of Encryption Schemes in Wireless Devices Thesis, University of Pittsburgh, Apr. 9,2003, Retrieved Oct. 1, 2008.
8. M. S. Hwang and C. Y. Liu, "Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.
9. M. H. Ibrahim, "A method for obtaining deniable public-key encryption," International Journal of Network Security, vol. 8, no. 1, pp. 1-9, 2009.
10.M. H. Ibrahim,"Receiver-deniable public-key encryption," International Journal of Network Security, vol. 8, no. 2, pp. 159-165, 2009.
11. S. Z. S. Idrus, and S. A. Aljunid, "Performance analysis of encryption algorithms text length size on web browsers," IJCSNS International Journal of Computer Science and Network Security, vol. 8, no.1, pp. 20-25, Jan. 2008.
12. K. McKay, Trade-offs between Energy and Security in Wireless Networks Thesis, Worcester Polytechnic Institute, Apr. 2005.
13. K. Nail, "Software implementation strategies for power-conscious systems," Mobile Networks and Applications, vol. 6, pp. 291-305, 2001.
14.P. Ruangchaijatupon, and P. Krishnamurthy, "Encryption and power consumption in wireless LANs-N," The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001.
15 B. Schneier, The Blowfish Encryption Algorithm, Retrieved Oct. 25, 2008.

16 A. Sinha, A. P. Chandrakasan, and JouleTrack, “A web based tool for software energy profiling,” Proceedings of the 38th Design Utomation Conference, pp. 220-225, DAC Las Vega, US, 2001.
17. W. Stallings, Cryptography and Network Security, Prentice Hall, pp. 58-309, 4th Ed, 2005.
18 A. A. Tamimi, Performance Analysis of Data Encryption Algorithms, Retrieved Oct. 1, 2008.
19.A. Nadeem, “A performance comparison of data encryption algorithms,” IEEE Information and Communication Technologies, pp. 84-89, 2006.
20. http://www.wisegeek.org/what-is-cryptography.htm#
21.https://www.supinfo.com/articles/single/3654-modern-type-of-cryptography
22. Results of Comparing Tens of Encryption Algorithms Using Different Settings-Crypto++ Benchmark, Retrieved Oct. 1, 2008.
23.http://www.garykessler.net/library/crypto.html
24.http://www.cryptographyworld.com/what.htm
25. http://www.ibm.com/developerworks/library/s- crypt02.html
26. http://www.simple-talk.com/dotnet/.net framework/symmetric-encryption/
27. http://www.encryptionanddecryption.com/
28.http://www.encryptionanddecryption.com/algorithms/ symmetric_algorithms.html
29.http://www.omnisecu.com/security/public-key- infrastructure/public-key-cryptography.htm.