International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue VIII, August - 2020

An Novel Approach on Encryption by Splitting Key and Text

Binusha R[1], M.E Computer science and Engineering,
Prof.J.N.Rajesh Kumar[2],Head of the department,Department of Computer Science and Engineering, [1,2]Sree Sastha Institute of Engineering and Technology, Chemparampakkam,Chennai,India
Mail id:binusharajan@gmail.com

ABSTRACT

Data transmission is happening in our day to day life.we need secure transmission of data from source to destination.wedon't want third person to read our messages which we send to destination.Security of data in a computer is needed to protect critical data and information from other parties.One way to protect data is to apply the science of cryptography to perform data encryption. For secure transmission so many approaches available nowadays.Eventhough the hackers hacked the messages and doing illegal activities. So we need to protect data in more secure manner.The proposed approach is that the key is derived to set of keys and the data is derived to set of data. Each data is assigned with a set of key.The logic of randomly assigning key and data is hidden from both sender and receiver as well as the opponent.It increases the complexity in security.Eavesdropping and any other attacks cannot be possible by this approach.This approach is highly secure.

1. INTRODUCTION

Security is a freedom from or against harm caused by others. Data security means protect data from corruption, destruction, interception, loss or unauthorized access. In this modern world, there is data transmission happening in day to day life. Data transmission refers to the process of transferring data between two or more devices, In data transmission there is some issues in security.We use Cryptography ideas to make more complex for attackers who access data without getting permission.

All departments needs security in data transmission. Data Security is an aspect of IT organisations of every size and type. Data security is also known as Information Security. The Technology is that data is encrypted and send to destination, Receiver get the encrypted message and key is shared between sender and receiver, Receiver decrypt the cipher text by using key. For more Complexity here we are using AES algorithm with splitting technique. This provides more security to data.

Cryptography

Cryptography means the method of protecting information through use of codes so that only for whom the information is intended can be read and processed. Crypt means hiding and graphy means writing. Cryptography uses two ideas: encryption and decryption. Encryption means convert plain text into cipher text and Decryption means convert cipher text into plain text. Persons who practice this field are known as Cryptographers.It allows users to transfer data

and receive data safely and without loss. In other words Cryptography means hiding something from unauthorised persons.

2. Existing system:

The Existing system approach the encryption using splitting technique. In this the system the data and key is splitted into n splits. First split of data is encrypted by using first split of key and second split is encrypted by using second split of key and so on. Combine the splits to get cipher text. In decryption side, the cipher text and key is splitted into n splits. First split of data is decrypted by first split of key and second split of data is decrypted by second split of key and so on. combine the splits to get the original message.

2.1 Drawbacks of existing system:

- Insecure
- Matching paves a way to attackers to guess the key or data
- If block of key is found by attackers, they easily find out the whole key and by using those keys, original data was found

3. PROPOSED SYSTEM

To overcome the existing system anomalies, this novel approach on encryption by splitting data and key is developed. This keeps data away from Eavesdroppers and hackers. In existing approaches simply data or key is splitted and encryption and decryption takes place. This provides lack in security and it provides a way to eavesdroppers and hackers. We introduced an novel approach on encryption by splitting key and text. By using key splitting and arranging, the data is splitted and arranged. Splitted data is encrypted and decrypted by splitted key. Rounding is done by AES algorithm.

3.1 Advantages of proposed system

- Secure
- Confidentiality
- Matching provides complexity to attackers in finding data or keys

3.2 Methods of proposed system

The approach is that key is converted into binary and splitted. A part of splitted 8bit is taken and again divided into two parts. calculate number of ones and first part binary number is converted into decimal number. That decimal number is subtracted from the constant number 4. That result is multiplied with decimal number which was calculated decimal number of second part. This process undergoes upto last 8 bits. Then arrange the Key based on the multiplied result value in ascending order.The plaintext is converted into binary and divided same as key. The arrangement of plaintext is based on the arranged order of key. The part of a plaintexts encrypted by the a part of key. Like that all parts are encrypted and transmitted to the destination. The sender receive the key and the encrypted message. The encrypted data is decrypted using the key and arrange by using the key order. The Concept behind this system is Encryption and Decryption.

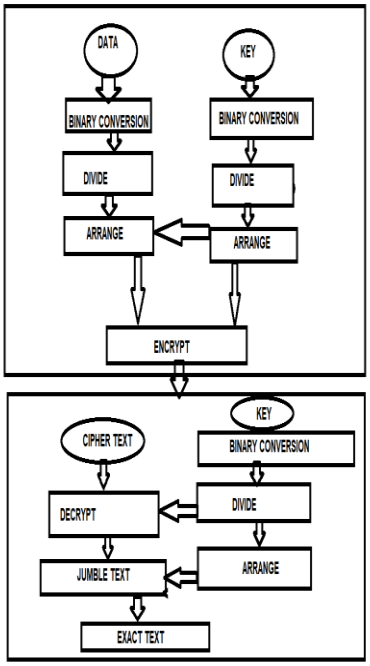
The value of a part of key is rounded by using AES algorithm. In AES algorithm total

round is 10. Here round is decided by :value % 16=round.

Algorithm

1. Get Data and Key
2. Convert Key into binary values
3. Divide the binary value into 8 parts of 8 bits
4. If bit size is less than 64, then zero padding will perform on the left side of the digits
5. Take a part of 8 bits and divide it into two equal halves
6. Find the value of G. G=number of ones in binary value of a part
7. Convert the first part of binary value into decimal value
8. Convert the second part of binary value into decimal value
9. Calculate y= 4-G. The result of y is multiplied with the decimal values of two parts
10. Repeat the step 6-9 for all 8 parts
11. The resultant values are arranged in ascending order
12. Thus the key is ordered by the resultant value
13. Data is taken and converted into binary value
14. Binary value of data is divided into 8 parts of 8 bits
15. Data part is ordered based on the arrangement of the key
16. Key arrangement is only for the arrangement of data
17. Each data part is encrypted by each key part
18. Encrypted data and key is send to the receiver side
19. In receiver side, by using key cipher text is converted into plain text
20. Plain text is then arranged by using key arrangement method which was used in sender side
21. Repeat the step 2-11,then the plain text is obtained.

3.3 Block diagram:



Advanced encryption standard:

AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the

length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each round consists of the following four steps to encrypt 128-bit block

Substitute Bytes Transformation

The first stage of each round starts with Sub Bytes transformation. This stage is depends on nonlinear S-box to substitute a byte in the state to another byte.

ShiftRows Transformation

The next step after SubByte that perform on the state is ShiftRow. The main idea behind this step is to shift bytes of the state cyclically to the left in each row rather than row number zero. In this process the bytes of row number zero remains and does not carry out any permutation. In the first row only one byte is shifted circular to left. The second row is shifted two bytes to the left. The last row is shifted three bytes to the left. The size of new state is not changed that remains as the same original size 16 bytes but shifted the position of the bytes in state.

MixColumns Transformation

The multiplication is carried out of the state. Each byte of one row in matrix transformation multiply by each value (byte) of the state column. In another word, each row of matrix transformation must multiply by each column of the state. The results of these multiplication are used with XOR to produce a new four bytes for the next state.

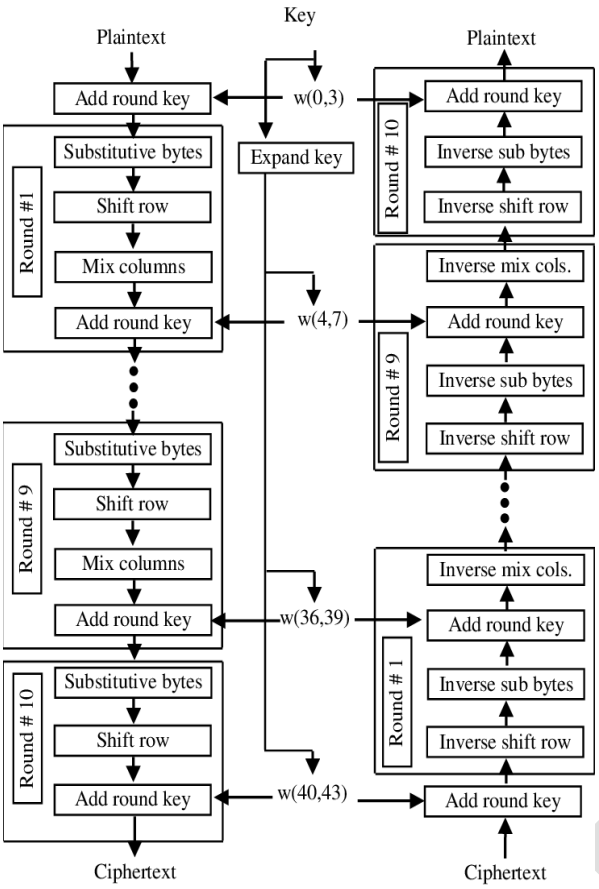
AddRoundKey Transformation

AddRoundKey is the most vital stage in AES algorithm. Both the key and the input data (also referred to as the state) are structured in a 4x4 matrix of bytes. This operation is based on creating the relationship between the key and the cipher text. The cipher text is coming from the previous stage. The AddRoundKey output exactly relies on the key that is indicated by users. Furthermore, in the stage the subkey is also used and combined with state.The size of subkey and state is the same. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

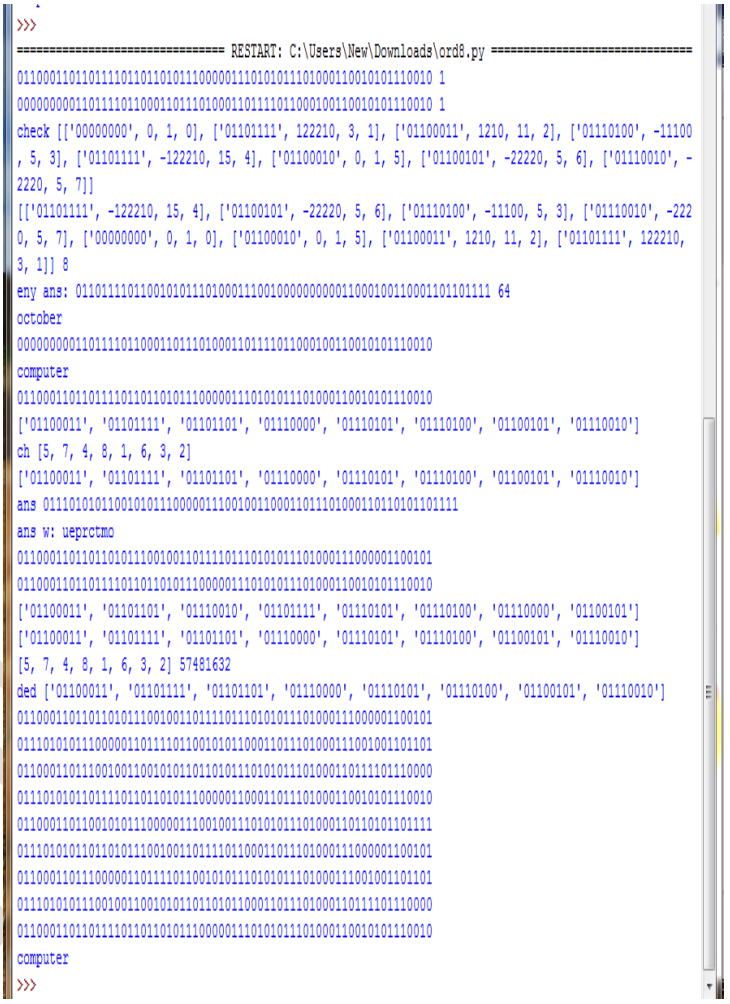
AES algorithm is based on AES key expansion to encrypt and decrypt data. The key expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x (Nr+1) words. Where Nr is the number of rounds. The process is as follows:

The cipher key (initial key) is used to create the first four words. The size of key consists of 16 bytes (k0 to k15) that represents in an array. The first four bytes (k0 to k3) represents as w0, the next four bytes (k4 to k7) in first column represents as w1, and so on. We can use equation K [n]: w[i] = k [n-1]: w[i] XOR k[n]: w[i]to calculate and find keys in each round easily.

International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue VIII, August - 2020



Result:



4. Conclusion

The project conclude that the implemented work is an novel approach on encryption by splitting key and text. The Advanced encryption standard algorithm is used as a part for security.The approach is that key is converted into binary and splitted.A part of splitted 8bit is taken and again divided into two parts. calculate number of ones and first part binary number is converted into decimal number. That decimal number is subtracted from the constant number 4. That result is multiplied with decimal number which was calculated decimal

number of second part. This process undergoes upto last 8 bits. Then arrange the Key based on the multiplied result value in ascending order.

The plaintext is converted into binary and divided same as key. The arrangement of plaintext is based on the arranged order of key. The part of a plaintext is encrypted by a part of key. Like that all parts are encrypted and transmitted to the destination. The sender receive the key and the encrypted message. The encrypted data is decrypted using the key and arrange by using the key order. The Concept behind this system is Encryption and Decryption.

The value of a part of key is rounded by using AES algorithm. In AES algorithm total round is 10. Here round is decided by :value % 16=round.

REFERENCES

1.AbhishekChaudhay,Avinash Kumar Sharma, Jolly dutta,Kanika Gupta,(2018), "Providing security by encryption and Splitting technique over cloud storage" , Internal Journal of Engineering and Techniques, vol-4, issue-2.

2. Ajay Kumar, S. Bose, (2016), "Cryptography and network security", Pearson publications India.

3.AkoMuhammadAbdullah,(2017),"Advanced Encryption Standard algorithm to encrypt and decrypt data", Research Gate publications.

4. DigvijayPawar, (2017), "Survey on network based cryptographic techniques for key generation and data encryption/decryption", International Research Journal of Engineering and Technology, vol-4, issue-5.

5.Jaishree Singh, Dr.J.S.Sodhi, (2013)," Secure data transmission using encrypted secret message", International Journal of ComputerScience and Technologies, vol-4(3).

6. Prof.S. Athinarayanan, S.Nivetha, R. Supriya, (2017)," secure data with key managers by using shamir scheme and AES algorithm", International Journal of computerscience Trends and Technology, vol-5, issue-2.

7.Vishnu Sharma, Meenakshisharma, (2015)," Security of file through splitting and hybrid encryption mechanism", International Journal of Advanced Research in Computer and communicational Engineering, vol-4, issue-9.

8.William Stallings, (2005), "Cryptography and Network Security",Prentice Hall,4th Edition.