IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Standardization Of AES Algorithum

Snehal Kundlikrao Waybhase,
Department of Computer Science & engineering, ,
G H Raisoni University,
Amravati,Maharashtra,India

Prof. Prashant Adakane
Asst. Prof.,Department of Computer science & engineering
G H Raisoni University,
Amravati,Maharashtra,India

***Abstract*—*In day to day life internet is counted as a part of daily needs and 60% population of the world is dependent on the internet. While Using internet there are challenges in data security and privacy as this data can be utilized by hackers thus, taking this in account in this paper we had proposed the advance custom configurable algorithm for AES. This is made by adding new layer of security for the each letter of a message so that its impossible to encrypt it by hackers. We Are changing the keys for each letter with new layer of encryption which is already defined by the algorithm, thus removing the vulnerability for frequent attacks. This new layer aids the protection to the AES algorithm, which is already more secure. In today's digital world, the importance of digital cryptography in securing electronic data transactions is unquestionable.. This data includes financial and legal files; medical information; automatic and internet banking information etc.. To accomplish these requirements, Advanced Encryption Standard (AES) for encryption of electrical data can be used. Although no major attacks on AES has been discovered yet,*

Keywords*— *AES(Advanced Encryption Standard); Internet; Security; Encriptions layer;

I.Introduction

The AES stands for Advanced Encryption Standard and is a majorly used symmetric encryption algorithm. It is mainly used for encryption and protection of electronic data. It was used as the replacement of DES(Data encryption standard) as it is much faster and better than DES. AES consists of three block ciphers and these ciphers are used to provide encryption of data.,AES is a block cipher. The key size can be 128/192/256 bits. Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

Working of the cipher :

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time. The number of rounds depends on the key length as follows :

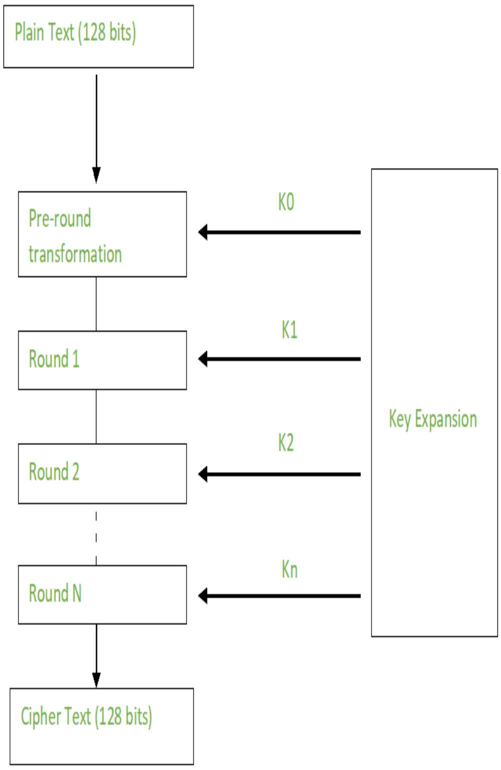
128 bit key – 10 rounds

192 bit key – 12 rounds

256 bit key – 14 rounds

Creation of Round keys :

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption



.

Fig.1 *Generating round keys process diagram*

II. Literature Servey

AES was developed by NIST(National Institute of Standards and Technology) in 1997. It was developed for replacing DES which was slow and was vulnerable to various attacks. So, therefore, a new encryption algorithm was made to overcome the shortcomings of DES. AES was then published on 26th November 2001.

B.Nageswara Rao et al. (2017) in their paper “Design of Modified AES Algorithm for Data Security” said that increase in the number of round(cycles) from 10 to 16 make the algorithm(AES) more secure. With the increase in no of the cycles then it will require more computational power and difficult to attack by the hacker to get into the system. The uses polybius square technique to generate the key.[1].

Ako Muhammad Abdullah (2017) in their paper “AES Algorithm to Encrypt and Decrypt Data” implemented 10 rounds of AES encryption is used with the help of keys size of 128bits, 192bits and 256 bits block cipher. The conclusion is made from his research is that the AES is having more security than the other algorithms like DES, 3DES etc.[2]

N Sivasankari et al. (2017) in their paper “Implementation of Area Efficient 128-bit Based AES Algorithm in FPGA” have said that both encryption and decryption has been actualized into a single solitary chip(FPGA-XC5VLX50T) and the performance of he operation (encrypt/decrypt) with low asset used and the high throughput of 38.65Gbps.[3].

Talari BhanuTeja et al. (2017) in their paper “Encryption and Decryption –Data Security for Cloud Computing –Using Aes Algorithm” implemented both RSA and AES algorithm are mixed for encryption handle utilizing USB gadget to upload and download data. Securely uploading and downloading of files is archived. The advantage is that system provides a spine structure to cloud storage frameworks where security. Is increased .The drawback is Proposed system works only on text files and not on data like image, audio, video, etc [4].

Encryption has a strong presence in today’s digital electronics with the frequent transmission and storage of sensitive data. AES as the standard encryption algorithm and

it is commonly used as a fast solution to secure data. When designing VLSI systems, the task of balancing the area, power, and speed is a challenge; hardware encryption is no different. System requirements drive certain performance parameters to the forefront, identifying how to alter design implementations to meet performance requirements is not always apparent. Multiple resources in this research field have identified AES algorithm features of interest and discussed their impact a few of the design trade spaces, however, a single comparative analysis was lacking. This project explores six different AES

features key size, mode specificity, round key storage, round unraveling, SBOX implementation, and pipelining. A summarized view of the resulting designs allows readers to quickly analyze how each of the six features impacts speed, power, area, latency and throughput.

III. Praposed Work

The program begins with the sender, who wants to send a text message, to an another user known as receiver. The plaintext is written in a textbox and when the sender hits the “encrypt” button the plain text is converted first to an intermediate ciphertext which is the result of encryption done by the Caesar cipher. The key generated for this encryption is the last letter of the plaintext and it is inserted at a particular index of the ciphertext depending on the length of the string being odd or even.

At this stage the plaintext is converted to ciphertext but only 50%. The next step of encryption is AES encryption which uses standard AES algorithm to encrypt the intermediate ciphertext into a complete ciphertext which is very difficult to crack by the attacker. At the receiver's side, the decryption process begins with changing the ciphertext to the plain text. The decryption process is the reverse of the encryption process. At first the ciphertext is decrypt using AES decryption and then further it is decrypted with the help of Caesar cipher decryption, with the key being hidden in the cipher text only. After both the stages of decryption is completed the receiver will receive the plaintext as sent by the sender. The main reason for effectiveness of this process is that no outsider can guess the steps it is using, as nowhere it is specified that Caesar cipher is being used. The user will have an application on which will ask two options:

ENCRYPTION –This will encrypt the plaintext to the ciphertext with the help of key.

DECRYPTION - This will decrypt the ciphertext to the plaintext with the help of the key.

Encryption – Here the user will enter the plaintext in a textbox and by clicking on the ‘encrypt' button the plaintext will be encrypted using custom made Caesar cipher encryption algorithm after which it will be further encrypted using AES Algorithm. Furthermore the user can custom configure it in order to make the ciphertext even more secure. To see the ciphertext of a particular plaintext one can select the required plaintext from the drop down and can press ‘SHOW’ button to reveal the encrypted ciphertext into the normal form. This is done at the Sender end by the user.

Decryption – Here the user will be able to decrypt the ciphertext to plaintext using the reverse of AES algorithm with custom configuration of the Caesar Cipher decryption. This is done at the Receiver’s end into the application. This is done with the help of JAVA programming language and writing the code for the AES algorithm. After encrypting the plaintext to ciphertext, it goes to the database where it gets stored. And for decrypting the same procedure is followed but in the reverse order. The ciphertext is pulled from the database and converted back to plaintext. Major use of this application will be in military and in various top-secret government intelligence agencies. Basically, any organization who needs to exchange messages with excessive security can implement this idea.

Characteristics

AES has keys of three lengths which are of 128, 192, 256 bits.

It is flexible and has implementation for software and hardware.

It provides high security and can prevent many attacks.

It doesn’t have any copyright so it can be easily used globally.

It consists of 10 rounds of processing for 128 bit keys.

Advantages

It can be implemented on both hardware and software.

It provides high security to the users.

It provides one of the best open source solutions for encryption.

It is a very robust algorithm.

RESULT

First we have to enter the text “Raisoni”which we want to send.

Plain Text	Raisoni
Ciphertext 1 (after Caser encryption)	V/726+Q2jR+AxTKOUZ
Ciphertext 2 (after AES encryption)	wJkWGKIR8ODObFdc99nAGb6pOGU+1DVUn7qADWVH4Dhp0
Ciphertext 3 (after AES decryption)	V/726+Q2jR+AxTKOUZ
Ciphertext 3 (after Caser decryption)	Raisoni

After that we have to click on the "ENCRYPT" button we get the our cipher text along with the key. Now we can copy and paste
the cyphertext into the another application and we can send that encrypted data to the another user with the help of another
application or we can even again encrypt that key for the security reason.
Now we send the data to the another user in the ciphertext form.
At the receiver end we will receive the data into the ciphertext then we will cut and copy the data and paste the data to the
same application on his system and enter the key which is received by him from the another network send by the sender or
even by the way.
Now he can just decrypt the data by just clicking on the "DECYRPT" option and the cipher text is converted into the plaintext.

CONCLUSION

The paper is based on extended AES algorithm with custom is a configuration which is an completely new concept. A configurable algorithm is proposed that allows the user to modify the algorithm each time encrypts text, without the user actually knowing it. The algorithm uses AES and adds some custom configurable steps in the system. As is known the world is advancing more towards the digital systems and internet accessibility worldwide is often good. Many governments use AES configuration for transmission of classified messages. Our algorithm is very useful for any such government as well as other organisations, because it adds an extra layer of security that is completely unknown to people, even to the user. Thus, theoretically it cannot be broken without inside help. Future work may include making the system adaptable to alpha numeric inputs. In this paper, randomization of only the caesar cipher key is explained, but in the future, the first key for AES expansion can also be randomized based on the input.

REFERENCES

[1] Rao B.Nageswara, Tejaswi, D., Varshini, K.Amrutha, Shankar, K.Phani, Prasanth B. “Design of Modified AES Algorithm for
Data Security”, International Journal For Technological Research In Engineering, Volume 4, Issue 8, pp 1289 – 1292 , April –
2017.
[2] Sivasankari N, Rampriya K, Muthukumar, A, “Implementation of Area Efficient 128-bit Based AES Algorithm in FPGA ”,
European Journal of Advances in Engineering and Technology, 4 , pp 541 -548, 2017.
[3] TalarI Bhanu Teja, Vootla Hemalatha,K Priyanka,“ Encryption And Decryption– Data Security For Cloud computing
using Aes Algorithm”,SSRG International Journal of Computer Trends and Technology(IJCTT), Special Issue,pp80-
83,April 2017.
[4] Rizky Riyaldi, Rojali, Aditya Kurniawan,“ Improvement of Advanced Encryption
Standard Algorithm it ShiftRow and S.Box Modificatio n Mapping in MixColumn ”,
2nd International Conference on
Computer Science and Computational
Intelligence (ICCSCI), pp401-407,13-14 October 2017.