International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

ENHANCEMENT IN AES ALGORITHM

Aakash[1], Deepak Beniwal[2]

[1]U.G Student, Department of Computer Science Engineering, Dronacharya college of Engineering, Gurugram, Haryana, India.
[2]U.G Student, Department of Computer Science Engineering, Dronacharya college of Engineering, Gurugram, Haryana, India.

---***---

Abstract: *The paper is primarily concerned with the data security issues faced during sending the data over the internet. The issues can be avoided with the proposed algorithm. Enhancement in AES algorithm with custom configurable encryption. The new layer of security is based on Caesar Cipher Encryption Algorithm. Although the algorithm is highly vulnerable to few attacks, our manipulation in the algorithm are tailor made to deny those attacks completely. The user has no idea that Caesar cipher is used for securing the data. Moreover, the key is changed according to each letter in the message, 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. Everyday, users establish a connection and communicate and shares a huge volume of information with others. This information includes financial and legal files; medical information; automatic and internet banking; phone conversations, pay-per-view television and other e-commerce transactions and sharing information with others. 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, it is presumed that AES might have been broken without the attack being known to us. Thus, an new layer is add to increase its security level.*

Keywords :- Cryptography, AES(Advanced Encryption Standard), Caesar cipher.

I. INTRODUCTION

Encryption is the process to secure the data or information. In this plain text is converted into the ciphertext. Most of the effect done in securing the information is done by the cryptography. In this technique the data is changed into a specific code, so that we can transmit it through the network (mainly it is internet) so that no one can read our data.

Encryption is generally categories in two ways: - Symmetric key and Asymmetric key encryption. One of the algorithms which is symmetric key encryption algorithm, is most widely used at present in the form of Advanced Encryption Standard (AES). AES is found at least around six times faster than triple DES. Another solution is needed for the DES because its key size was too small. Computing it with more power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome with this drawback, but it was found to be sluggish.

AES uses iterative cipher rather than Feistel cipher and it is based on 'substitution-permutation network'. It has a series of linked operations, some of which replace inputs by specific outputs is known as Substitutions and others by shifting bits which is also known as permutation. It performs all its calculation on bytes rather than bits. AES with 128-bit key (16 bytes) uses around 10 cycles, 192-bit (24 bytes) keys uses 12 cycles for it and for 256-bit (32 bytes) keys uses around 14 cycles. Each of these rounds uses a different 128-bit (16 bytes) round key, which is calculated from the original AES key. For encryption it uses byte substitution (Sub Bytes), shiftrows, mixcolumns and addroundkey respectively. For decryption of it is same as the encryption process but in the reverse order. AES has been widely adopted and supported by both in the hardware and software. No practical cryptanalytic attacks against AES have been found but security is only guaranteed only if it is correctly implemented and proper use of the keys is done. Each and everything has its own advantages and disadvantages, same case applies to AES as well. Cryptanalysts have found a flaw in AES that it can crack secret keys faster than before. Key scheduling of AES –192 and AES –256 are weak because they have been attacks on these variants when used in a network. The cipher AES –256 is used in SSL/TLS across the network. It's still the top cipher used in government organizations. In theory it's not crack able since the combination of keys are massive. We should not use AES –256 for building a hash function. National Security Agency recommends that 128-bit key (16 bytes) for encryption. AES –256 is weaker than AES –128. Even a supercomputer would take 149 trillion years to crack the 128 –bit AES. This is more than the age of the universe (around 13.75 billion years). Caesar Cipher is mono-alphabetic cipher where each alphabet(letter or text) of plaintext is substituted by another alphabet(letter or text) to form the ciphertext. It is made possible because of replacing each alphabet by another alphabet which is known as shifting by some fixed number between 0 and 25. A number between 0 and 25 becomes the key of encryption. It is not a secure cryptosystem because there are only 26 possible keys to guess. A hacker (mainly cryptanalytic) can compute an exhaustive key search with a limited computing resources.

2. LITERATURE SURVEY

Neenu Shaji et al. (2015) in their paper titled " Design of AES architecture with area and speed tradeoff" have discussed about the work adresess and the area optimization of AES. It is done with the help of by mapping the transformation to the lower datapath hardware and by using the iterative loop architecture. They achivied the tradeoff between the speed and are area, without using the BRAM. From the obtained performances, they concluded that their purpose of AES Architecture is suitable to be used in resource constrained systems is fulfilled [7].

Rizky Riyaldhi et al. (2017) in their paper titled " Improvement of Advanced Encryption Standard Algorithm with ShiftRow and S-box Modification Mapping in MixColumn " they have successful optimize the Advanced Encryption Standard by the help of reducing shiftrows circular process and S-Box modification for MixColumn transformation. Their achieved a percentage improvement of 86.143% avergely(decrement by three millisecond) on encryption process and 13.085% (decrement by two millisecond)averagely on decryption process. The purpose of their method is to consume bigger memory to store the two modified S-box map and array Shiftrow map[5].

Karim Shahbazi et al. (2017) in their paper titled " Design and implementation of an ASIP based cryptography processor for AES, IDEA and MD5 " have discussed about a new ASIP-based crypto processor for AES, IDEA and MD5 designed. The instruction set must have both of the general purpose and specific instructions for the above cryptographic algorithms. A software developer can select its own encryption method. Maximum achieved frequency is about 166.916 MHz . Their new design is also having higher throughput than other ASIP-based crypto processors. The performance of design is entirely dependent upon the selection of specific instructions by the user. This will allow the users to select an encryption algorithm of their desire [6].

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 encryptionis 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.[3]

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 the operation (encrypt/decrypt) with low asset used and the high throughput of 38.65Gbps.[2].

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].

Sreyam Dasgupta, Pritish Das (8 june 2019) in their paper "Extended AES Algorithm with Custom Encryption for Government-level Classified Messages" have created a new alogrithm by combining the AES algorithm and ceaser algorithm. They provided a new security of layer which is unknown to the peoples and the user. That make it unbreakable theoretically without the help of inside. The drawback is proposed system works only on text files and not on the alpha numeric. [8]

2.1. Limitation of the existing system.

AES is one of the most secured encryption processes. In theory, it is not crack by anyone. But it is suspected that it has been cracked already, without anyone knowing about it. That's why different algorithms are being implemented to make it more secure. One of the primary reasons of such suspicion is due to the length of the key not being long enough. AES uses too simple algebraic structure which is very hard to implement with software. Each and every block is encrypted in the same way. AES in counter mode is complex enough to take implementation in software for both performance and security into considerations. The way of handling different types of attacks, by AES is explained below. The traditional of Caesar Cipher encryption is common and it can be easily broken by hacker.

ES keys are of different size, the minimum length being 128 bits. It can provide 2^128 possible keys. Using brute force attack on this domain of keys is going to prove highly ineffective. Even if the original key is found after searching half the key set, it will still require searching 2^127 keys. Brute-Force attack is very effective in breaking Caesar cipher encryption. Only 25 possible keys are there. Each one of them can be tried and the key which leads to useful word meanings can be chosen. From there, all other messages can be broken using that key.

A.2 Mathematical Attack Multiplicative inverse of a given number in the Galois finite field is calculated and is used for the generation of S–box substitution table in AES. This helps in stopping all types of linear and differential cyber-attacks.

A.3 Timing attack AES is susceptible to timing attacks. Timing attacks involve implementation level attacks on the algorithms which do not run in a fixed time. The S-box substitutions in AES is dependent on the substitution table given to it at the time of creation. S–box substitutions may be removed but it will slow down the AES cipher, which is also not desirable.

A.4. Frequency analysis Frequency Analysis is very useful in breaking Caesar cipher encryption. The frequency of letters in ciphertext is compared with the English letter frequencies.

3. PROPOSED WORK

3.1. Proposed system overview

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 2 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.

In this application we can change a complete file at a time or even a image can also be converted into the ciphertext there are option present to do that or even we can send data by hiding in into the image and then we can encrypt that image also.

3.2. Advantages of AES

Since this algorithm uses a different key for every different word, frequency analysis, which is a major way of breaking Caesar cipher, is not going to work and we know that it can be implemented in both hardware and software, it is most robust security protocol till now. Counting the frequency of letters in each word to find the key is not going to work here.

Another relatively easy way of breaking Caesar cipher is using brute-force by trying all the alphabets and seeing which letter makes sense. Now for one key it requires at most 25 tries. But when two keys are used it requires 25^2 tries for breaking the cipher. Hence for n different keys, it requires25^n tries.

4. RESULT AND DISCUSSION

First we have to enter the text which we want to send.

Plain Text	**Gerrard**
Ciphertext 1 (after Caser encryption)	V/7Z6+Q2jR+AxTKOUZ
Ciphertext 2 (after AES encryption)	wJkWGKIR8OD0bFdc99nAGb6pOGU+uDVUn7qADWVH4DhpO
Ciphertext 3 (after AES decryption)	V/7Z6+Q2jR+AxTKOUZ
Ciphertext 3 (after Caser decryption)	**Gerrard**

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.

5. 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 Modification Mapping in MixColumn ", 2nd International Conference on Computer Science and Computational Intelligence (ICCSCI), pp401-407,13-14 October 2017.

[5] Karim Shahbazi, Mohammed Eshghi, Reza Faghih Mirzaee," Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5", Engineering Science and Technology, an International Journal 20, pp13 08 – 1317, 2017.

[6] Neenu Shaji, Bonifus P.L," Design of AES architecture with area and speed tradeoff ", International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST), PP1135-1140, 2015.

[7] Sreyam Dasgupta, pritish Das "Extended AES Algorithm with Custom Encryption for Government- level Classification Messages", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue - 8,June, 2019.