IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. VI (Nov – Dec. 2015), PP 75-82
www.iosrjournals.org

Prevention of Cheating Message based on Block Cipher using Digital Envelope

[1]Sanyasamma, [2]Koduganti Venkata Rao
[1]M.Tech Scholar, Computer Science Department, VIIT College of Engineering
[2]Professor, Computer Science and Engineering Department, Vignan's Institute of Information Technology

***Abstract**: Quick assessment of advanced information trade happens as of late. Because of that security of data is much critical in information stockpiling and transmission process. That implies there is a need to shield the information or some message from an assailant that is miscreant. An advanced envelope (encryption) is what might as well be called putting our message into a fixed envelope to give security and imperviousness to altering. Also, is the most guaranteeing procedure which gives key security highlight like uprightness, validation, non-renouncement, protection. This Paper depicts a configuration of successful Digital Envelope furthermore giving security to information correspondence by AES calculation for encryption and decoding so the miscreant implies aggressor cannot get to the our touchy data, here only message by which anticipation of deceiving a message should be possible.*
***Keywords:** Advanced Encryption Standard (AES), Block Cipher, Digital Envelope, FIPS, NIST, Rijndael,*

I. Introduction

Because of expanding utilization of PCs, now a day security of computerized data is most essential issue. Gatecrasher is an undesirable individual who peruses and changes the data while transmission happens. This movement of interloper is called interruption assault. To maintain a strategic distance from such assault information may be encoded to a few configurations that is garbled by an unapproved individual. In the previous couple of years the security and trustworthiness of information is the principle concern. In the present situation all the information is exchanged over PC systems because of which it is defenceless against different sorts of assaults. To make the information secure from different assaults and for the honesty of information we must scramble the information before it is transmitted or put away. Cryptography is a strategy for putting away and transmitting information in a structure that just those it is planned for can read and process. It is an investigation of encoding so as to secure data it into an indiscernible arrangement. It is a compelling method for securing touchy data as it is put away on media or transmitted through system correspondence ways. Reason for cryptography:

1. Validation: The procedure of demonstrating one's personality. It is another piece of information security that we experience with regular PC use. Simply think when you sign into your email, or blog account. The basic sign-in procedure is a type of validation that permits you to sign into applications, records, organizers and even a whole PC framework. Once signed in, you have different given benefits until logging out. Some framework will scratch off a session if your machine has been unmoving for a sure measure of time, requiring that you demonstrate confirmation by and by to re-enter. The straightforward sign-on plan is additionally actualized into solid client confirmation frameworks. Be that as it may, it obliges people to login utilizing various elements of confirmation. Non-renouncement: In this, the recipient ought to know whether the sender is not faking. For instance, if assume when one buys something on the web, one ought to make sure that the individual whom one pays is not faking.

2. Respectability: Many a times information should be redesigned however this must be finished by validated individuals.

3. Security/classification: Ensuring that nobody can read the message aside from the expected collector. Encryption is the procedure of clouding data to make it confused without exceptional learning. Encryption has been utilized to ensure interchanges for quite a long time, yet just associations and people with a phenomenal requirement for mystery had made utilization of it. in any case, different methods are still expected to make interchanges secure, especially to check the respectability and validness of a message.

II. Related Work

AES is mainly advance version of data encryption standard (DES). Effort towards developing the AES was started by NIST from January 1997. AES is a symmetric key encryption algorithm, and NIST made a worldwide public call for the algorithm to succeed DES. Initially 15 algorithms were selected. After detail analysis they were reduced down to 5 algorithms namely MARS, RC6, Rijndael, Serpent and Twofish. After complete analysis Rijndael is selected as the algorithm for AES. Characteristics of Rijndael are: High security, mathematical soundness, resistance to all known attacks, high encryption speed, worldwide royalty free use, suitability across wide range of hardware and software.

1. D. S. Abdul. Elminaam et.al., (2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices in their paper named "Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices." following points are concluded by him from his experimental result. 1. If packet size is changing with or without transmission of data using various WLANs protocols and different architectures. It was concluded form the result that Blowfish and AES has better performance than other common encryption algorithms used, followed by RC6. Worm holes are present in the security mechanism of DES and 3DES; Blowfish and AES do not have such worm holes any so far [4].

2. Energy Consumption of RC4 andAES Algorithms in Wireless LANs is analyzed in the year 2003 by P. Prasithsangaree and his collegeue P. Krishnamurthy. RC4 and AES encryption algorithms performance evaluation is made by their research. The matrics for such evaluation are as follows: CPU work load, encryption throughput, key size variation and energy cost. Experimental results conclude that for encrypting large packets the RC4 is energy efficient and fast. However, for a smaller packet size encryption AES was more efficient than RC4.

3. Seyed Hossein Kamali, Reza Shakerian, MaysamHedayati, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard (AES) Based Algorithm for Image Encryption" (2010) [26] The authors proposed an enhanced model of Advanced Encryption Standard to possess good level of security and better range of image encryption. The modification process can be carried out by adjusting the Shift Row Transformation. As the result shown, that the comparison has been made in between the original AES encryption algorithm and the modified algorithm which produces very good encryption results focusing towards the security against statistical attacks.

III. PROPOSED WORK

AES, a symmetric key encryption calculation, made a World Wide open require the calculation to achievement DES. At first 15 calculations were chosen, then they were lessened to 4,RC6, Rijndeal, serpent and Two-angle, all of which were iterated square figures. The 4 finalists were all resolved to be qualified as the AES. The structure of AES is as per the following:

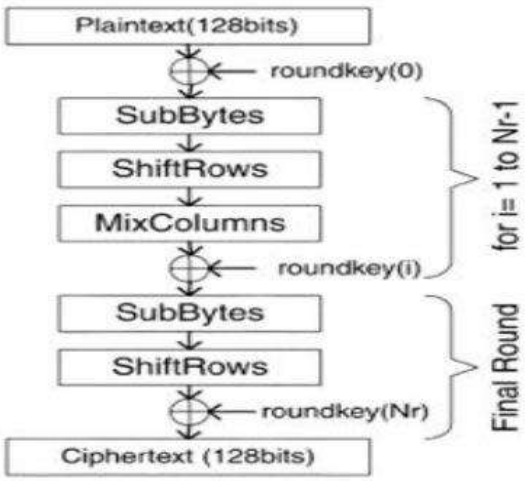


Figure1: structure of AES Algorithm

Here encryption and unscrambling should be possible in a manner that the assailant or the miscreant ought not to uncover our touchy data that is our mystery message. Keeping in mind the end goal to perform this we are doing the key development.

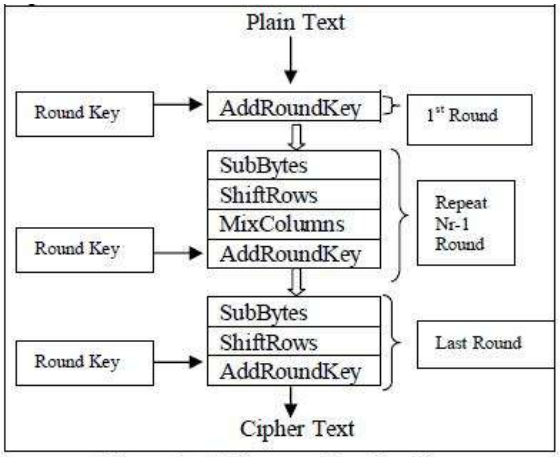


Figure 1: AES encryption algorithm

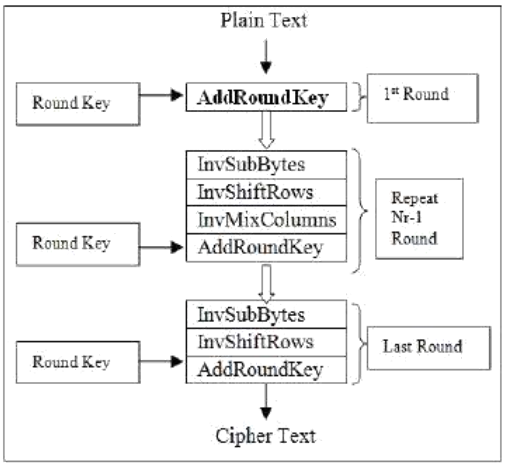


Figure 2: AES decryption algorithm

IIII. IMPLEMENTATION

The algorithm is based on AES Key Expansion technique.

AES Key Expansion technique in detail.

A. AES Key Expansion Pseudo code for AES Key Expansion: 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 first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k0 to k15). The first four bytes (k0 to k3) become w0, the four bytes (k4 to k7) become w1, and so on.

- The rest of the words (wi for i=4 to 43) are made as follows

C. Steps Involved

a) Key Selection: The sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k[0],k[1]...k[15]. Where each block is 8bits long (8*16=128 bits).

b) Generation of Multiple keys: The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a one time process; these expanded keys can be used for future communications any number of times till they change their

initial key value.

c) Encryption: Encryption is done in spans, where we process 16 pixels in each span. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey.

d) Decryption: The decryption process is similar as encryption, but we use Inverse SubByte Transformation 1. If (i mod 4) != 0, wi=wi-1 xor wi-4. 2. If (i mod 4) = 0, wi=t xor wi-4. Here t is a temporary word result of applying SubByte transformation and rotate word on wi -1 and XORing the result with a round constant.

B. Modifications in AES Key Expansion Certain changes made in the above key expansion process improves the encryption quality, and also increases the avalanche effect. The changes are

1. The Rcon value is not constant instead it is being formed from the initial key itself, this improves the avalanche effect.

2. Both the s-box and Inverse s-box are used for the Key Expansion process which improves non-linearity in the expanded key and also improves the encryption quality.

3. We do not use the S-box and Inverse S-box as such for this algorithm; instead we perform some circular shift on the boxes based on the initial key this improves the key sensitivity.

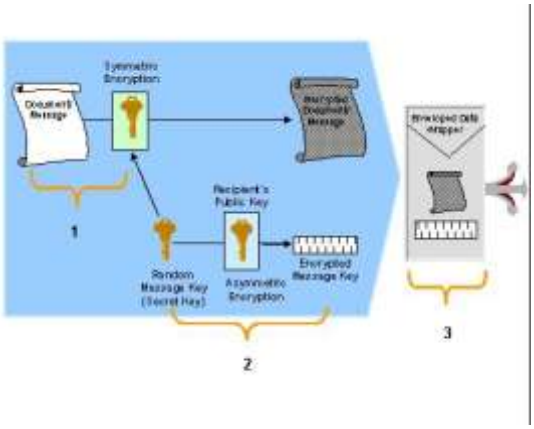
The above changes in the algorithm can be represented as

a) Formation of Rcon values
Rcon [0]=key[12:15]; Rcon [1]=key[4:7];
Rcon [2]=key[0:3]; Rcon [3]=key[8:11];

b) Using Inverse S-Box for key expansion The _temp' value used in the algorithm is formed as temp = SubWord(RotWord(temp)) XOR InvSubWord(Rcon[i/4]); Where InvSubWord: InverseSubByte transformation table value

c) Shifting of S-box and Inverse S-box Sbox_offset = sum(key[0:15])mod256; Inv_Sbox_offset = (sum(key[0:15])*mean(key[0:15]))mod256; The initial key is represented as blocks key[0],key[1],..,key[15]. Where each block is 8bits long (8*16=128 bits)

Digital Envelope



The following explains what happens at each step:

a) The message is encrypted using symmetric encryption. Typically, a newly generated random message key (secret key) is used for the encryption.

Symmetric encryption means that the same key is used for both encryption and decryption (a secret key). Anyone wanting to decrypt the message needs access to this key.

b) To transfer the secret key between the parties, the secret key is encrypted using the recipient's public key.

c) The encrypted document and the encrypted message key are packed together in a single datapacket to save or send to the intended recipient. We use a digital envelope to protect a digital document from being visible to anyone other than the intended recipient. The following are possible reasons for using digital envelopes:

a) Sending confidential data or documents across (possibly) insecure communication lines
b) Storing confidential data or documents (for example, company-internal reports)

To create a digital envelope, we need access to the intended recipient's public key. How to obtain access to the public key depends on the public-key infrastructure of our organization. We also need the digital document that we want to protect.

Let us see the **creation of the digital envelope** as shown below

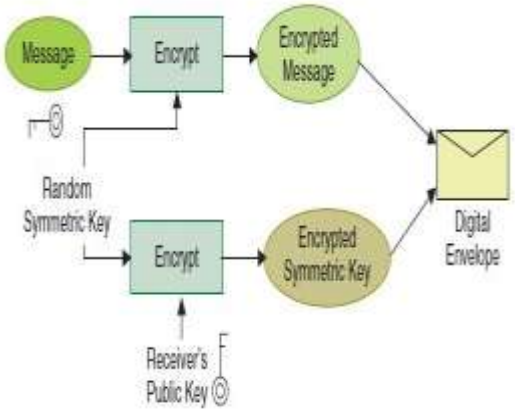
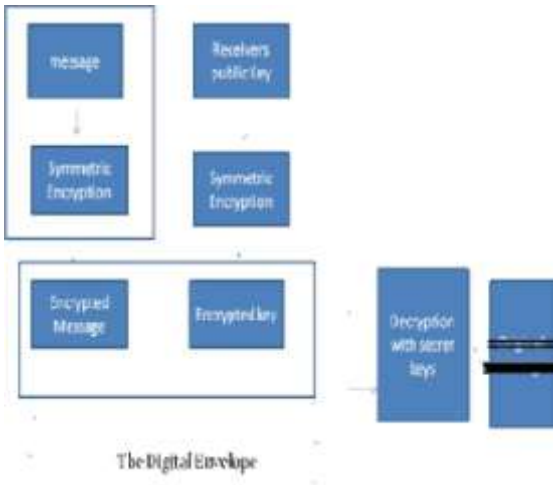


Figure: Digital Envelope Creation



METODOLOGY:

Step 1: When the sender wants to send the massage, that should be encrypted with secret key that is symmetric encryption using AES algorithm.

Step 2: The receiver's public key also encrypted with that secret key which can be shared by both sender and receiver.

Step 3: Both encrypted message and encrypted key are packed in a single packet, to protect our data we are using the Digital Envelope, which is to be sent to the receiver.

Step 4: At the receiver side (no need to use symmetric key encryption, can use asymmetric encryption for the secret key transmission) decryption will be performed to get the original message.

After the successful transmission of the massage we can see the performance as shown below

The structure is as follows

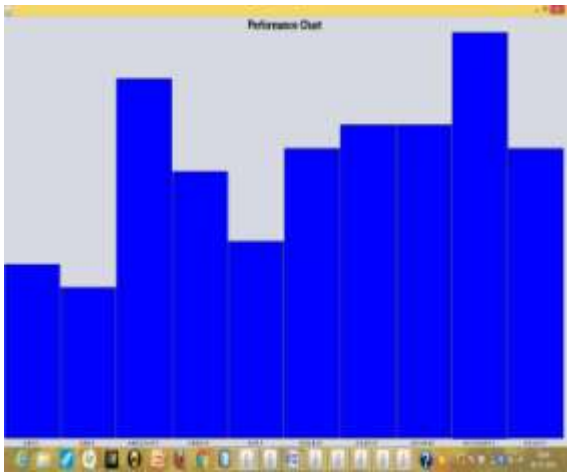


Figure: Performance Chart

The Results for the cheater is as given below.

e) CONCLUSION

The proposed algorithm provides high encryption quality. There is right now no confirmation that AES has any shortcomings making any assault other than comprehensive hunt, i.e. animal power, conceivable. Indeed, even AES-128 offers an adequately extensive number of conceivable keys, making a comprehensive quest unreasonable for a long time. In this venture as we are performing the symmetric, and a square figure calculation alongside the advanced envelope henceforth it is impractical for the aggressor called miscreant to get to the conveying data that is, message between the customer and server, this is, the way we can keep a message from tricking

f) FUTURE WORK

The same algorithm can again be modified to be used for Image Encryption and Decryption. Various algorithms were developed for image encryption like Image Encryption Using SCAN Patterns and Image Encryption Using Combinational Permutation Techniques. But they were mainly developed for single application scenario and hence had its own limitation when considering a general Image security application. In the digital envelope the public encryption can also be applicable.

References

[1] P.Karthigaikumar, Soumiya Rasheed, ―Simulation of Image Encryption using AES Algorithm‖, IJCA Special Issue on ―Computational Science - New Dimensions & Perspectives‖ NCCSE, 2011, pp 166-172.

[2] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma, ― Analysis and Comparison between AES and DES Cryptographic Algorithm‖, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012, pp 362-365

[3] Irfan AbdulGaniLandge, ―Implementation of AES Encryption and Decryption using VHDL‖, International J. of Engg. Research &Indu. Appls. (IJERIA). ISSN 0974-1518, Vol. 4, No. III (August 2011), pp 395-406.

[4] Duquesne S and Tanja Lange (2006), "Arithmetic of Hyper elliptic curves" from "Handbook of Elliptic and Hyper elliptic curve

cryptography" by Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, Taylor and Francis Group, Florida, 2006.
[5] Avanzi R M and Tanja Lange (2006), "Introduction to Public key cryptography" from "Handbook of Elliptic and Hyper elliptic curve cryptography" eds. Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, TaylorandFrancis,Florida, 2006.
[6] Burton S. Kaliski Jr., Cetin K.Koc and ChrisofPaar, (2002), "Cryptographic Hardware and Embedded systems", 4th International workshop, Bedwood shores, CA, USA, 2002.
[7] AES (2001), U.S. Department of Commerce / National Institute of Standard and Technology, FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), November 2001 from http://csrc.nist.gov/encryption/aes.

Bibliography

J. Sanyasamma has received her BTech degree from Nova Institute of Technology for Women's. She is currently pursuing her M.Tech degree from Vignan's Institute of Information Technology, Visakhapatnam. Her areas of Interest are Software Engineering, Networking.

Koduganti VentakaRao is working as Professor Vignan's Institute of Information Technology, Visakhapatnam. He has experience for over 22 years in teaching field. He has published 30 papers in his area of expertise. His areas of interest are Security and Cryptography, Key Distribution, Cognitive Sciences.