AES algorithm using advance key implementation in MATLAB

Chaudhary Saifurrab[1], Saqlain Mirza[2]

[1] M.Tech. Scholar department of ECE, Al-Falah University, Faridabad, Haryana (India)

[2]Asst. professor [1]department of ECE, Al-Falah University, Faridabad, Haryana (India)

---***---

Abstract- *During the last decade information security has become the major issue. The encrypting and decrypting of the data has been widely investigated because the demand for the better encryption and decryption of the data is grdually increased for getting the better security for the communication between the devices more privately. The cryptography play a major role for the fulfilment for this demand. The purpose of this paper is to provide the better as well as more secure communication system by enhancing the stregth of Advance Encryption Standard (AES) algorithm. AES algorithm was known for providing the best security without any limitations. But in recent days there are some methods are found by cryptanalyst that can crack the AES algorithm.So we need some improvement in the AES algorithm. In this paper we enhance the key (256-bit) by the advance method and algos by which the key size of AES is look like the size of 512-bit. By enhancing the key size see that the more improvement in security in the encrypted data which is provided by us for the communication between the devices. Due to this provision it becomes more resistent to linear and diffrential encrypt analysis providing high security. All as in[1],[2],[7],[10],[11] and [14] in prefrences.*

Key Words: Security, cryptography, AES-(128,192, 256), proposed AES, AES of 512 bits, etc.

1. Introduction

Network security has become very important as we spend more and more time being connected in the network. The security attacks such as unauthorized reading of a message of files. The most publicized method for attacking on communication is virus attack. As in [1], [5],[11], and [13] in prefrences. That not only attack on our communication system but also it can make changes in our data and it also slows down our system. So we need to introduce the encryption technique that can fulfill our need of security. The security of communication can be achieved by using cryptographic algorithms such as DES, Two fish, AES and many others. The data encryption standard (DES) was the first encryption standard which was suggested by NIST as the first encryption standard of the world. DES has 64-bit key size and 64-bit piece size. But unfortunately it was cracked by the hackers after some years. As in[10] in prefrences. When DES was cracked then we need to create new encryption standard. 3DES is the improved version of the DES. It has 64-bit piece size and 192-bit key size. In this standard encryption is like DES connected 3 times to expend the encryption level and normal safe time. As in[7], [11] and [13] in prefrences. The AES is the advance encryption standard algorithm that been in use since 2001 since it provide high level security and it can be easily implemented. The AES has 128-bit block size but has 3 different key sizes of 128, 192,256-bits. As in [5], [11], [13] in prefrences.

2. Comparison between most popular Encryption Algorithms

There are many encryption algorithms used to provide the security of communication systems. The complexity of all encryption algorithm techniques differs from one another. Here we compare these techniques with respect to their complexity and other parameters. As in[1] in preferences.

Algorithm	Block size	Key size	Rounds	Status
DES	64-bits	56-bits	16	Cracked
RC2	64-bits	128-bits	16 mix 2 mashing	Cracked
RC4	Variables	Variables	unknown	Cracked
BOWFISH	64-bits	128-bits	16	Not cracked yet
TWOFISH	128-bits	(128,192,256)-bits	16	Not cracked yet
3DES	64-bits	(112,168)-bits	48	Not cracked yet
AES	128-bits	(128,192,256)-bits	10,12,14	Not cracked yet

3. AES algorithm by using advance key implementation

The advance encryption standard algorithm is the most popular algorithm till now. It has 128-bits block size and (128,196,256)-bits key size. The cryptanalyst have found some methods by which crackers can cracks the AES. So we need to improve the key size of AES algorithm by using advance bit implementation algorithms that changes the size of key from 256-bits. The enhanced size can look like the 512-bits.

4. Methodology-

In this section of our article we will se the methodology for the working of system for the prposed advance encryption standard (AES) algorithm.

Here we explain the all steps for the system of our proposed AES algorithm.

we see the flow chart for the encryption and decryption process and other steps of the proposed system.

In which we see the working of the proposed system. To communicate with any user enters a message to the user for checking the authenticity.

The device will check the authenticity of the user by using RSA algorithm.

It checks both the authenticity of users using different algorithm.

If the user is authorized then the message will proceed for encryption stage.

In case of unauthorized user no further process will proceed.

For authorized users the encryption process has started by using proposed AES algorithm technique (i.e. 512 bit key encryption) Encrypted data get transmitted to receiver.

At the receiving end when the receiver receives the encrypted data it starts the Symmetric decryption process.

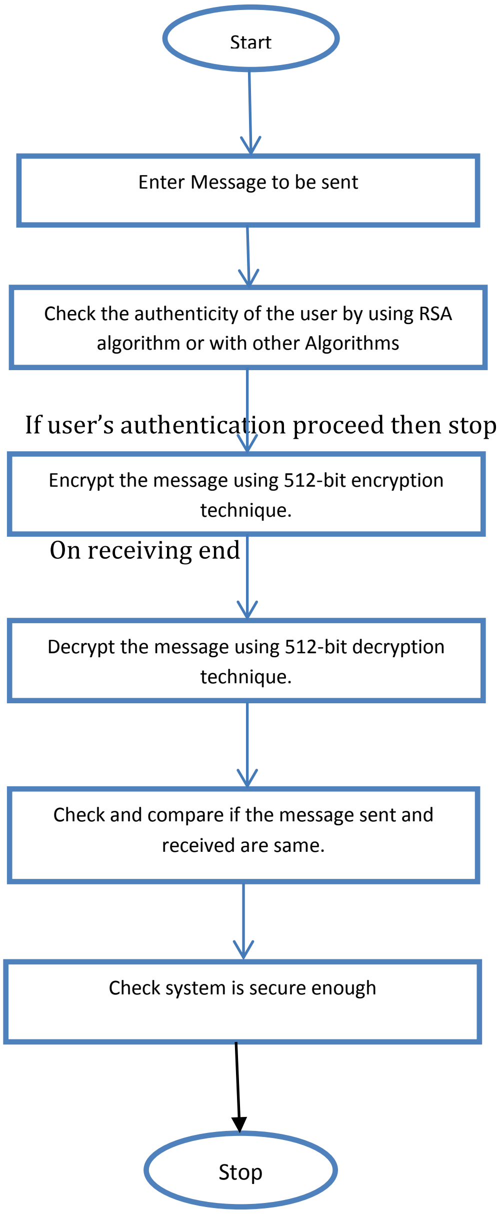
Now the system will check that the received message is matching with transmitted message or not.

In case of message not matched request message to the user is sent.

At the next step system security is checked against virus, spam, and any internal and external threats.

If the system is not secure then check that where problem has occurred.

If the system is secure then the process is stopped and our communication is processed securely without any problem.



5. Working of the proposed AES

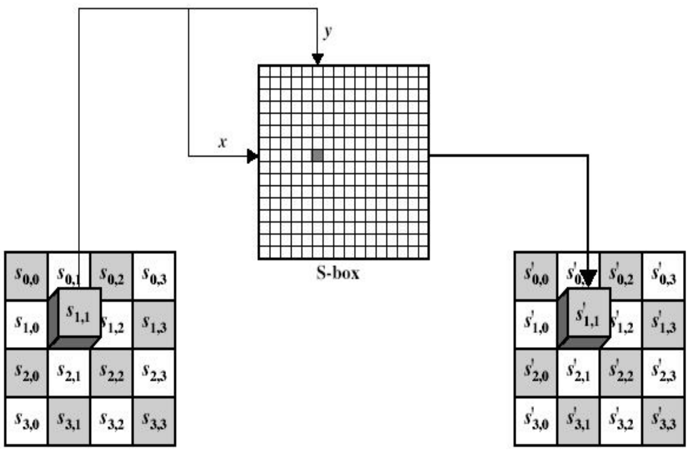
There are many steps for Encryption and decryption.

5.1 The steps for Encryption of data

The steps for the Encryption are given below. All the steps of working of AES as [1], [5],[7],[9],[10],[11],[13] and [15] in prefrences.

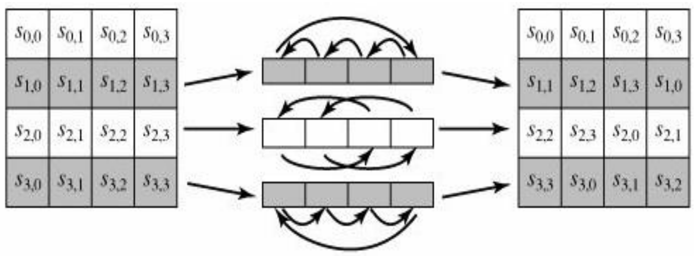
5.1.1 Byte substitution

The proposed algorithm has key size of look like 512-bits by using advanced key implementation the 512-bits input plaintext is organized in the array of 64 bytes. That can be obtained in byte substitution. This process is used for achieving the security according to diffusion-confusion Shannon's principle for the cryptographic algorithm design. The example for the s-box transfrmation is given below. As in [11],[13] and [15] in prefrences.



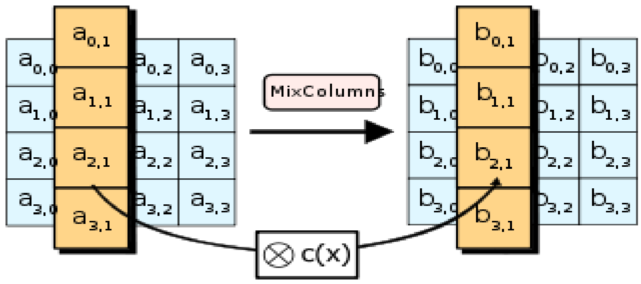
5.1.2 Shift row

In the next step we perform row shifting process in which we don't touch the first row. For other rows we perform the operation as given in figure below. As in [11],[14] in prefrences.



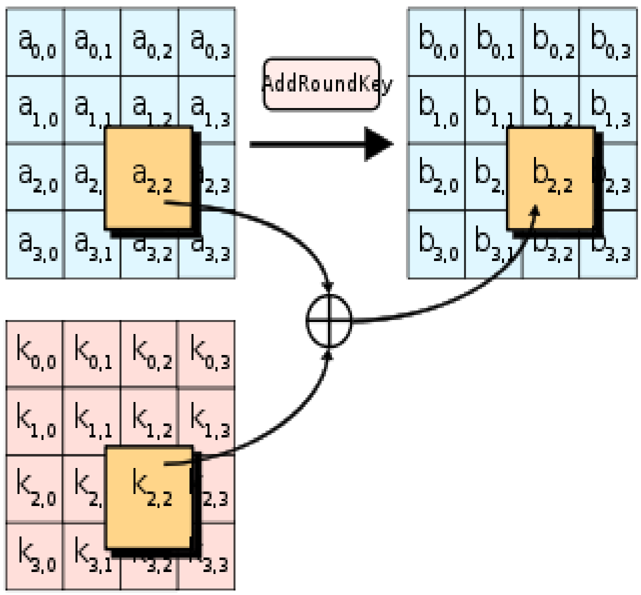
5.1.3 Mix column

In this step each column of the state is multiplied with the fixed polynomial C(x). In this step matrix multiplication is composed using multiplication and addition of the given data. Here addition is done using simple XOR operation and multiplication is irreducible polynomial. As in [5],[11] and [14]



5.1.4 Add round key

In this step the sub byte is combined with the state. For each round the sub key is derived from the main key on the basis of Rijndael key schedule. Each sub key is the same size as the state. We do the XOR operation with the sub byte key for the specific round. The example for this step is given below. As in [9],[10],[11] and [13] in prefrences.



5.1.5 Add cipher text

The cipher text is used only used for the speeding up the execution process of the data. In this step we combine the sub byte and mix row step with the shift row by transforming them into a sequence of table lookup. As in [1],[5],[7],[10],[11] and [13] in prefrences.

5.2 Steps for decryption of received data

For decrypting the received data at the receiving end we do the same steps like encryption but in inverse order of encryption process. Cipher text can be obtained as the input with key but the original data can be obtained by using decryption process. The algorithm is implemented in the MATLAB. As in [9],[10],[11] and [13] in prefrences.

6. Performance analysis

In which we check the performance of the proposed method with the old AES algorithm methods. In which we check that the performance of processor on the operation of encryption and decryption, time taken for full operation and parameters.

Parameters	AES-128,256 bits	Proposed AES algorithm
Key size	128,256-bits	Look like 512-bits
Data block size	128-bits	128-bits
Rounds	10,14	10
Time to encrypt 128-bit character message	Approximately 30-50 seconds	Approximately 23-36 seconds
Security	Less as compare to proposed AES	More than AES 128,256-bits
Processor required	More amount	Less as compare to 128,256-bits

Here we see that old AES algorithm has the key size up to 256-bits. But we have change the key size to like 512-bits. But the block size is same as the old algorithms of Advance encryption standard (AES). In our proposed AES algorithm there are 10 rounds only for both encryption and decryption process but in old algorithm we have 10-14 rounds for the encryption and decryption. Because of this our time is become less as compare old AES algorithms due to less round required. Because of large key size as compare to AES 128,192 and 256-bits the security is also improved. Here processor use for processing of encryption and decryption is also improved means our proposed algorithm use less amount of processor as compare to AES (128,192,256) bits.

Conclusion

As we can see that our proposed encryption algorithm is better than the old AES algorithms. It takes less time as compare to AES-128,256-bits algorithms. AES 128-bit algorithm is widely used in most of the devices now a day. AES 128-bit has128-bit block size and 128-bit key. But in proposed algorithm the block size is of 128-bits but the key size is of 512-bits. Hence, due to enhanced key size it takes less time as compare to AES 128,256-bits key size A. It also consumes less amount of the processor as compare to AES 128,256-bits algorithms

Acknowledgements

I am very profoundly grateful to my guide asst. professor Mr. Saqlain Mirza for his expert guidance and continuous encouragement throughput to see that the project rights its target. Without his expert guidance I couldn't reach to my target. At the end I am very thankful to my guide to giving me his valuable time for project.

References

1. Obaida Mohammad Awad Al-Hazaime , a new Approach for complex encryption and decryption ofdata , Al-balqa Applied University, AL-Huson University College, Irbid, Jordan.2011
2. Rohan Rayarikar, Sanket Upadhyay, Priyanka Pimpale, "SMS Encryption using AES Algorithm on Android", IJCA, Volume 50- No.19, 2012
3. Hassan Mathkour, GhazyAssassa, A. Al-Muharib, A. Juma, "A Secured Cryptographic Messaging System", International Conference on Machine Learning and Computing IPCSIT vol.3, 2011.
4. Zirra Peter Buba and Gregory MakshaWajiga, "Cryptographic Algorithms for Secure Data Communication", International Journal of Computer Science and Security (IJCSS), Volume (5),2011
5. Abidalrahman Moh'd and Yaser Jararweh, "AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evolution", IEEE Transaction 2011
6. H. Mohan, R. Raji "Performance Analysis of AES and MARS Encryption Algorithms". International Journal of Computer Science Issues *(IJCSI)*, Vol. 8, issue 4. 2011.
7. S.Radhika, A.ChandraSekar, "AES Algorithm Using 512 Bit Key Implemented For Secure Communication", GJCST, Vol. 10, 2010.
8. Nikolas Bardis, KonstantinosNtaikos, "Design of a Secure Chat Application based on AES Cryptographic Algorithm and Key Management"2009.
9. J. Daemen and V. Rijmen, the Design of Rijndael: AES- The Advanced Encryption Standard"2009.
10. NIST, —Advanced Encryption Standard, FIPS PUB 197, pp. 1-5, November 2001.
11. J. Daemen and V. Rijmen, —The Block Cipher Rijndael,|| Lecture Notes in Computer Science, vol.1820, pp.277-284, Berlin: Springer-Verlag, 2000.
12. S.Lucks, Attacking seven rounds of Rijndael under 192-bit and 256-bit keys", pp 215-229, April 2000.
13. J. Daemen and V. Rijmen, the Design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag, Berlin Heidelberg, 2002.
14. Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap Student, AES Algorithm Using 512 Bit Key Implementation for Secure 2011
15. Kshyamasagar Mahanta1, Hima Bindu Maringanti An Enhanced Advanced Encryption Standard Algorithm, IJATCSE, Vol. 4, No.4 Pages : 28 - 33 (2015)
16. Ashwaq T. Hashim , "A Proposed 512 bits RC6

Encryption Algorithm", IJCCCE, vol.10, no.1, 2010.

17. P.Karthigaikumar and Soumiya Rasheed (2011), Simulation of Image Encryption using AES Algorithm.