Aes Algorithm Using 512 Bit Key Implemented For Secure Communication

S.Radhika, A.Chandra Sekar

GJCST Classification (FOR) E.3

***Abstract*-The main aim of this paper is to provide stronger security for communication over the Internet by enhancing the strength of the AES algorithm. Rijndael's algorithm was selected as the Advanced Encryption Standard. The AES algorithm was believed to provide much more security without any limitations. But, recently some breaking methods on the AES have been found by cryptanalysts. In AES algorithm, the number of rounds involved in the encryption and decryption depends on the length of the key and the number of block columns. So, the number of rounds is increased to improve the strength of the AES. The strength of the AES algorithm is enhanced by increasing the key length to 512 bit and thereby the number of rounds is increased in order to provide a stronger encryption method for secure communication. Code optimization is done in order to improve the speed of encryption and decryption using the 512 bit AES.**

Keywords-Cryptography, Encryption, Java implementation, Decryption, AES algorithm

I. INTRODUCTION

Network security is becoming more and more important as people spend more and more time connected in a network. It involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. Security attacks include unauthorized reading of a message of file, traffic analysis, modification of messages or files and denial of service. One of the most publicized types of attack on information systems is the computer virus. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. Security involving communications and networks is not as simple as it might first appear to the novice. The expansion of the connectivity of computers makes ways of protecting data and messages from tampering or reading important. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. One solution to this problem is, through the use of cryptography. Cryptography ensures that the messages cannot be intercepted or read by anyone other than the authorized recipient. It prevents intruders from being able to use the information that they capture. Cryptography secures information by protecting its confidentiality and can also be used to protect information about the integrity and authenticity of data.

1) *Related Work*

The first open encryption algorithm, Data Encryption Standard (DES) was adopted by the National Institute of Standards and Technology(NIST) to protect the sensitive information as Federal Information Processing Standard 46 (FIPS PUB 46) in 1977 [1]. However, the shorter length of key, the complementary property and existence of weak and semi-weak keys reduce the security of DES. Differential cryptanalysis attack is capable of breaking DES in less than 2^{55} complexities. The linear cryptanalysis method can find a DES key given 2^{43} known plaintexts, as compared to 2^{47} chosen plaintexts for differential cryptanalysis. So, it was more essential to find a stronger encryption algorithm to substitute the DES.In spite of the vulnerability of DES to a brute-force attack, there has been considerable interest in finding an alternative. One approach is to design a completely new algorithm and another alternative would be the one that preserves the existing one by using multiple encryption with DES and multiple keys. Three other algorithms were found to solve the problems of DES. They are Double DES, Triple DES with two keys and Triple DES with three keys. The principal drawback of Triple DES is that it has three times as many rounds as DES and hence it is much slower. Triple DES uses a 64 bit block size which is another drawback because for both efficiency and security, a larger block size is desirable. Because of these drawbacks, Triple DES is not favorable for long term use.The Rijndael algorithm was adopted as an encryption standard, the Advanced Encryption System (AES) by the NIST as FIPS PUB 197 (FIPS 197) on November 2001 [2]. The AES algorithm was believed to provide more security than the DES [3]. The AES algorithm was designed to have resistance against all known attacks, speed and code compactness on a wide range of platforms and design simplicity [7]. AES has three variable key lengths but block length is fixed to 128 bits [2]. The three key sizes of AES are 128, 192 and 256 bits. Their number of possible keys is 3.4×10^{38}, 6.2×10^{57} and 1.1×10^{77} respectively [2]. There are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys. AES with 128-bit keys has stronger resistance to an exhaustive key search than DES.

Abou[1]t- Lecturer Dept. of Electrical and Electronics Engineering Sathyabama University Chennai-600 119 radhikachandru79@gmail.com
About[2]- Professor Dept. of Computer Science and Engineering St. Joseph's College of Engineering Chennai-600 119 drchandrucse@gmail.com

2) *Drawbacks of AES 256*

Rijndael has very strong resistance against the differential cryptanalysis and linear cryptanalysis attacks since it used Wide Trail Strategy in its design [8]. Although these linear attacks are invalid for the AES, they have been extended in several ways for recent years and new attacks have been published that are relative to them [4-6, 9-11]. The newest attack combined boomerang and the rectangle attack with related-key differentials was introduced by E. Biham, et al. in 2005 [9]. It uses the weaknesses of few nonlinear transformations in the key schedule algorithm of ciphers, and can break some reduced-round versions of AES. It can break 192-bit 9-round AES by using 256 different related keys. Rijndael inherits many properties from Square algorithm. So, the Square attack is also valid for Rijndael which can break round-reduced variants of Rijndael up to 6 or 7 rounds (i.e.AES-128 and AES-192) faster than an exhaustive key search [6]. N. Ferguson et al. proposed some optimizations that reduce the work factor of the attack [5]. So, this attack breaks a 256-bit 9-round AES with 2^{77} plaintexts under 256 related keys, and 2^{224} encryptions.

II. AES USING 512 BIT KEY

AES is a block cipher and the most popular algorithm used in symmetric key cryptography. It is a substitution-permutation network and not a Fiestel network like DES. When the number of rounds is increased in AES, the complexity of AES encryption and decryption also increases. The number of rounds (Nr) in the
AES algorithm depends on the length of main keys (Nk) and the number of block columns (Nb), i.e. Nr = Nk+Nb+abs(Nk-Nb). So, the length of the key is increased to 512 bits in order to increase the number of rounds. The structure of AES is quite simple. The input to the encryption and decryption algorithms is a single 128-bit block and the key is 512 bits. It requires the same key to be used for encryption and decryption.

1) *Implementation of AES encryption*

AES operates on a 16×32 array of bytes, termed the state. The input key for encryption is 512 bits. To represent the 512 values 9 bits are required. So each entry in S-box of AES 512 is 9 bits long. The cipher is specified in terms of repetitions of processing steps that are applied to make up rounds of keyed transformations between the input plain-text and the final output of cipher-text. The encryption procedure of AES 512 has been illustrated in figure 1.Each round in AES 512 encryption includes four different round transformations namely Substitute Bytes, Shift Rows, Mix Columns and Add Round Key. The last round of AES 512 encryption alone does not include the Mix Columns transformation.

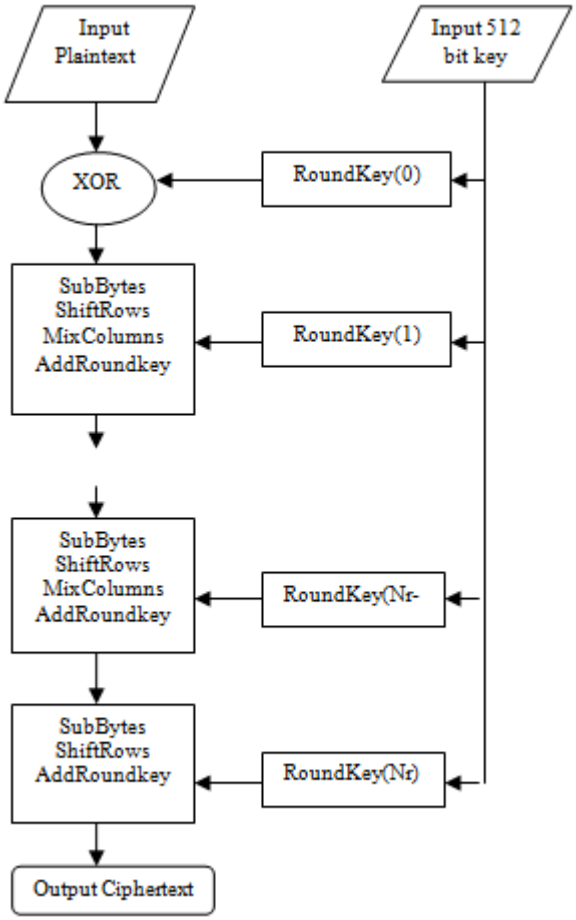

Figure: 1 Encryption procedure of AES 512

2) *Implementation of AES decryption*

A set of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key. The four reverse transformations used are Add Round Key, Inverse Mix Columns, Inverse Shift Rows and Inverse Substitute Bytes. The inverse S-box contains 512 values in its 16x32 array of bytes. Each round in decryption of AES 512 includes all the four reverse transformations except in the first round. The Inverse Mix Column transformation is violated in the first round of decryption since it does not occur in the last round of encryption. The decryption procedure of AES 512 is illustrated in figure 2.

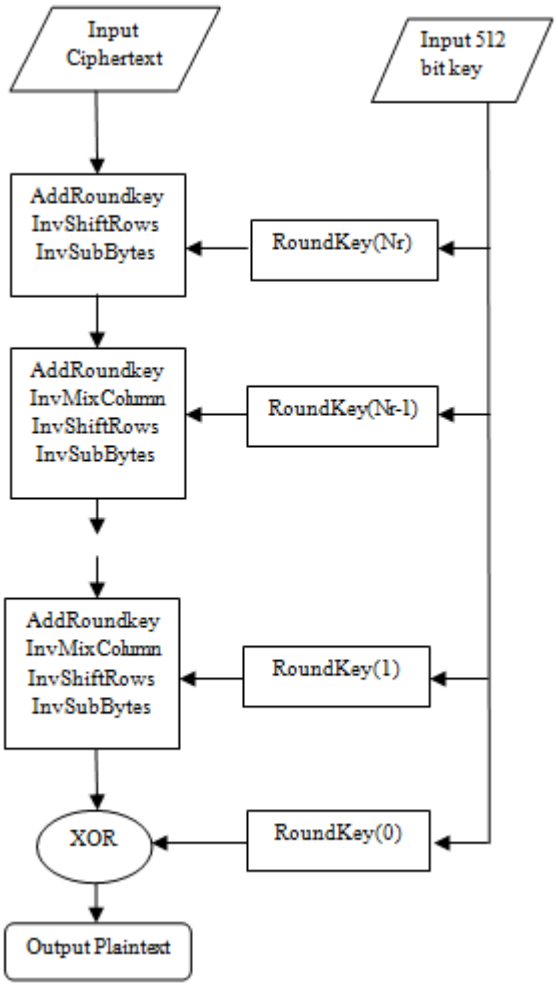

Figure: 1 Decryption procedure of AES 512

3) *Comparison of AES 256 and AES 512*

The performance of 256 bit AES algorithm is compared with the performance of AES 512 algorithm. Encryption and decryption of AES 256 is implemented to compare it with AES 512. In terms of security the 256 bit AES algorithm is weaker than the 512 bit AES algorithm. This is because the length of the key used in 512 bit AES increases the number of rounds for both encryption and decryption. But when the number of rounds increases, the encryption and decryption procedures become more complex thereby degrading the speed of the 512 bit AES algorithm. Thus there is a tradeoff between speed and security. The performance is compared in terms of time taken. The time taken for encryption and decryption of AES 256 bit and AES 512 bit are noted to measure their speed. The system time is noted at the start of encryption process and the end time, after encryption completes is also noted. The same process is repeated for decryption also to calculate the time taken for decryption.

4) *Code Optimization*

Speed and security are the most important factors that influence the transmission of any data over the network. In AES 512, a higher level of security is achieved due to the increased length of the key. But as mentioned above there is degradation in speed. It is very essential to maintain a balance between the speed and security parameters of the AES algorithm. Java implementation of AES 512 encryption and decryption is done. Code optimization techniques reduce the amount of time that a program takes to perform some task. Hence code optimization techniques are employed to improve the speed of the 512 bit AES algorithm. The source code level optimization technique is applied here. That is because avoiding bad quality coding can also improve performance, by avoiding obvious slowdowns. Creating local variables dynamic, restricting new operator, if statements are replaced with switch cases and removal of unnecessary declarations are some of the code optimizations employed.

III. Performance Evaluation

The performance of AES 512 is evaluated on the basis of two major parameters: security and speed. AES 512 has better security than the AES 256 algorithm since the number of rounds is increased. Optimization is done on AES 512 to improve its speed. We found that, the optimized AES 512 has an acceptable speed of encryption and decryption when compared to the AES 512 that was not optimized.

IV. Conclusion

AES is a new cryptographic algorithm that can be used to protect electronic data. Its security has attracted cryptographist's attentions. The methods of new attacks welled show the weaknesses of AES algorithm. When the number of rounds is increased, it improves the complexity of the algorithm making it strong against the cryptographic attacks. The length of the key is increased in order to increase the number of rounds involved as number of rounds depend on the length of the key used. Thus the increase in length of the key gives the AEs algorithm strong resistance against the new attacks and has an acceptable speed of data encryption and decryption.

V. Reference

1) U.S. Department of Commerce/NIST, "Data Encryption Standard," FIPS PUB 46-3, pp. 1-26, October 1999.
2) NIST, "Advanced Encryption Standard," FIPS PUB 197, pp. 1-51, November 2001.
3) J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag, Berlin Heidelberg, 2002.
4) H. Gilbert and M. Minier, A collision attack on seven rounds of Rijndael, Proceedings of the 3rd AES Candidate Conference, pp.230-241, April 2000.

5) N. Ferguson, J. Kelsey, S. Lucks, et al. “Improved cryptanalysis of Rijndael,” Lecture Notes in Computer 1-4244-1035-5/07/$25.00 .2007 IEEE. 221 Science,vol. 1978, pp.213-230, Berlin: Springer-Verlag, 2001.
6) S. Lucks, “Attacking seven rounds of Rijndael under 192-bit and 256-bit keys,” Proceedings of the 3rd AES Candidate Conference, pp. 215-229, April 2000.
7) J. Daemen and V. Rijmen, “The Block Cipher Rijndael,” Lecture Notes in Computer Science, vol.1820, pp.277-284, Berlin: Springer-Verlag, 2000.
8) J. Daemen, and V. Rijmen, “The Wide Trail Design Strategy,” Lecture Notes in Computer Science, vol. 2260, pp.222 - 238, Berlin: Springer-Verlag, 2001.
9) E. Biham, O. Dunkelman, and N. Keller, “Related-Key Boomerang and Rectangle Attacks,” Lecture Notes in Computer Science, vol. 3494, pp. 507-525, Berlin: Springer-Verlag, 2005.
10) G. Jakimoski and Y. Desmedt, “Related-Key Differential Cryptanalysis of 192-bit Key AES Variants,” Lecture Notes in Computer Science, vol. 3006, pp. 208-221, Berlin: Springer-Verlag, 2004.
11) J. H. Cheon, M. J. Kim and K. Kim,et al., “Improved Impossible Differential Cryptanalysis of Rijndael and Crypton,” Lecture. Notes in Computer Science, vol. 2288, pp. 39-49, Berlin: Springer-Verlag, 2002.