ISSN : 2348 - 9065 (Online)
ISSN : 2349 - 3143 (Print)
Vol. 2, Issue 1 Jan. - Mar. 2015
International Journal of Research in Electronics and Communication Technology (IJRECT 2015)

Encryption and Decryption Using AES in the Field of Network Communication based on Confidentiality

[I]Abhishek Kumar Sinha, [II]Jayaraj N
[I]M. Tech, Dept. of ECE, The Oxford College of Engineering, Bangalore, India
[II]Asst. Prof, Dept. of ECE, The Oxford College of Engineering, Bangalore, India

Abstract
Maintaining confidentiality in network communication is bigger task to achieve. Improving secure data communication many techniques are available presently. In this paper Advanced Encryption Standard (AES) algorithm is used to maintain confidentiality between users across communication channel by encryption and decryption at the transmitter and receiver respectively. To achieve privacy and security services can be configured by AES ensuring high performance. The software tools used for simulation and synthesizing the verilog code is Modelsim and Xilinx.

Keywords
Confidentiality, AES, Encryption, Decryption, Modelsim.

I. Introduction

In modern days, confidentiality is most important between users surrounded by networks. The network communication requires secured information and data to be stored in privacy manner such that the users across the channel get the required information without delay and shown in correct way without duplication. Confidentiality is the component of information security which is defined as the prevention of disclosure of any secured computer related information to unauthorized user. It is widely applicable in credit card transaction. Credit card number is required on internet for transaction between buyer and merchant. Encryption enforces confidentiality during transmission and restricting access where information is stored. Breaching can be occurred by showing the confidential information of the system, giving confidential information over telephone and selling or stealing the laptop containing sensitive and highly confidential data and information. Privacy is related to confidentiality which ensures the individual to prevent the access of unauthorized user from his personal information. It asks what information should be collected, how, who and for what purpose should use it and who will maintain the controlling rights for the information.

Various encryption algorithms are present such as RSA, DES and AES algorithms. These are classified under two categories which are symmetric and asymmetric algorithms. Symmetric algorithm consists of secret key which is used in AES algorithm. Asymmetric algorithm consists of private and public key which is used in RSA algorithm. AES is standard technique for encryption. It is used to transform plain message into a cipher or hidden message which is invisible from real world. In history, the text written in the form of hidden message was used during war. Many ciphers are Caesar's cipher, Substitution cipher where the messages are replaced or substituted by numbers or characters. Ciphers are known as encrypted message. The decryption technique is also present. The decryption is used to retrieving the original message. Inverse ciphers are known as decrypted message. The secret key is used in encryption and decryption transformation. This can be seen in simple key – lock mechanism. The key is used for locking the lock or unlocking the lock. The key is referred to as secret key and the lock is the message. The locking and unlocking configuration refers to the encryption and decryption. This is used in wider application such as financial transaction, e-mail and ATMs.

FIPS 197 (2002) gives specification on notations and convention, mathematical preliminaries, algorithmic specification and implementation issues. AES standard specifies the Rijndael algorithm which is a symmetric block cipher processing 128 bits of data block consisting of 128, 192, and 256 bits length of cipher keys [1]. Xinmiao Zhang et al (2002) have presented various approaches in AES for efficient hardware implementation. Two classes are categorized for optimization methods which are architectural optimization and algorithmic optimization. In architectural optimization, the strength of pipelining, loop unrolling and sub-pipelining are exploited. Processing multiple rounds simultaneously increases speed at the cost of increased area and not an effective solution in feed-back mode. Loop unrolling architecture can achieve a slight speedup with significantly increased area. Sub pipelining is non feedback mode where maximum speed can attain with best speed/area ratio. Algorithmic optimization exploits algorithmic strength inside each round unit. Resource sharing issues are discussed for both encryptor and decryptor are needed to be implemented in small area [3].

In this paper we have proposed the system which shows confidentiality by using AES algorithm for encryption and decryption of a given message. This confidential system can be used for Voice Protocol Network (VPN) encryption, online banking and cloud computing.

II. Theory

AES algorithm uses encryption and decryption process for information/ data protection. AES algorithm was introduced by Joan Daeman and Vincent Rijimen. Rijndael algorithm proposal of AES algorithm was taken by National Institute of Standards and Technology (NIST) in 2001 and published in Federal Information Processing Standards Publications (FIPS-199).This algorithm uses single key i.e. a secret key and it is symmetric in nature. It has high speed compared to asymmetric algorithm. There are different types of length of cipher key is used such as 128, 192 and 256 bits for AES-128, AES-192 and AES-256 respectively.

Rijndael algorithm uses AES-128, consists of 128 bits of plaintext, cipher and key. The combination of key, block and round are given as 4 words for key length, 4words for block length and number of rounds are 10. It has state matrix of 4x4 row and column order with 8 bit data width and 256 addresses. Rijndael encryption and decryption process includes four operations which are as follows:

ISSN : 2348 - 9065 (Online)
ISSN : 2349 - 3143 (Print)

A. Sub-bytes/Inverse sub-bytes

In this transformation, byte of the sub arrays of state matrix is substituted by standard s-box and inverse s-box in encryption and decryption process respectively. Affine transformation and Galois field (GF (2^8)).

B. Shift rows/Inverse shift rows

In this transformation, byte of sub arrays in rows of state matrix is circular shifted in left and right in encryption and decryption process respectively. First row remains unchanged while other rows are shifted by one byte respectively i.e. row R2 shifted by 1 byte, similarly R3 shifted by 2 byte and R4shifted by 3 byte.

C. Mixed Columns/Inverse mixed columns

In this transformation, byte of sub arrays is permuted by using different polynomials for columns of state matrix right in encryption and decryption process respectively. In mixed columns and inverse mixed columns the polynomials used are:

$a(x) = \{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$ (1)

$a^{-1}(x) = \{0b\}x^3+\{0d\}x^2+\{09\}x+\{0e\}$ (2)

The normal multiplication is not used. The cyclic shift operation with xor logic is applied for numbers i.e. {03}. For {01} data is unchanged, no shifting operation is performed. Similarly for {02} data is changed by 1bit circular shift and for {0e} data is equivalent to circular shift of data by 3 bits xor with circular shift of data by 2 bits xor with circular shift of data by 1 bit.

D. Add round keys/Inverse add round keys

In this transformation, application of xor is used. Here 10 round keys are employed with the help of key expansion which uses 10 keys for schedule. In key scheduling 44 words are obtained.

III. Block Diagram

In network communication three modules are present which are transmitter, channel and receiver.

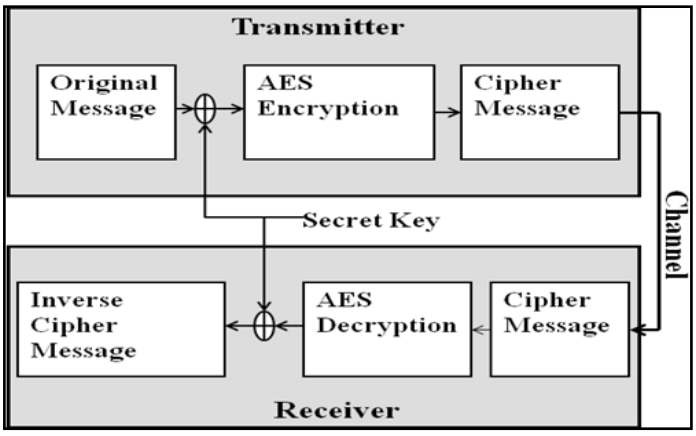

Fig. 1: AES encryption and decryption process at transmitter and receiver trough a network channel for a confidential system.

The transmitter also called sender as it is used to transmit the information while the information is passed through the channel. The receiver also called reception as it is used to receive the information through the channel. The channel is the interface between the transmitter and the receiver and it should have less noise, less disturbance and applicable in real time environment. The proposed block diagram shows the original message is xor with secret key which is processed for encryption by performing encryption algorithm at the transmitter and encrypted information is propagated through the channel in the form of cipher to the receiver where decryption algorithm is performed to retrieve the original message in the form of inverse cipher with the help of secret key.

IV. Algorithm

A. Encryption Algorithm

- Message (Plaintext) is xor with original key given by $k_{0,e}$.
- Apply s-box and shift row transformation.
- Apply mix column transformation.
- Key schedule occurs with the help of key expansion.
- Repeat process for 10 rounds, mix column transformation is not performed in last round.
- Plaintext is transformed into cipher.

B. Decryption Algorithm

- Cipher is xor with last scheduled key.
- Apply inverse shift row and inverse s-box transformation.
- Apply inverse mix column transformation.
- Using key schedule from encryption, the given keys are $k_{10,e} = k_{0,d}$,....., $k_{0,e} = k_{10,d}$.
- Repeat this for 10 rounds, inverse mix column transformation is not performed in last round.
- Cipher is transformed into inverse cipher/ original message.

V. Simulation and Results

The simulation of verilog code for AES encryption, decryption and key expansion is obtained in Modelsim 6.3. The synthesis is done in Xilinx 12.2.

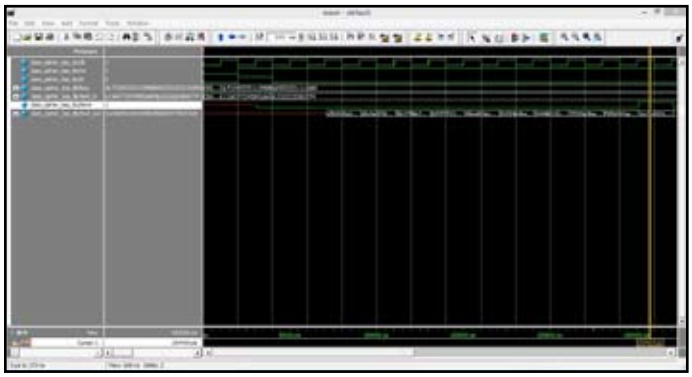

Fig. 2: AES cipher simulation.

The 128- bit message (plaintext) is transformed into 128- bit cipher with the help of 128-bit key. At 10th round encrypted message is obtained when the done pin is high which show the process is completed. The 128- bit cipher is transformed into 128- bit inverse cipher/ original message with the help of 128-bit key. At 10th round decrypted/ original message is obtained when the done pin is high which shows the process is completed.

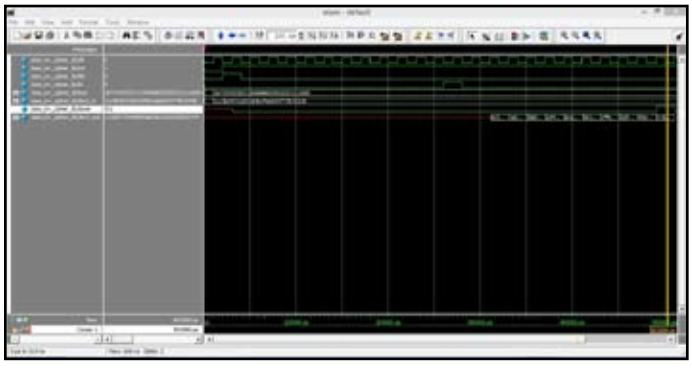

Fig. 3: AES inverse cipher simulation.

The key expansion is used for key scheduling. There are 10 keys for scheduling having 44 words. The process starts at kld pin is high with positive edge clock. The 10th key is obtained after 10 clock cycle where the process is completed.

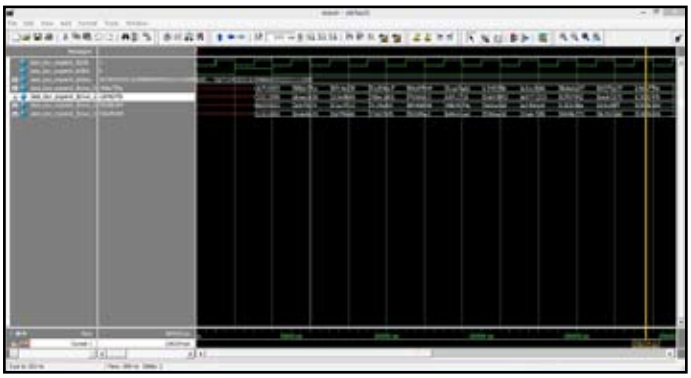

Fig. 4: AES key expansion simulation

The proposed system maintains confidentiality by hiding the message across the network channel. The performance is higher with reduce clock cycle with less delay. There is less disruption i.e. reduced noise across the network channel.

VI. Applications

The applications involved for secured communication and distributed systems. In online banking process, user login password with one time password (OTP) for a unique user has been provided by banks which can access all the details related to his/ her account. The user can buy any items from any online stores. The access period for login is limited for different banks i.e. 5 minutes. The privacy and security is maintained by strong encryption and decryption algorithm.

In VPN, at the sender end of the transmitter section encryption algorithm is used to encrypt the data which is invisible across the channel and at the reception end of the receiver section the encrypted data is transformed into the original message by decryption algorithm. The information is sent by the user to another user in a networking channel is maintained privately and secured with resource protection in a confidential manner.

The cloud computing is the application delivering services between internet, distributed systems, hardware and software. There are four delivery models related to cloud computing which are private, public, community and hybrid cloud. The services are delivered to private organization, government organization, community and several organizations. There are four service models which are Software as service (SaaS), Platform as service (PaaS) and Infrastructure as service (IaaS). All service and delivery models ensure confidentiality with privacy for a secured system.

VII. Conclusion

In this paper the confidential system uses AES algorithm which ensures confidentiality across the network communication with privacy. The obtained simulation verifies the system is maintaining confidentiality with data protection in real time environment.

Hence the confidential system is used in many distributed systems to prevent hackers from accessing unauthorised information.

VIII. Acknowledgement

I would like to thank my guide Jayaraj N of The Oxford College of Engineering Bangalore for supporting the study.

References

[1] *FIPS-197, National Institute of Standards and Technology, Announcing the Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.*

[2] *M. Goswami and S. Kannojiya, "High Performance FPGA Implementation of AES Algorithm with 128-Bit Key"s, Proc. IEEE International Conf. Advances Computing Comm., vol. 1, Himarpur, India, 2011, pp.281-286.*

[3] *Xinmiao Zhang and Keshab K. Parhi "Implementation Approaches for the Advanced Encryption Standard Algorithm" IEEE 2002.*

[4] *P. Rogaway, "Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC", Advances in Cryptology—Asiacrypt 2004, Lecture Notes in Computer Science, vol. 3329, pp. 16-31, Springer-Verlag, 2004.*

[5] *Morris Dworkin, NIST Special Publication 800-38E, "Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices".*

[6] *B. Schneier. Applied Cryptography. John Wiley & Sons, Inc., second edition, 1996.*

[7] *FIPS-199, National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information System, February 2004.*

[8] *Sen, J. (2010f), "A Trust-Based Robust and Efficient Searching Scheme for Peer-to-Peer Networks", Proc. 12th International Conference on Information and Communication Security (ICICS), pp. 77-91, December 2010, Barcelona, Spain, Springer LNCS Vol 6476.*

[9] *Security Engineering: A Guide to Building Dependable Distributed Systems.*

[10] *http://www.cl.cam.ac.uk/~rja14/Papers/SE-04.pdf*