International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

AES Algorithm: Encryption and Decryption

Shivangi Wadehra, Shivam Goel, Nidhi Sengar
Maharaja Agrasen Institute of Technology, GGSIPU, Delhi, India

ABSTRACT

Advanced Encryption Standard (AES) algorithm is one of the most common and widely used symmetric block cipher algorithm. This algorithm has its own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software, all over the world.

It is extremely difficult for hackers to get the real data when encrypting by AES algorithm. In AES algorithm, encryption and decryption involves a number of rounds that depends on the length of the key and the number of block columns. So, to improve the strength of the AES the number of rounds is increased. Till date there is not any evidence to crack this algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. This paper will provide an overview of AES algorithm and explain several crucial features of this algorithm in detail.

1. INTRODUCTION

Network security is becoming much more important because people spend a lot of time connected in a network. To protect the value and ongoing usability of assets, the integrity and continuity of operations, different techniques and methods have been using by private and public sectors to protect sensitive data from intruders because of the security of electronic data is crucial issue. Cryptography is one of the most significant and popular techniques to secure the data from attackers by using two vital processes that is Encryption and Decryption.

Encryption is the process of encoding data to prevent it from intruders to read the original data easily. It is used to convert the original data (Plaintext) into unreadable format known as Cipher text. The next process that has to carry out by the authorized person is Decryption. Decryption is contrary of encryption. It is the process to convert cipher text into plain text without missing any words in the original text.

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 can be acquired. Thereafter, cryptography secures information by protecting its confidentiality and can also be used to protect authenticity of data and information about the integrity.

Modern cryptography provide the confidentiality, integrity, no repudiation and authentication. There are a number of algorithms available to encrypt and decrypt sensitive data which are divided into two types. First one is symmetric cryptography where the same key is used for encryption and decryption data. Second one is Asymmetric cryptography. This type of cryptography relies on two different keys for encryption and decryption.

2. RELATED WORK

The **Data Encryption Standard** (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher and uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only)**.** A replacement for DES was needed as its **key size** was too **small**. With the increasing

computing power, it was considered vulnerable against exhaustive key search attack. **Triple DES** was designed to overcome this drawback but it was found slow. Hence, AES was introduced.

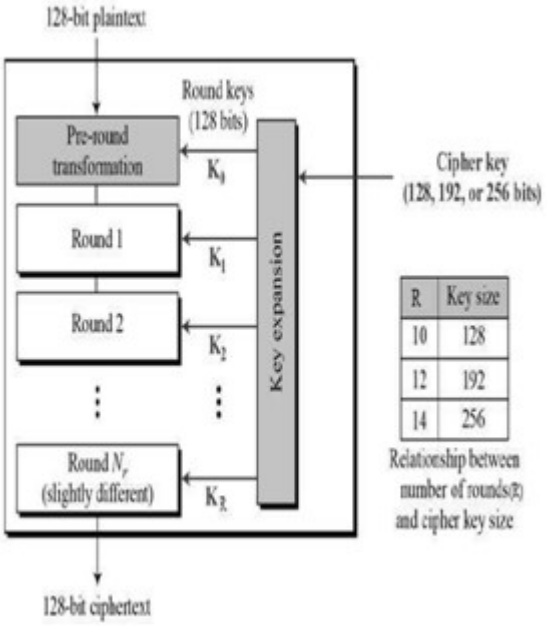
3. IMPLEMENTATION:

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'.

It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

AES algorithm performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing in the form of a matrix.

The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12

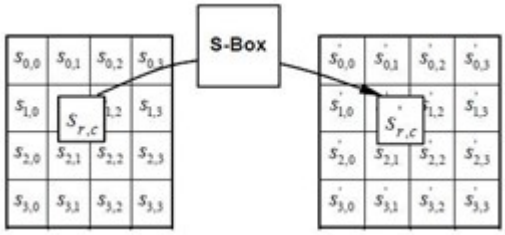


R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

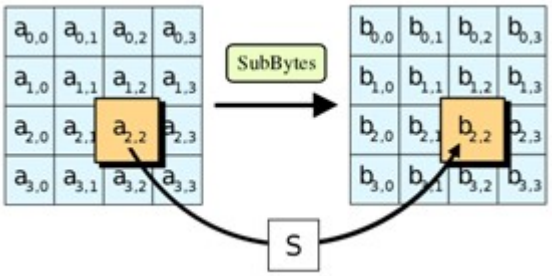
ENCRYPTION PROCESS:
Each round of the encryption process consists of four sub round processes. These include:

Byte Substitution:
The 16 input bytes are substituted by looking up a fixed table (S-box) given in lookup table. The result is then stored in a matrix of four rows and four columns.

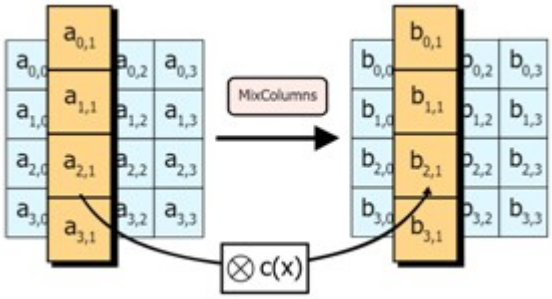


Shift rows:
Here, all the four rows are shifted to the left.

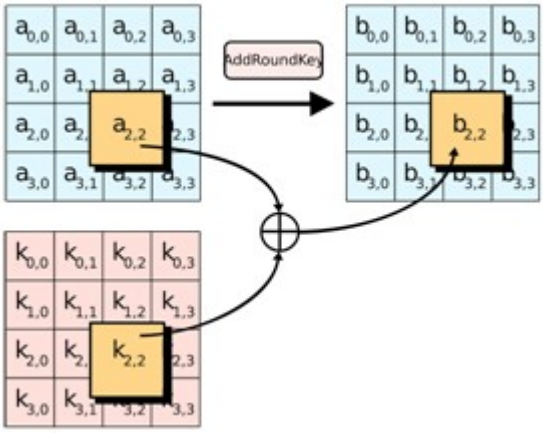
- The first row is not shifted
- The second row is shifted by one position (byte).
- The third row is shifted by two positions.
- The fourth row is shifted by three positions.



Mix Columns:
All the four columns of the matrix are transformed using a special function.
The function takes input as the four bytes of the column and output a completely different column. Thus, we get a completely different matrix as the output.



Add Round Key
The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

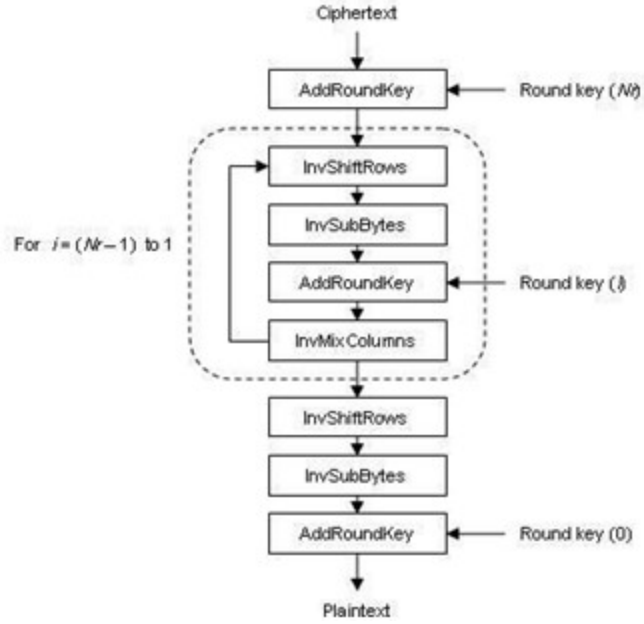


Thus one round of the AES algorithm consists of four sub rounds explained above.

3.2 DECRYPTION PROCESS

The decryption process is similar to that of encryption except the processes are reversed in order.

They are performed as follows:
1. Add Round key
2. Mix Columns
3. Shift Rows
4. Byte Substitution



4. CONCLUSION

Using internet and network are increasing rapidly and everyday a lot of digital data have been exchanging among users. Some of the data is sensitive and needs to be protected from intruders. Encryption algorithms play vital roles to protect original data from unauthorized access. Advanced encryption standard (AES) algorithm is one of the efficient algorithms and it is widely supported and adopted on hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. It is much more secure than DES and Triple DES.

Additionally, AES has built-in flexibility of variable key length and thus it allowing a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

REFERENCES:

1. https://www.tutorialspoint.com/c ryptography/advanced_encryptio n_standard.htm
2. http://imps.mcmaster.ca/courses/ SE-4C03-07/wiki/siaa/se4c03_aes_wiki(7).html
3. https://www.researchgate.net/pu blication/317615794_Advanced_E ncryption_Standard_AES_Algorith m_to_Encrypt_and_Decrypt_Data
4. Deshpande, H. S., Karande, K. J., & Mulani, A. O. (2014, April). Efficient implementation of AES algorithm on FPGA. In Communications and Signal Processing (ICCSP), 2014 IEEE International Conference on (pp. 1895-1899)
5. Wikipedia volunteers. "Advanced Encryption Standard". 27 March 2007. Accessed 16 March 2007. URL:<http://en.wikipedia.org/wiki/Advanced_En cryption_Standard>
6. 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.
7. U.S. Department of Commerce/NIST, —Data Encryption Standard,FIPS PUB 46-3, pp. 1-26, October 1999.
8. J. Daemen and V. Rijmen, —The Block Cipher Rijndael, Lecture Notes in Computer Science, vol.1820, pp.277- 284, Berlin: Springer-Verlag, 2000.
9. Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on (pp. 277-285).