# A Comparative Study on AES 128 BIT AND AES 256 BIT

**Article** *in* INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING · September 2018

DOI: 10.26438/ijsrcse/v6i4.3033



**1 author:**

Toa Bi Irie guy-cedric
Jain University
**7** PUBLICATIONS **11** CITATIONS

SEE PROFILE

International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.4, pp.30-33, August (2018)
Research Paper
E-ISSN: 2320-7639

# A Comparative Study on AES 128 BIT AND AES 256 BIT

**Toa Bi Irie Guy-Cedric[1*], Suchithra. R.[2]**

[1] Research scholar, Jain University, Bangalore-560043, India
[2]Head of Department of MSc IT, Jain University, Bangalore-560043, India

**Corresponding Author: guy-ced@hotmail.fr*

**Available online at: www.isroset.org**

Accepted: 15/Aug/2018, Online: 31/Aug/2018

***Abstract*—** Cloud computing present a new thinking to apply security since basic administrations are regularly outsourced to the cloud vendor. The current encryption techniques are regularly exposed to threats. Therefore it is important to study the features of the existing algorithm. This paper studies AES 128 and AES 256 based on various parameters and compare their performance that may suggest in development of better encryption technique.

***Keywords*—** Cryptography, Cloud Computing, AES

## I. INTRODUCTION

Nowadays security concern grows with cloud adoption at organizations level, data center, current users and cryptography algorithms has a tremendous impact security concern. Indeed cryptography algorithms are used for ensuring confidentiality, data protection, communication, authorization and non-repudiation and play a major role in security software and hardware. It includes two groups, symmetric and asymmetric algorithm. Cryptography is a technique to transform data into secret data meaning only authorized users can read it. It based on the mathematics and the process to convert data is called encryption by using a key during the process to encrypt and decrypt. See Figure 1 [1].

Symmetric cryptography: Symmetric algorithm is one of encryption algorithm using one key to encrypt and decrypt the message. That key is called secret shared key or private key. Nowadays most symmetric algorithm validate by peers and used is Advanced Encryption Standards (AES) proposed by Vincent Rijmen, Joan Daemen (Rijndael). It has been standardized in Federal Information Processing Standard (FIPS) 192, published in November 2001 [2, 3]. AES is based on a substitution–permutation network and works on 128 bit fixed block with three variant respectively depending of the key size as 128, 192 and 256 bits.

Asymmetric cryptography: Asymmetric cryptography uses two key during the process of cryptography like Rivest–Shamir–Adleman (RSA) with one key for encryption known as public key and one key for decryption known as private key. Indeed the secrecy of asymmetric cryptography depends on how receiver of the message keep the private key as secret. This paper analyses the difference between AES-128 and AES-256 that is explained with the implementation research to show their efficiency. The rest of the paper is organized as follows. In Section II, we briefly describes Advanced Encryption Standards (AES). In Section III, contain Proposed AES algorithm implementation. Comparisons and analysis are shown in Section IV and finally, we conclude this paper in Section V.

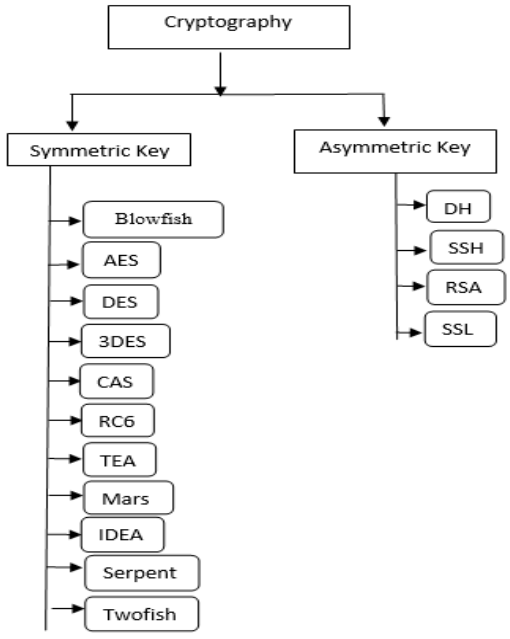


Figure 1: Cryptography Family

 

## II. AES OVERVIEW

Advanced Encryption Standards (AES) was introduced in 2000 by Vincent Rijmen, Joan Daemen (Rijndael), to replace Data Encryption Standard (DES). AES is a block cypher algorithm that encrypt data on a per-block basis (block matrix) and supports key size of 128, 192 and 256 bits and block size of 128 bits. It is based on Substitution Permutation Networks (SPN). SPN has been introduced by Shannon to protect cypher against statistical cryptanalysis attack. SPN is a consecutive series of mathematical operations (substitution and linear transformation) which is used in block cipher. Let's define some key words for a better understand of how AES works.

- Round

A round is a transformation process used during encryption process that include some function substitution, transposition and mixing, with the achievement to have a higher output cipher text. Each key size is associated with the number of round which provide a high secure system. As shown in table 1.

| AES TYPES + Key Size | Data Block Size | Matrix Block | Number of Round |
|---|---|---|---|
| AES-128 | 128 | 4*4 | 10 |
| AES-192 | 128 | 4*6 | 12 |
| AES-256 | 128 | 4*8 | 14 |

Table 1: Structure of AES

- Block Cipher

A Block Cipher is a method to encrypt data by group at time and uses the same key in decryption and encryption. Indeed the purpose of block cypher method is to avoid the similarity of ciphertext during encryption even if the same message is encrypted again. Table 2 gives a representation of 128 in block matrix 4 × 4 column-major

Table2: Representation of AES 128 in block matrix 4 × 4 column major

| | | | |
|---|---|---|---|
| $b_{0,0}$ | $b_{0,1}$ | $b_{0,2}$ | $b_{0,3}$ |
| $b_{1,0}$ | $b_{1,1}$ | $b_{1,2}$ | $b_{1,3}$ |
| $b_{2,0}$ | $b_{2,1}$ | $b_{2,2}$ | $b_{2,3}$ |
| $b_{3,0}$ | $b_{3,1}$ | $b_{3,2}$ | $b_{3,3}$ |

## III. PROCESS OF ENCRYPTION AND DECRYPTION

The standard process of AES encryption and decryption is shown on figure 2 AES-128 bits algorithm [4]. Indeed the process is composed of different rounds depending on the size of key expansion and each round follows an iterative process [5].

In encryption process each round follows four steps:

- SubBytes – is a process who performs a non-linear substitution step by replacing each byte with another value from substitution box (S-box)
- ShiftRows – is called a row-wise step by performing a circular shifts on the last three rows of the state, respectively line 2= 1, line 3= 2 and line 4= 3.
- Mixcolumns is a linear transformation. It is a matrix product using the four bytes of a column. Columns are treated as polynomials as shown in that formula (1):

GF (28) and multiplied modulo $x^4 + 1$ with fixed polynomials

$$\begin{bmatrix} c_{0,i} \\ c_{1,i} \\ c_{2,i} \\ c_{3,i} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b_{0,i} \\ b_{1,i} \\ b_{2,i} \\ b_{3,i} \end{bmatrix} \text{ for } 0 \leq i \leq 3 \quad (1)$$

- AddRoundKey – is to apply XOR operation on output of the previous three steps combined the round key which is generated from the cipher key as shown in that formula (2):

$$C_{0,i} = (\{2\} \bullet b_{0,i}) \oplus (\{3\} \bullet b_{1,i}) \oplus b_{2,i} \oplus b_{3,i}$$

$$C_{1,i} = b_{0,i} \oplus (\{2\} \bullet b_{1,i}) \oplus (\{3\} \bullet b_{2,i}) \oplus b_{3,i}$$

$$C_{2,i} = b_{0,i} \oplus b_{1,i} \oplus (\{2\} \bullet b_{2,i}) \oplus (\{3\} \bullet b_{3,i})$$

$$C_{3,i} = (\{3\} \bullet b_{0,i}) \oplus b_{1,i} \oplus b_{2,i} \oplus (\{2\} \bullet b_{3,i})$$

 

For decryption process each round follows four steps:

- Inverse ShiftRows
- Inverse substitute bytes
- AddRoundKey key
- Inverse mix columns.

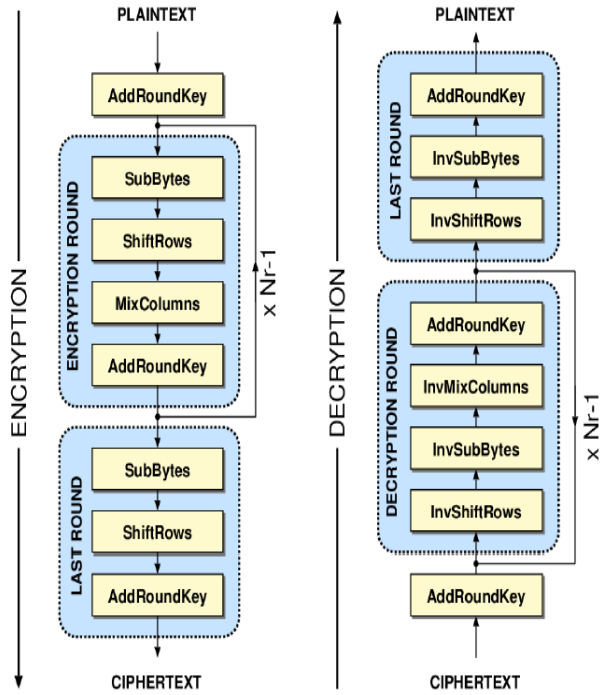


Figure 2: Encryption and Decryption process

## IV. Proposed AES algorithm implementation

This section discuss the results of our implementation between AES-128 bits and AES-256 bits is taken by varying the amount of file size being between (100 kb, 500kb and 1024 kb ) selected and the checking time for encryption and decryption . The obtained results are tabulated as well as given in the form of graphs.

- Checking the time of encryption and decryption based on some documents.

### AES Standard Algorithm

AES algorithm (128,192 and 256) is outline form [6]:

```
With: Nb = 4(nb) number of columns

      Nr = Number of round
      Nk = Number of key word

Cypher (byte in [4*Nb], byte out
[4*Nb], word w[Nb*(Nb+1)]
```

```
begin

   Byte state [4, Nb]
   State = in
   AddRoundKey (state, w[0, Nb-1])

   for round = 1 step 1 to Nr-1
       SubBytes (state)
       ShiftRows (state)
       MixColumns (state)
       AddRoundKey (state, w[round*Nb,
(round1)*Nb-1])
   end for

   SubBytes (state)
   ShiftRows (state)
   AddRoundKey (state, w[Nr*Nb, (Nr+1)*
Nb-1])

   Out = state
  end
```


Figure 3. Comparative encryption time of AES-128 and AES-256

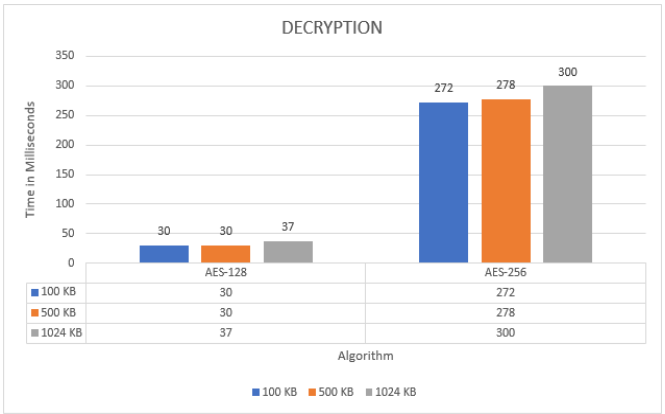


Figure 4. Comparative decryption time of AES-128 and AES-256

 

## IV. DISCUSSION

The results in figure 3 & 4 shown how the time of encryption varies alongside with the key choose. However when the key is strong and long, the encryption time take more time in both types of AES.
Conversely, AES-256bit are more robust because of this architecture rounds and take more time to decrypt file while of AES-128bit has an average decryption time (around30 milliseconds). Nowadays AES has shown be more secure and robust than other cryptography algorithm used when this one is properly implemented.

## V. CONCLUSION

Security is an important part of cloud data center, while cryptography is one of the main technics used for data security. This paper briefly describes the different types of AES encryption model and present some highlight. It was observed from the experiment that the time of encryption and decryption process is tied with the size of key and also the hardware used. However some studies on security issue have shown one particular attack is more efficient to crack hardware or software based on AES.

## REFERENCES

[1]. Samiul Islam "Comparative Analysis of AES Algorithms and Implementation of AES in Arduino" 20.12.2015
[2]. V. R. Joan Daemen. AES Proposal: Rijndael, version 2, AES submission. 1999.
[3]. Joan Daemen, Steve Borg and Vincent Rijmen."The Design of Rijndael: AES The Advanced Encryption Standard", Springer, 2002.
[4]. Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis" May 2, 2014
[6] cs.utsa.edu/~wagner/laws/AESintro.html
[5]. csrc.nist.gov/publications/fips/fips197/fips 197.pdf. NIST_SP-500-291_Version-2_2013_June18_FINAL
[7]. Chenhui Jin, Ting Cu "Classification of SPN Structures From the Viewpoint of Structural Cryptanalysis" IEEE, December 27, 2017
[8] Umer Farooq, M. Faisal Aslam "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA", Journal of King Saud University – Computer and Information Sciences, 10 January 2016, sciencedirect
[9]. Arash Karimi, Hadi Shahriar Shahhoseini "Cryptanalysis of a Substitution-Permutation Network Using Gene Assembly in Ciliates" Int'l J. of Communications, Network and System Sciences Vol. 5 No. 3 ,2012.

### Authors Profile

Mr. Toa Bi Irie Guy-Cedric pursed Bachelor of Science from Institut National Polytechnique Felix Houphouet-Boigny, of Cote d'Ivoire in 2011 and Master of Information Technology from Shridhar University, India in year 2013. He is currently pursuing Ph.D. in Computer Science from Jain University, India. He has published many research papers in reputed international journals and conferences. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy.

Dr. Suchithra R pursed Bachelor of Commerce, Master of Computer Application and Ph.D in Computer Science from Manonmaniam Sundaranar University , India in year 2009. She worked as Associate Professor and Head of MS (IT) Department in Jain university since 2010. She has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & other) and conferences and it's also available online. Her main research work focuses on Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Programming. She has 15 years of teaching experience and 6 years of Research Experience.

 