International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 7– No.8, September 2014 – www.ijais.org

Investigating the Effects of varying the Key Size on the Performance of AES Algorithm for Encryption of Data over a Communication Channel

Kazeem B. Adedeji
Electrical/Electronics Engineering Dept
Federal University of Technology
Akure, Nigeria

John O. Famoriji
Electrical/Electronics Engineering Dept
Federal University of Technology
Akure, Nigeria

ABSTRACT
Key size of an algorithm is an important aspect of cryptographic technique as high key bits is considered more secure than low key bits. Different research work has been conducted to have secure and reliable protection techniques for transmitting data over a communication networks. This paper shows the effects of varying the key size on Advanced Encryption Standard (AES) algorithm for encryption of data. AES algorithm with key sizes of 128 bits, 192 bits and 256 bits were considered. The performance of the system were examined based on the encryption and decryption time, throughput, average data rate and the central processing units (CPU) power consumption. Consequently, AES with key size of 128 bits has a lower encryption time, higher throughput and low CPU power consumption than AES with 192 bits and 256 bits keys.

Keywords
AES, Average data rate, CPU power consumption, Cryptography, Encryption, Key, Throughput.

1. INTRODUCTION
The recent advances in computing and internet facilities have made data communication a very easy task. Internet facilities have or are capable of reaching every location in the world today. The internet is a global system of interconnected computer networks that uses the standard internet Protocol Suite (TCP/IP) to serve billions of users worldwide [1]. Since Government sector, banking sector, military and others now tend to send data over a communication network; such a data has to be protected from an unauthorized party (security). Also the authenticity of the data sent is of paramount important so that the receiver of a particular data will be able to confirm that such a data has not been tampered with during transmission. To have a secure data transfer over a communication network, cryptography plays a vital role.

Encryption is the process of transforming plaintext data into cipher text to conceal its meaning and so preventing any unauthorized recipient from retrieving the original data [2]. Encryption works by running the data (represented as numbers) through a special encryption formula called a key [3]. The science used in cipher text attack to recover any data or to forge the data as to try to pass it off as authentic is known as cryptanalysis [4].

Various studies and research has been conducted to analyzed and study the comparative performance of algorithms, Himani and Marisha (2012) [5] analyzes various symmetric encryption techniques and compared them on points such as execution time and avalanche effects by varying key or plain text. The security of encrypted data depends primarily on the choice of algorithm and key length [6].

This paper annexes the effects of varying the key sizes on the performance of AES algorithm by computing the encryption and decryption time for each key, the key used in this paper are 128 bits, 192 bits, and 256 bits. The throughput and the average data rate of the AES algorithm for three different AES keys was also computed and analyzed.

2. BACKGROUND KNOWLEDGE AND RELATED WORK
Cryptographic algorithms are basically classified in to three main categories; secret key or symmetric cryptography, public key or asymmetric cryptography and hash function. Symmetric technique uses a single key for both encryption and decryption of data. DES, AES, CAST, Blowfish, Twofish, IDEA and Secure and Fast Encryption Routine (SAFER) are some examples of symmetric technique [7]. In an asymmetric technique, two different keys that are mathematically related are used. It uses one key (public key) for encryption and another (private key) for decryption. The public key is widely distributed while the private key is secret, which is known to the receiver only. RSA, Diffie-Hellman, DSA, Elgama and ECC are some public key cryptographic system [8]. The hash function uses a mathematical transformation to irreversibly "encrypt" information. This type of system includes MD5, SHA-1, SHA-2 [9]. Most data encryption algorithms are computational intensive and tend to draw significant amount of power and battery. Some symmetric cryptographic algorithm such as AES, Blowfish and RC4 has been used for smaller packet data for wireless device. Prasithsangaree and Krishnamurthy (2003) [10], works on analysis of energy consumption of RC4 and AES algorithms in wireless LANs. They show how AES can be used for encrypting IEEE 802.11 management packets. From their results, with a small packet sizes, AES tends to have better performance than RC4. According to Lenstra and Verheul, (2001) [11], a longer key size would provide stronger security of data. Hence, it is necessary to investigate the effect of increasing key sizes on data encryption algorithms.

2.1 Overview of AES
AES is a symmetric key algorithm (same key is used encryption and decryption). It is a block cipher which means it breaks data in blocks and combines key with each to get encrypted data [12]. AES has transformation rounds

which are called a definite number of times to encrypt data depending on the bit length. The entire process to obtain a cipher text in the AES rounds is shown in Fig. 1.

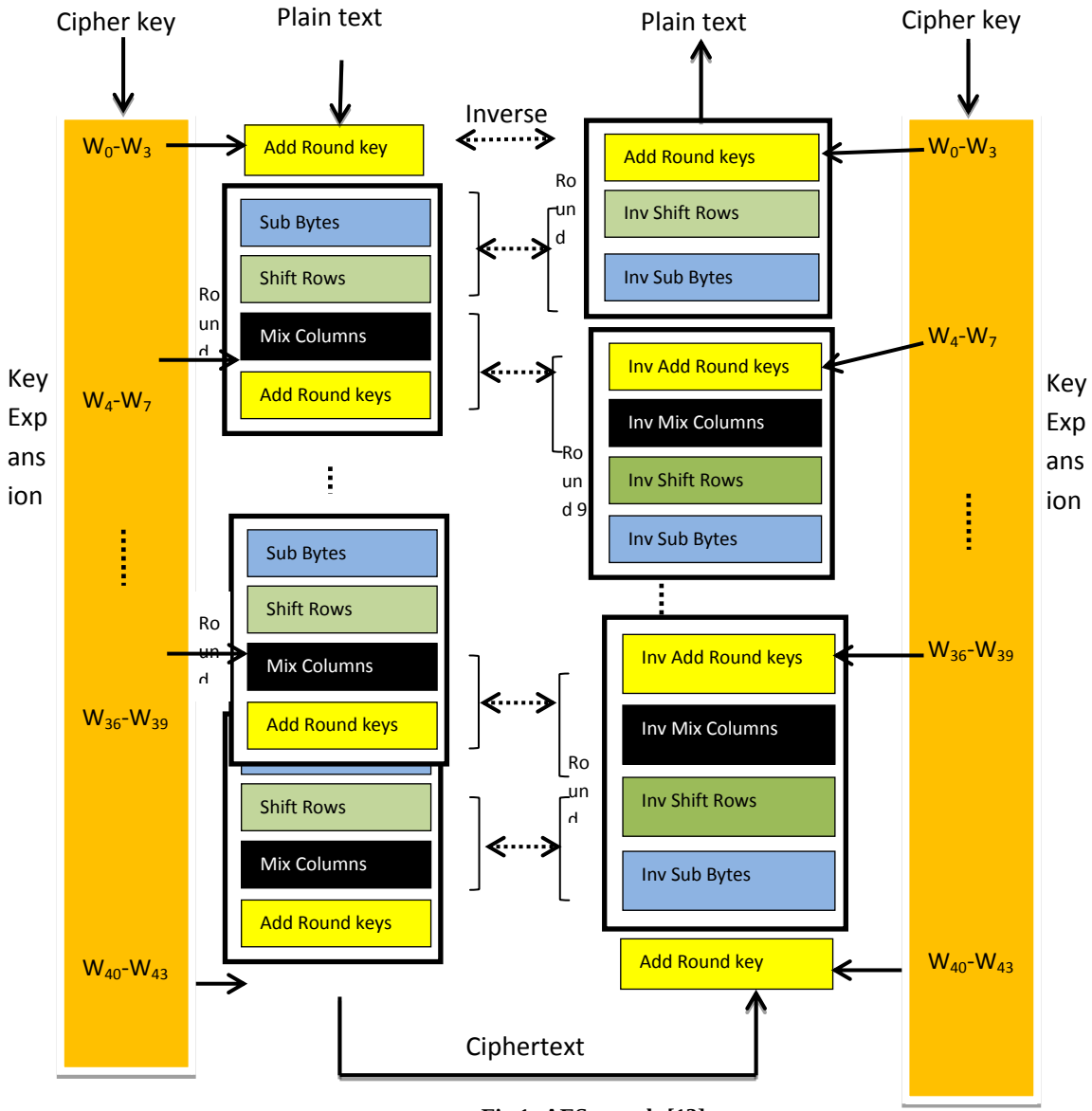

Fig.1: AES rounds [13]

AES is the Advanced Encryption Standard, a United States government standard algorithm for encrypting and decrypting data. Key lengths can be 128 8bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively [14]. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. The main loop of AES performs the following functions according to Eric, (2007) [14]:

- Sub Bytes ()
- Shift Rows ()
- Mix Columns ()
- Add Round Key ()

The first three functions of an AES round are designed to thwart cryptanalysis via the methods of "confusion" and "diffusion." The fourth function actually encrypts the data [14].

3. SYSTEM PARAMETERS

The results were simulated using C sharp language installed on Intel (R) Atom CPU N270 with 1.60GHz processor and 1.00GB RAM with 32-bit operating system

4. RESULTS AND DISCUSSION

The encryption and decryption time for different key sizes used for the AES algorithm was recorded. The average data rate was also calculated for all the key sizes based on the recorded data. The average data rate was calculated as

$$Avg.data\ R = \frac{1}{N_b}\sum_{I=1}^{N_b}\frac{M_i}{t_i} \qquad (kB/Sec) \qquad (1)$$

where $Avg.data\ R$ is the average data rate in (kb/s), N_b is the number of message, M_i is the message size (kb) and t_i is the time taken to encrypt message M_i.

According to Anand and Kartthikeyan (2012) [7], it is very important to calculate the throughput of an encryption algorithm to know the performance of the algorithm. The encryption time for the algorithm was used to calculate the throughput of an encryption scheme. It indicates the speed of the encryption. The throughput is given by

$$Throughput = {}^{T_p}/_{E_t} \quad (MB/Sec) \qquad (2)$$

where T_p is the total plaintext encrypted and E_t is the total encryption time.

Table 1 and Table 2 shows the recorded data for encryption and decryption based on different input data sizes and AES keys. It also shows the throughput of the algorithm which was calculated using Eqn. (2) and the average data rate calculated Eqn. (1)

Table 1: Simulation Time for (Millisecond) of Encryption data sizes with different key sizes

Data Size (KB)	Simulation Time (Millisecond)		
	AES 128	AES 192	AES 256
40	29	47	58
70	80	88	96
100	90	102	118
550	140	177	188
800	190	251	274
1000	300	304	318
Average Data Rate (KB/Sec)	2472.97542	2035.16331	1876.02892
Throughput (MB/Sec)	3.0880579	2.64189886	2.43346008

Table 2: Simulation Time for (Millisecond) of Decryption data sizes with different key sizes

Data Size (KB)	Simulation Time (Millisecond)		
	AES 128	AES 192	AES 256
40	30	48	62
70	82	90	100
100	93	105	120
550	145	180	189
800	200	260	280
1000	302	304	322
Average Data Rate (KB/Sec)	2394.43707	1997.57406	1841.88008
Throughput (MB/Sec)	3.00469484	2.59371834	2.3858341

The performance of the system with varying key sizes can be shown graphically; the results shown in Table 1 and Table 2, also demonstrated in Fig. 2 and Fig. 3 show that AES 128 has the lowest simulation time for encryption and decryption, which means it is faster than AES 192 and AES 256.

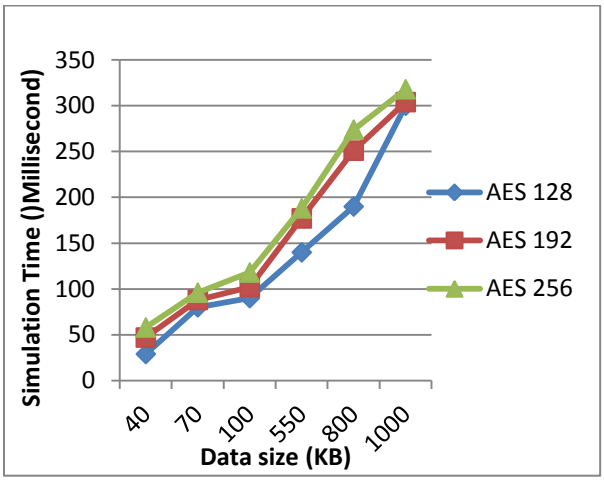

Fig. 2: Input data size versus Encryption time for the three AES key sizes.

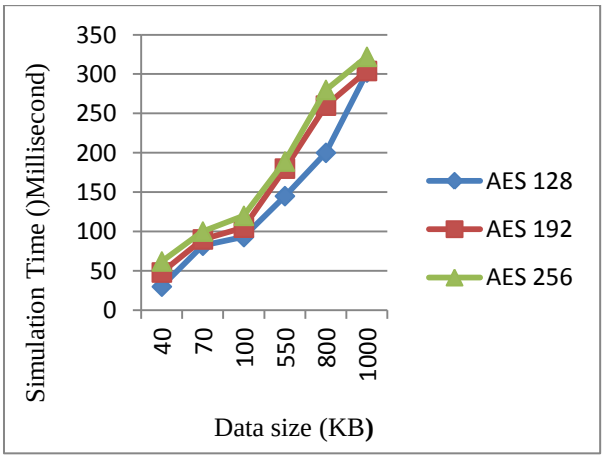

Fig. 3: Input data size versus decryption time for the three AES key sizes

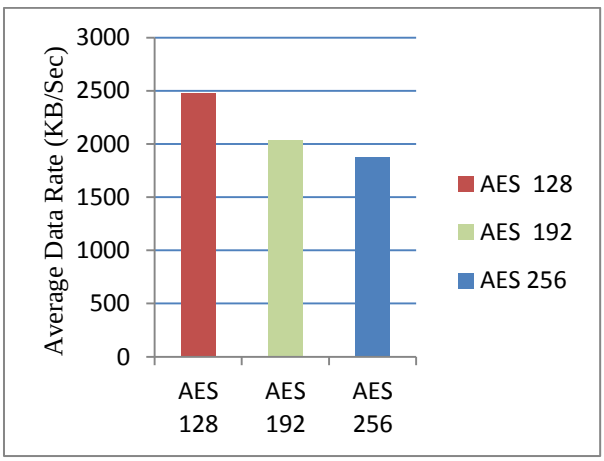

Fig. 4: Average data rate for encryption with the three AES key sizes

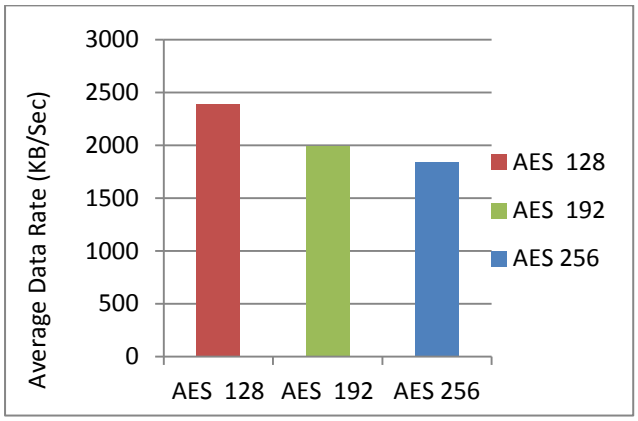

Fig. 5: Average data rate for decryption with the three AES key sizes

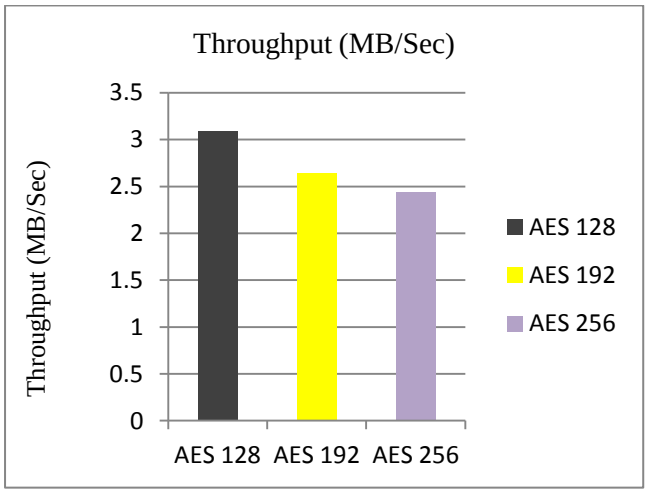

Fig. 6: Throughput for encryption with the three AES key sizes

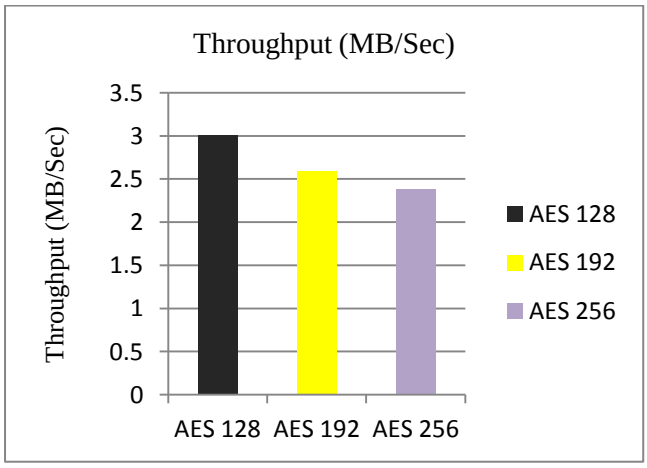

Figure 7: Throughput for decryption with the three AES key sizes

Fig. 4 and Fig. 5 show the average data rate for the algorithm while Fig. 6 and Fig. 7 reflect the throughput. AES 128 gain top with maximum throughput as it encrypt and decrypt data in minimum time, this is followed by AES 192 which is fairly better than AES 256 in terms of encryption time and throughput. The results presented in this paper are in accordance to accordance to Aman *et al* (2012) [15], which state that, if the throughput is increased, the CPU power consumption is decreased. The throughput of a data encryption algorithm is inversely proportional to the CPU power consumption. It can also be seen that, the lower the key size, the lower will be the encryption and decryption time and the higher will be the throughput. As the key size increases, the time taken to encrypt a data increases and the throughput decreases. Consequently, decrease in throughput causes high power consumption by central processing unit.

5. CONCLUSION

The selected AES key sizes have been analyzed in this paper. AES 256 bits consume large amount of time to perform encryption and decryption operation. A simulated result shows that, AES 128 bits has better performance than AES 192 and AES 256 bits in terms of throughput and power consumption. It could be concluded that as the key size increases, the simulation time increases, the throughput decreases and the power consumption level increases. Hence AES 128 bits performed better than AES 192 and AES 256.

The results were simulated using C sharp language installed on Intel (R) Atom CPU N270 with 1.60GHz processor and 1.00GB RAM with 32-bit operating system.

6. ACKNOWLEDGEMENT

Our thanks go to the experts who have contributed towards the success of this work.

7. REFERENCES

[1] A.R. Choudhar and A. Sekelsky," Securing IPv6 network infrastructure: A new security model", IEEE International conference on Technologies for Homeland Security, 2013.

[2] A. Naser, H. Fatemeh, and K. Riza, "Developing a new hybrid cipher using AES, RC4 and SERPENT for encryption and Decryption", International Journal of Computer Applications Vol.69, No.8, 2013.

[3] S. William, 2005 "Cryptography and Network Security", 4th Edition, Prentice-Hall Inc., pp.58-309.

[4] V.S. Janakiraman, R. Ganesan, and M. Gobi M, "Hybrid Cryptographic Algorithm for Robust Network Security", ICGST-CNIR, Vol.7, 2007.

[5] A. Himani and S. Marisha, "Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of Science and Technology, Vol. 13, 2012, pp.1173-1176.

[6] Parliamentary Office of Science & Technology Post note, 2006 "Data Encryption", No. 270, p 2

[7] K.M. Anand, and S. Karthikeyan, "Investigating the efficiency of Blowfish and Rejindael (AES) Algorithms", International Journal of Computer netweorks and Information Security, Vol. 2, 2012, pp. 22-28.

[8] G.A. Marin, Network Security basics, IEEE Security and Privacy, 1(3), 2005, p 68. .

[9] M. Edney, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison Wesley Inc., New York, 2003, p.7

[10] Prasithsangaree, P. and Krishnamurthy, P. (2003) "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs", IEEE GLOBECOM, pp. 1445-1449.

[11] Lenstra A.K. and Verheul E. R, " Selecting Cryptographic Key sizes", Journal of Cryptography, vol. 14 No. 4, pp. 255-293, 2001.

[12] M. Serge, and E.T. Stafford, "Cryptanalysis of Rc4 like Ciphers". In Proceedings, Workshop in Selected Areas of Cryptography, SAC '98. 1998.

[13] R.P. Jignesh, S.B. Rajesh, and K. Vikas, "Hybrid Security Algorithm for Data Transmission using AES-DES", International Journal of Applied Information Systems, Vol.2, 2012, USA, pp.15-19.

[14] Eric C. (2007), "Advanced Encryption Standard", Backshore Communications, United States.

[15] K. Aman, J. Sudesh, and M. Sunil, "Comparative Analysis between DES and RSA Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, 2012, pp. 386-389.