6-30-2022

Analyzing Computational Components of Standard Block Encryption Schemes

Chu-Wen Cheng
The University of Texas Rio Grande Valley

Miranda Heather Cantu
The University of Texas Rio Grande Valley

Sanjeev Kumar
The University of Texas Rio Grande Valley

Recommended Citation

Cheng, C.-W ., Cantu, M.H. and Kumar, S. (2022) Analyzing Computational Components of Standard Block Encryption Schemes. Journal of Computer and Communications, 10, 81-89. https://doi.org/10.4236/jcc.2022.106007

Scientific Research Publishing

Journal of Computer and Communications, 2022, 10, 81-89
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Analyzing Computational Components of Standard Block Encryption Schemes

Chu-Wen Cheng, Miranda Heather Cantu, Sanjeev Kumar*

Department of Electrical and Computer Engineering, The University of Texas—Rio Grande Valley, Edinburg, USA
Email: *sj.kumar@utrgv.edu

How to cite this paper: Cheng, C.-W., Cantu, M.H. and Kumar, S. (2022) Analyzing Computational Components of Standard Block Encryption Schemes. *Journal of Computer and Communications*, **10**, 81-89.
https://doi.org/10.4236/jcc.2022.106007

Received: March 18, 2022
Accepted: June 27, 2022
Published: June 30, 2022

Abstract

Encryption is used to secure sensitive computer data which may be at rest or in motion. There are several standard encryption algorithms that have been used to encrypt and protect blocks of sensitive data to ensure confidentiality. The most popular standard block encryption schemes are the Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and the first standardized encryption scheme, which is no longer the standard scheme now, namely the Data Encryption Standard (DES). AES is the current standard for block encryption used worldwide and is implemented on many processors. In this work, we compare the hardware performance of these three encryption schemes. First, we identified the underlying computational components for these three encryption schemes, and then we analyzed to what extent these computational components were being used in these block encryption schemes to encrypt and decrypt a given message. In this paper, we compared the contribution of these computational components to evaluate the overall encryption efficiency in terms of speed and computational delays for encrypting a given block of data for a given hardware platform. AES was found to be the faster scheme in terms of hardware computation speed in accomplishing the same encryption task compared to the other two block encryption schemes, namely, the DES and 3DES schemes.

Keywords

Data Encryption, DES, 3DES, AES

1. Introduction

Cryptography is a challenging field of research combining multidisciplinary knowledge of Computer Engineering, Computer Science, Digital Logic Design, and Ma-

thematics. Knowledge from all these fields is used in design of encryption schemes to keep important data secure. Information in the computer is stored in a binary form, and then these bits are mathematically worked on according to the encryption scheme until the plaintext (original text) is disguised as encrypted text. DES, 3DES, and AES are the known standard (past and present) for block encryption algorithms that use a symmetric key to encrypt the data. The basic information about the algorithms is shown in **Table 1** [1]. There have been several different comparisons done in literature [2] [3] [4] [5]. However, none of the prior work utilized implementation on the newer Intel's Cyclone IV FPGA hardware involving responsibility of computational components for the overall delays. In this paper, we identify the basic computational components used by these standard block encryption schemes. Computational components are the underlying logic operations used by a given hardware for these encryption schemes. The basic computational components used by these standard encryption schemes were found to be shift, substitution, permutation, and XOR operations. Our motivation is to find out which computational components (underlying logic operations) are responsible for the overall delays incurred by these encryption schemes for a given hardware platform.

2. Standard Encryption Schemes and Their Computational Components

International Business Machines (IBM) designed the Data Encryption Standard (DES) in 1973, based on the Lucifer cipher, and DES became the first encryption standard of America in 1977 [2]. Originally, computing power was not as advanced, and DES was a strong algorithm, but in 1997 as the computing power increased, DES was broken. The overview of DES is shown in **Figure 1** [6].

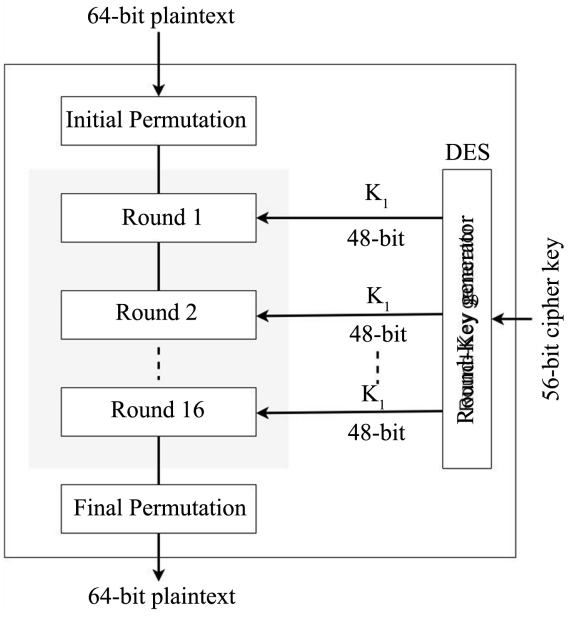

Figure 1. Overview of DES algorithm [6].

Table 1. Standard encryption algorithm AES overview.

	Key Size (Bits)	Block Size (Bits)	Year of Creation	Status
DES	64	64	1973	Obsolete
3DES	64, 128, 192	64	1998	To retire by 2023
AES	128, 192, 256	128	2001	Current Standard

3DES was a suggested alternative to make DES stronger, which is still a US standard. Triple DES, also known as 3DES, is essentially the DES encryption scheme that runs three times using three different keys. This means there are three separate keys which can be repeated or kept different, and the block chain scheme is used for simulation of 3DES. Having three different keys is the most secure while having one key is the least secure. However, in practice, 3DES uses two separate keys since it has been proven that a two key 3DES scheme has similar performance to that of a three-independent keys 3DES encryption scheme [7] as shown in **Figure 2**, which means that the third key doesn't increase the security level. For this paper and for comparison, we still use three keys to consider the worst-case scenario for 3DES encryption scheme in hardware. 3DES is more secure than DES, but it is also slower computation wise to encrypt and decrypt blocks of data. According to the National Institute of Standards and Technology (NIST) draft guidance [8], 3DES will be retired in 2023 [8] and another NIST guidance urged all users of 3DES to migrate to AES as soon as possible [9]. In this paper, we are rather comparing the hardware computational advantage of AES over other two previous standard Block encryption schemes, DES and 3DES.

In 1999 when DES was hacked in less than 24 hours, there was a need for a newer standard, and soon after, Advanced Encryption Standard (AES) became the new standard in 2001 [10] [11]. AES is an iterative symmetric block cipher, based on the Rijndael Cipher [11]. It has three different key sizes, and the key sizes will determine how many iterations the algorithm would implement. The main components of AES are similar to DES but have different names, such as RoundKey, which uses XOR operation; SubBytes, which uses a complex form of substitution; and ShiftRow, which is similar to permutation as it involves a table look up and the rearranging of the bits. Intensive computation of AES takes place in the Rijndael Mix Column segment and the implementation of Mix Columns is based on the mathematical analysis in the Galois field. Like substitute bytes, the Mix Column transformation operates on each column of the 4-byte by 4-byte matrix formed from the input 128-bit data block. Each byte of the column is mapped into a new value that is a function of all four bytes in that column. **Figure 3** shows the overall structure of the AES encryption process according to the AES standard scheme which has been adopted by the US government as the NIST standard for encryption [11]. In the last round, the Mix Column is not used according to the AES standard. The final round only includes steps of Substitute bytes, ShiftRows, and AddRoundKey to add obscurity.

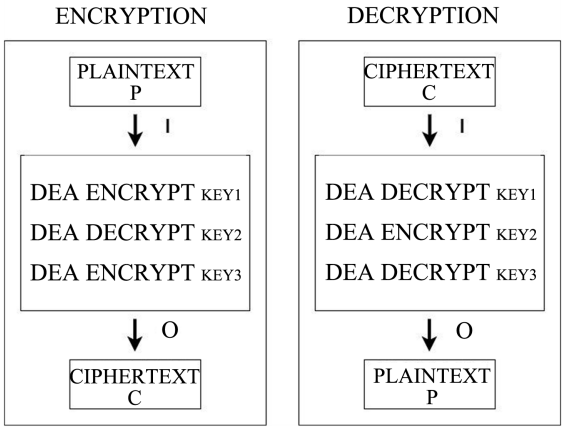

Figure 2. Overview of 3DES algorithm [7].

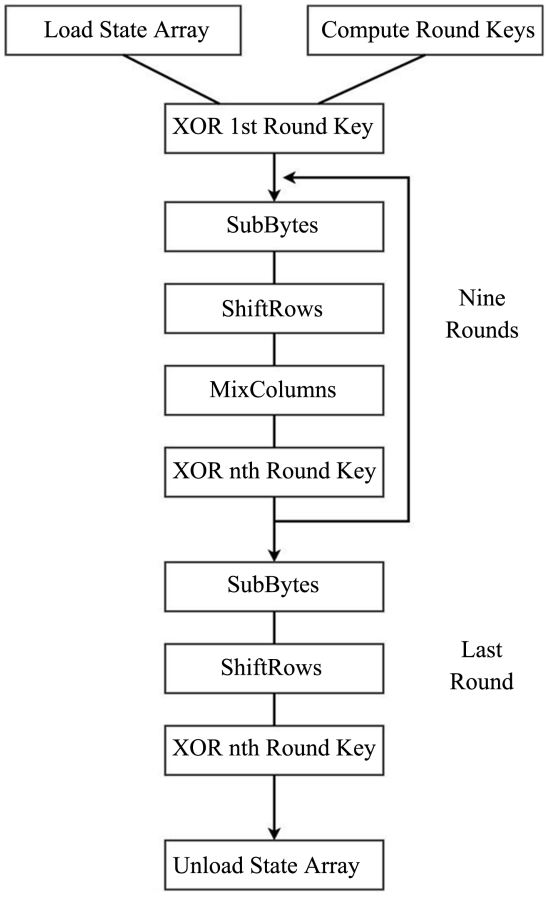

Figure 3. Overview of AES [11].

3. Analyzing Computational Components

We identified that there were four underlying computational components for these standard encryption schemes, namely: 1) Shift operations, 2) Substitution operations, 3) Permutation operations, 4) XOR operations. Analyzing these computational components being used for the DES, 3DES, and AES encryption schemes enabled us to compare the speed of the respective encryption scheme. We con-

ducted simulations to obtain Time delays for computational components for the DES encryption algorithm. We used respective multiplicative factors to obtain delays for 3 DES encryption schemes based on DES simulation results. For AES, delay information was obtained from prior work [12].

4. Method

DES, 3DES, and AES were used to compare encryption of a 128-bit plaintext, by calculating the number of times different operations were performed, and the time it took to complete the shift, substitution, permutation, and XOR operations for each of these algorithms. DES and 3DES use 64 bits of plaintext whereas AES uses 128 bits for the plaintext for one cycle of encryption. Therefore, the numbers of computational operations performed in DES and 3DES are doubled to compare with performance of AES while encrypting 128 bits of the plaintext. Evaluation was done for the number of such operations performed by these three encryption schemes on a block of 128-bit plaintext. Overall delays were computed utilizing the individual delays to perform these operations on a given hardware platform for comparison. Hardware platform chosen was Altera Cyclone IV FPGA as shown in **Figure 4** for this paper.

The Cyclone EP4CE115 device [13] equipped on the DE2-115 features 114,480 logic elements (LEs), the largest offered in the Cyclone IV E series, up to 3.9-Mbits of RAM, and 266 multipliers. In addition, it delivers an unprecedented combination of low cost and functionality, and lower power compared to previous generation Cyclone devices. We use the EDA tools available on the Altera website to evaluate our designs. These tools, the Quartus II Web Edition and the Altera University Program Simulator, allow code to be built, compiled, synthesized, simulated, and finally programmed into DE2 hardware. The simulation to compute and analyze the delay performance for these three popular block encryption algorithms used the Intel Quartus II software and Verilog Hardware Description Language for a given Altera Cyclone IV FPGA platform.

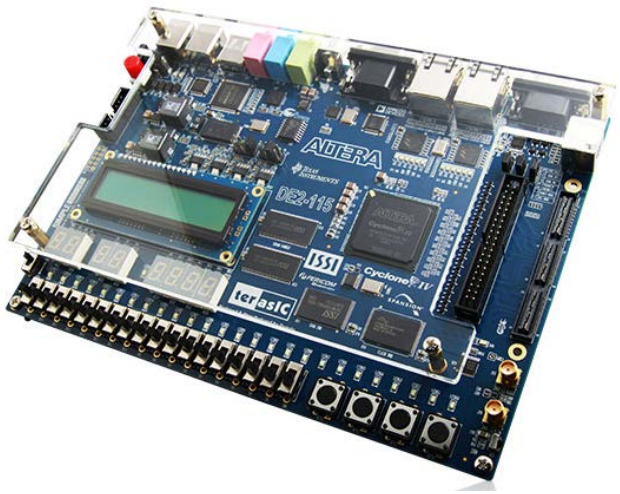

Figure 4. Altera cyclone IV 4CE115 FPGA device [13].

5. Results

Based on the DES, 3DES, and AES standard schemes which have been adopted by the US government as the NIST standard for encryption [6] [14] [15], the main computational components of the DES, 3DES, and AES encryption schemes were analyzed in this paper by running the timing simulation of all operations and calculating total time of repeated operations that were performed for each encryption scheme. The graphs demonstrate the number of times a given operation is repeated and the total time it took for the operations to be completed for the three encryption schemes. The numbers shown reflect the performance of the algorithms on a 128-bit plaintext. The reason we chose 128-bit plaintext is because AES standard [11] uses a minimum of 128-bits of plaintext. However, DES, the previous-standard [6] and 3DES standard [15] used 64-bit plaintext. To compare DES and 3DES computational performance with the AES scheme, DES and 3DES encryptions would require encryption of 128 bits of plaintext in two chunks of 64 bits of plaintext data. The number of operations to encrypt a 128-bit block of plaintext is shown in **Table 2** and **Figure 5**. The timing simulation showing delays of all operations are shown in **Figure 6**. The total time delay is shown in **Figure 7** after we calculated the time for individual components of computation.

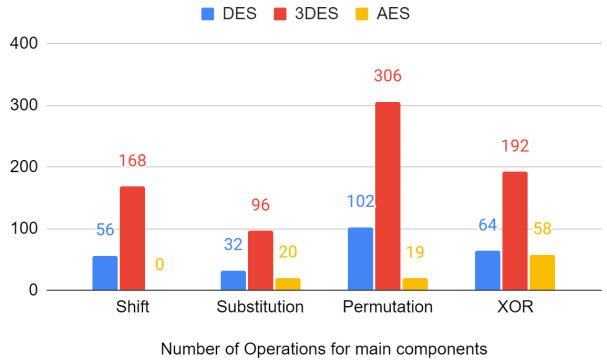

Figure 5. The total number of the operations performed by the algorithms to encrypt 128-bit of plaintext.

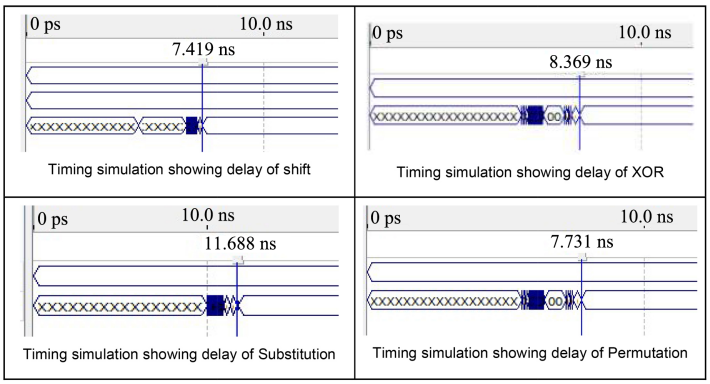

Figure 6. Timing simulation for individual components for 64-bit block of plaintext using DES.

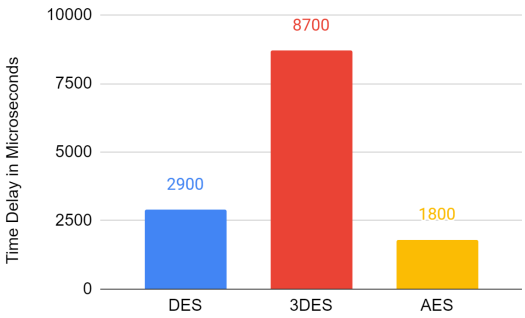

Figure 7. Total time delay of the operations in DES, 3DES, and AES.

Table 2. Total number of operations (main components) performed by three encryption algorithms for a 128-bit block of plaintext.

Number of Operations for main components	DES	3DES	AES
Shift	56	168	0
Substitution	32	96	20
Permutation	102	306	19
XOR	64	192	58

6. Discussion

Our analysis shows that the creators of AES used complex math like an irreducible prime polynomial and Galois field as a basis for the AES algorithm which reduced the number of operations such as substitutions, shift, permutation, and XOR operations. AES improved on the features of DES/3DES by reducing the number of these operations and reducing the overall encryption time needed to effectively secure data. Our analysis and hardware simulation showed that the main contributor to the delays in DES and 3 DES was the high number of permutations performed by these two algorithms, whereas such permutation operations in AES were way much reduced. AES scheme performed approximately 5 times less permutation operations compared with DES scheme, and 16 times less permutation operations compared with 3DES scheme. As a result, for a given hardware implementation, AES scheme used the shortest amount of time to encrypt a 128-bit plaintext while 3DES took the longest. AES was found to be approximately 1.6 times faster than DES and 4.8 times faster than 3DES for a given hardware platform and for a given plaintext.

AES was a faster encryption computation wise for a given hardware platform and offered a high level of security against brute force attacks compared to DES and 3DES schemes that were previously used as the encryption standard. This advantage of high security and high computation speed attributed for it to become the US and now a global standard for block encryption.

7. Conclusion

In this study, we analyzed and estimated computational advantages of the AES

data encryption scheme that may have favored it to become the US and now the global standard for block encryption. AES is computationally faster for hardware encryption processes compared to DES and 3DES while it is much stronger, security wise, compared to DES and 3DES. AES is the superior block encryption algorithm based on reduced number of repeated operations compared with previously used standards DES and 3DES. AES was found to be approximately 1.6 times faster than DES and 4.8 times faster than 3DES for a given hardware platform and for a given plaintext. This paper provides insight that the superior security performance against attacks, and faster hardware encryption speed, mainly due to reduced permutation operations, helped AES to become the encryption standard worldwide.

Acknowledgements

The support for this research is provided in part by Houston Endowment Chair for Science, Math and Technology Fellowship, Lloyd M. Bentsen, Jr. Endowment Chair in Engineering, and UTRGV's Presidential Graduate Research Assistant (PGRA) scholarship funding and High Scholars Program. Authors would also like to acknowledge helpful discussions with students in the lab.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Alanazi, H.O., *et al.* (2010) New Comparative Study between DES, 3DES and AES within Nine Factors. ArXiv abs/1003.4085, 152-155.

[2] Patila, P. and Prashant, N. (2016) A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3 DES, AES, RSA and Blowfish. *Procedia Computer Science*, **78**, 617-624. https://doi.org/10.1016/j.procs.2016.02.108

[3] Aleisa, N. (2015) A Comparison of the 3DES and AES Encryption Standards. *International Journal of Security and Its Applications*, **9**, 241-246. https://doi.org/10.14257/ijsia.2015.9.7.21

[4] Nazeh, M., Wahid, A., Ali, A., Esparham, B. and Marwan, M. (2018) A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. *Journal of Computer Science Applications and Information Technology*, **3**, 1-7.

[5] Singh, G. and Supriya. (2013) A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, **67**, 33-38. https://doi.org/10.5120/11507-7224

[6] National Institute of Standards and Technology (1999) Data Encryption Standard (DES). https://csrc.nist.gov/CSRC/media/Publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

[7] Keller, S. (1999) Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, Special Publication (NIST

SP), National Institute of Standards and Technology, Gaithersburg, MD. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151204

[8] Barker, E. and Roginsky, A. (2015) Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-131Ar1

[9] NIST (2017) Update to Current Use and Deprecation of TDEA. https://csrc.nist.gov/news/2017/update-to-current-use-and-deprecation-of-tdea

[10] NIST (2022) CVE-2016-2183 Detail (Modified). https://nvd.nist.gov/vuln/detail/CVE-2016-2183

[11] FIPS 197 (2001) Advanced Encryption Standard (AES)—NIST Technical Report. 51 p. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[12] Aaron, B., Cheng, C.-W. and Kumar, S. (2020) A Fast Implementation of the Rijndael Substitution Box for Cryptographic AES. 2020 3*rd International Conference on Data Intelligence and Security* (*ICDIS*), 3, 20-25.

[13] Terasic.com.tw/en/ (2022) Altera DE2-115 Development and Education Board. https://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&CategoryNo=165&No=502&PartNo=2#contents

[14] Barker, W. and Barker, E. (2012) Recommendation for the Triple wData Encryption Algorithm (TDEA) Block Cipher. https://doi.org/10.6028/NIST.SP.800-67r1 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf

[15] Dworkin, M., Barker, E., Nechvatal, J., Foti, J., Bassham, L., Roback, E. and Dray, J. (2001) Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.FIPS.197