Jurnal Inovatif : Inovasi Teknologi Informasi dan Informatika, 5 (1) (2022) 60-66
Journal homepage: http://ejournal.uika-bogor.ac.id/index.php/INOVA-TIF/index
E-ISSN : 2654-5519. P-ISSN : 2654-553 | DOI : 10.32832/inovatif
Published by: Universitas Ibn Khaldun

Security Analysis and Encryption Time Comparison Description on Cryptography Advanced Encryption Standard (AES)

Taufiqqurrachman [1], Dani Elsandi [2].

[1,2] Universitas Saintek Muhammadiyah

E-mail: taufiq1219@gmail.com[1], elsandidani72@gmail.com[2]

Received : May 2022	Accepted : June 2022	Published : June 2022

Abstract

AES is a cryptographic computation intended to work on 128bit, 192bit, and 256bit message blocks. The four main calculation procedures consist of a process (ShiftRows) and three substitution processes (SubBytes, MixColumns, and AddRoundKey). The AES encryption procedure is intended to perform encryption confidentially with a non-linear level of security with time complexity as effectively as possible, using a light change procedure in its implementation. On the other hand, the inverse of this procedure has low effectiveness, so the AES description procedure is slow. By examining the calculations, it was found that AES has complexity in the O(n) level for both encryption and decryption procedures. From a security check, AES has a very high level of security. From the speed correlation test results, it can be concluded that AES has a high level of effectiveness. Meanwhile, through testing encryption versus description, it can be understood that from timeliness, encryption is not equivalent to description, with the effectiveness of description being quite low.

Keywords : AES, Cryptography, Encryption, Description

Introduction

The increase in innovation in the field of computers is undeniable with the unlimited utilization of computer frameworks with which all are connected to the network through the network as a mode of correspondence for information and data. This situation has had an unsettling influence and attempted data robbery on the development of information or data, so cryptographers are expected to plan information correspondence channels as much as possible to be protected from the course of information breaches by data thieves. In general, cryptographic methods can be used to encode messages and verify messages. Advanced Encryption Standard (AES) is a cryptographic procedure or calculation of message encryption that aims to secure data or information with a symmetrical block method. AES itself was developed by Vincent Rijmen and Joan Daeman in 1997 and was set as the standard security cryptography in 2000.

Methodology

The AES calculation encryption procedure consists of 4 byte change models, namely SubBytes, ShiftRows, Mixcolumns, and a specific AddRoundKey. The first encryption procedure, the input that has been copied into the state will go through the AddRoundKey byte change. then the state will go through SubBytes, ShiftRows, MixColumns, and AddRoundKey changes repeatedly by Nr. This procedure in the AES calculation is referred to as a round function. The last round is a bit unique in relation to the previous round where in the last round, the state does not change the MixColumns.

Inovatif is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Result

Security Analysis

Table 1 AES test data with reduced round variants

Algorithm, Round	*Rounds* (*Key Size*)	*Type of Attack*	*Mem. Bytes* *Texts*		*Ops.*
MARS 16 *Core*	11C	*Amp. Boomerang*	265	270	2229
(C)	16M, 5C	*Meet-in- Midle*	8	2236	2232
16 *Mixing*	16M, 5C	*Diff. M-i-M*	250	2197	2247
(M)	6M, 6C	*Amp. Boomerang*	269	273	2197
	14	*Stat. Disting*	2118	2112	2122
	12	*Stat. Disting*	294	242	2119
RC6 20	14 -192,256	*Stat. Disting*	2110	242	2135
	14 -192,256	*Stat. Disting*	2108	274	2160
	15 (256)	*Stat. Disting*	2119	2138	2215
AES	4	*Truncated Diff.*	29	small	29
(Rijndael) 10 (128)	5	*Truncated Diff.*	211	small	240
12 (192) 14 (256)	6	*Truncated Diff.*	232	7* 232	272
	6	*Truncated Diff.*	6 *232	7* 232	244
	7 (192)	*Truncated Diff.*	19* 232	7* 232	2155
	7 (256)	*Truncated Diff.*	21* 232	7* 232	2172
	7	*Truncated Diff.*	2128- 2119	261	2120
	8 (256)	*Truncated Diff.*	2128-	2101	2204

Inovatif is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

			2119		
	9 (256)	*Related Key*	277	NA	2224
	7 (192)	*Truncated Diff.*	232	7* 232	2184
	7 (256)	*Truncated Diff.*	232	7* 232	2200
	7 -192,256	*Truncated Diff.*	232	7* 232	2140
	8 -192,256	*Amp. Boomerang*	2113	2119	2179
	6 (256)	*Meet-in- Middle*	512	2246	2247
	6	*Differential*	283	240	290
	6	*Differential*	271	275	2103
	6 -192,256	*Differential*	241	245	2163
Serpent 32	7 (256)	*Differential*	2122	2126	2248
	8 -192,256	*Boomerang*	2128	2133	2163
	8 -192,256	*Amp. Boomerang*	2110	2115	2175
	9 (256)	*Amp. Boomerang*	2110	2212	2252
	6 (256)	*Impossible Diff.*	NA	NA	2256
Twofish 16	6	*Related Key*	NA	NA	NA

One of the limitations that can be estimated to determine the degree of security of cryptographic calculations from a security angle is the check between the round speed of all cryptographic calculations and the number of rounds that are likely to be lost. Through test attack situations using reduced round variants, information is obtained as shown in Table 6. "Round(Key Size)" indicates the number of rounds that can be performed for the experiment with the associated key size. "Text" indicates the data that is expected to impact the attack, explicitly, the size of the plaintext block against the ciphertext block comparison using the secret key. The "Mem. Bytes" column shows the largest byte size of memory used when executing the attack. While the column "Operation". indicates a measure of the quantity of activity expected to carry out an attack. NA represents data information that cannot be entered. Based on this information, it was found that the side effects of the treatment test for the calculation of AES (Rijndael) were as follows:

For 128bit, 6 to 7 out of 10 total rounds can be attacked (ratio=0.6-0.7). For 192 keys, 7 out of 12 total rounds can be attacked (ratio = 0.583). Meanwhile, for a 256bit key with 14 full rounds, 7 (ratio = 0.5), 8 (ratio = 0.571), to 9 (ratio = 0.643) rounds can be attacked. Regarding the resources needed to attack AES, it

Inovatif is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

is a very expensive activity. Rijndael's level of security resistance is in a very capable class, the worst ratio is 0.7.

Time Analysis (Encryption speed and description)
Based on the test results on various platforms implementing the 128bit key block initiated by NIST, the following results are obtained:

Table 2 Encryption Time and Description

	MARS	RC6	AES (Rijndael)	Serpent	Two fish
32 bit (C)	2	1	2	3	2
32 bit (Java)	2	1	2	3	3
64 bit (C and Assembler	2	2	1	3	1
8 bit (C and Assembler	2	2	1	3	2
32 bit smartcard	2	1	1	3	3
Digital Signal Processor	2	2	1	3	1

The table above can be referenced
1 = High time level'
2 = Average time level
3 = Lowest time level
From the data above, it has a very consistent high time capability even though it will experience a decrease in capacity in 192bit and 256bit blocks.

Time Implementation Test
The following is a comparison analysis of the time between encryption and description using 6 files with different byte sizes, with several test results (repeatedly 5 times)

Table 3 Comparison of encryption and description times

No	**File Name**	**File Size** (*Byte*)	**Encryption** (Second)	Deskription (Second)
1	hassle-free form.pdf	511	1,571	2,358
2	Session Registration Form.pdf	239	0,744	1,105
3	Application design.pdf	885	2,736	4,127
4	Archives Information System and Mail Administration.pdf	715	2,201	3,319

Inovatif is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

5	security-system-implementation.pdf	443	1,375	2,054
6	docdownloader.com-pdf-journal-information-system.pdf	545	1,714	2,581

Based on the table above, the larger the file size, the more time needed for encryption and description, this happens because the larger the message block size, the greater the literacy process required.

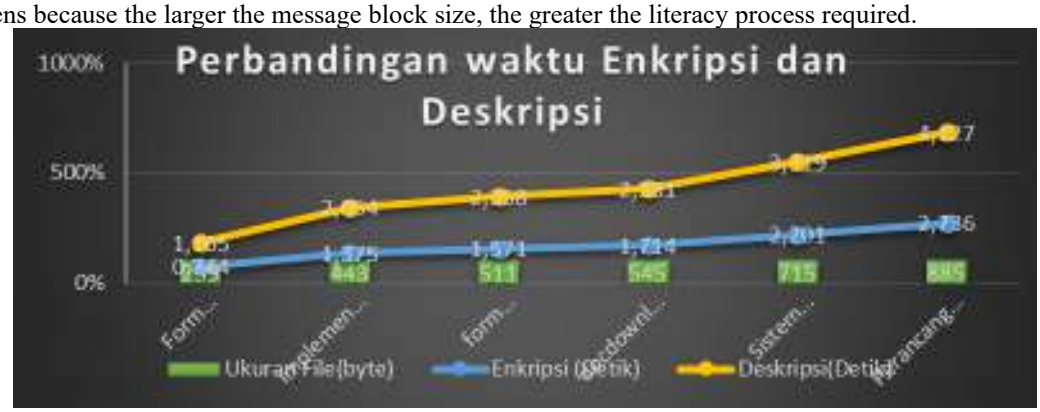
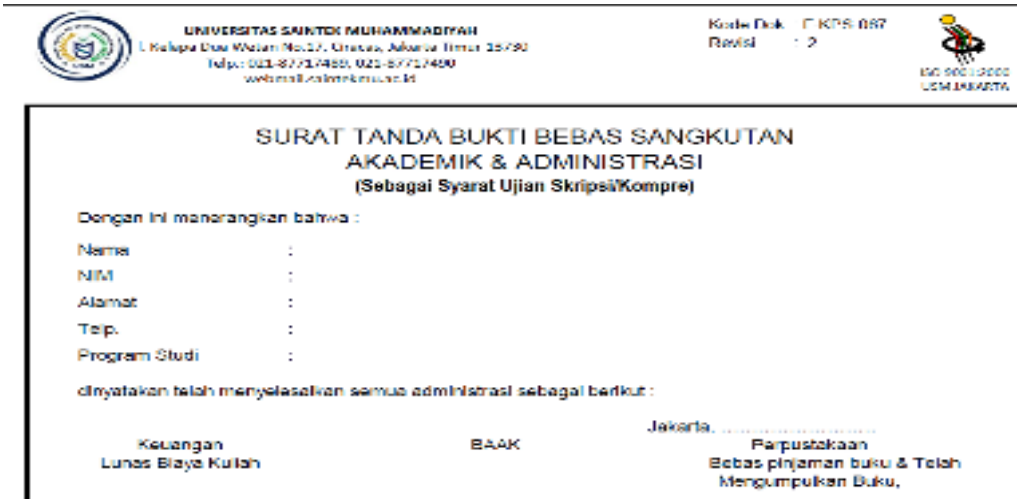


Fig 1 Comparison graph of Encryption and Description time

Implementation of AES Encryption and Description

Encryption is a procedure to change plaintext into ciphertext with the aim that the data or information in a file can be kept confidential and not easily read by cryptanalysis. While the description is the opposite of encryption that is changing the ciphertext into plaintext. So it is necessary to check whether the encrypted file when described can return to the original file in its entirety. Here is an example file before encryption



UNIVERSITAS SAINTEK MUHAMMADIYAH

SURAT TANDA BUKTI BEBAS SANGKUTAN
AKADEMIK & ADMINISTRASI
(Sebagai Syarat Ujian Skripsi/Kompre)

Dengan ini menerangkan bahwa :

Nama :
NIM :
Alamat :
Telp. :
Program Studi :

dinyatakan telah menyelesaikan semua administrasi sebagai berikut :

Jakarta, ...

Keuangan
Lunas Biaya Kuliah

BAAK

Perpustakaan
Bebas pinjaman buku & Telah Mengumpulkan Buku,

Figure 2 PDF extension letter file “free form.pdf”

Inovatif is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

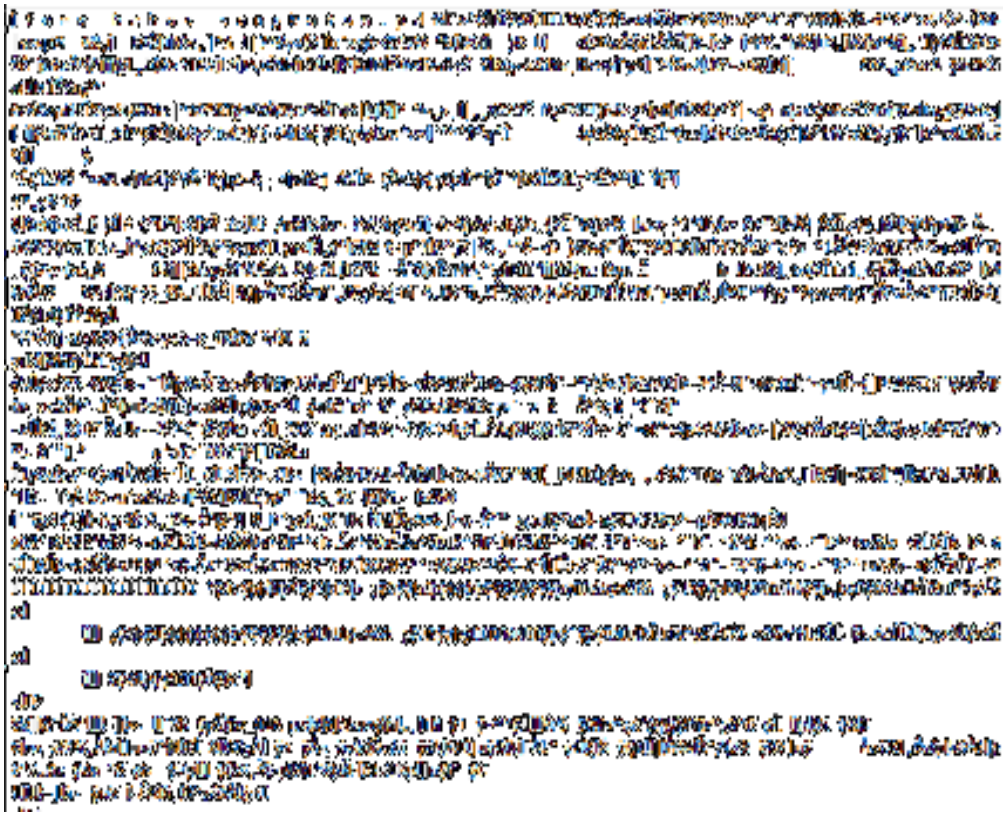
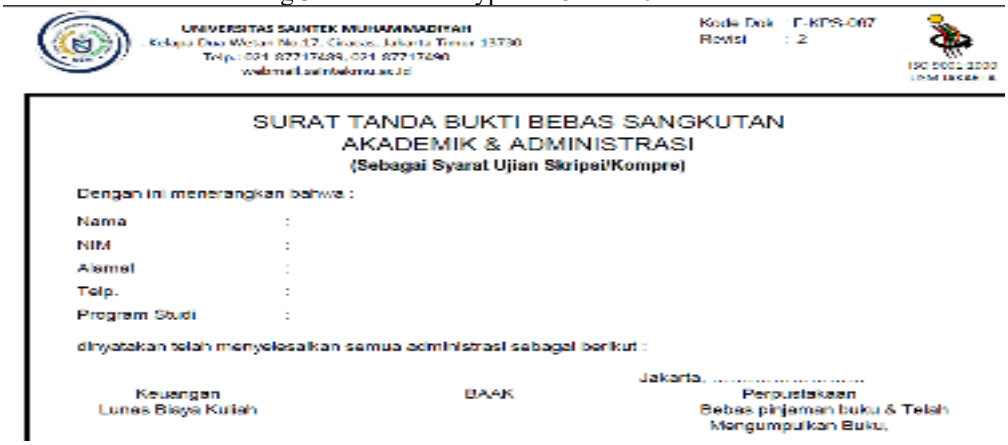


Fig 3 File after Encryption “5aaaAa04a1.enc”



UNIVERSITAS SAINTEK MUHAMMADIYAH

SURAT TANDA BUKTI BEBAS SANGKUTAN
AKADEMIK & ADMINISTRASI
(Sebagai Syarat Ujian Skripsi/Kompre)

Dengan ini menerangkan bahwa :

Nama :
NIM :
Alamat :
Telp. :
Program Studi :

dinyatakan telah menyelesaikan semua administrasi sebagai berikut :

Keuangan
Lunas Biaya Kuliah

BAAK

Jakarta, ...
Perpustakaan
Bebas pinjaman buku & Telah Mengumpulkan Buku.

Figure 4 Files that have been described as "free form.pdf"

From the sample above, the file “free form.pdf” shows that after the description of the file which was originally encrypted, the file can return to its original state without any changes, even the extension does not change after the description.

Conclusion

Based on the problems above, it can be concluded that: (1) Encrypted files can return to the source file as before, because when encrypted the system adds a header to load source file extension information. (2) Files that are encrypted and then decrypted are the same source files. (3) The time required for encryption and description is very different, due to system resources. (4) When we change the contents of the encrypted file

Inovatif is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

with the extension.aes or enc, then when the file is described there will be a content file that will not return to the original (source file), that's because file.aes is no longer an encrypted file but a file text, so there will be a header change in the file.aes or enc. (5) The Advanced Encryption Standard is O(n) in complexity and applies to encryption and decryption procedures. (6) From the above review, it is obtained that the level of security resistance is considered from the lowest ratio, between the round value of the chance of being attacked and the overall round, AES has a very high level of security.

Refrence

[1] Aditia Rahmat Tulloh, Yurika Permanasari, Erwin Harahap, Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. Jurnal Matematika UNISBA Vol 15 No 1, Mei 2016

[2] Angga Aditya Permana , Desi Nurnaningsih, Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes), Jurnal Teknik Informatika Vol 11 No. 2, Oktober 2018

[3] Denny Ardianta Sitepu, Nurhayati, S.Kom.,M.Kom, Husnul Khair. M.Kom, Implementasi Pengamanan Data Menggunakan Algoritma Advanced Encryption Standart (Aes), Jurnal Ilmiah Kaputama (Jika), Vol.6 No.1, Januari 2022

[4] Nechvatal J. *et al*. 2000. Report on the Development of the Advanced Encryption Standard (AES). Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Administration U.S. Department of Commerce. http://csrc.nist.gov/rng/. [17, Agustus 2022]

[5] Rifki Sadikin, Kriptografi Untuk Keamanan Jaringan, ANDI Yogyakarta

[6] Rinaldi Munir, Kriptografi Edisi Kedua, INFORMATIKA Bandung, April 2019

[7] Stallings W. 2003. Cryptography and Network Security Principles and Practice. Third Edition. New Jersey: Pearson Education.

[8] Ritzkal R, Setiadi D. Data Storage System Arrival and Departure Airnav Halim Perdana Kusuma Airport. Jurnal Mantik. 2021 Jun 15;5(2):555-62.

[9] Ritzkal R, Subchan M. Quality Measurement of a Web-Based Activity Management Reporting System for Email-Based Alerts. Inof the 2nd National Teknoka Seminar UHAMKA 2017.

[10] Khaerudin M, Ramdhani A, Priatna W, Warta J, Ritzkal R. Analysis of Memory Usage for Graphic Design Applications on Windows and Linux Operating Systems. Jurnal Mantik. 2022 Apr 3;6(1):102-5.

[11] Fikriyadi F, Ritzkal R, Prakosa BA. Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. Jurnal Mantik. 2020 Nov 1;4(3):1658-62.

Inovatif is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).