© 2018 IJSRST | Volume 4 | Issue 10 | Print ISSN : 2395-6011 | Online ISSN : 2395-602X
Themed Section: Science and Technology

Data Security using 128-bit Advanced Encryption Standard Algorithm

Virdyra Tasril, Andysah Putera Utama Siahaan
Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

ABSTRACT

The development of computer and telecommunications technology has experienced the significant change in progress. It can be seen that technology has become a necessity because technological advances can accomplish tasks quickly, accurately, and efficiently. In line with the development of these technologies, it increasingly changes the way people communicate. There needs to be security protection to protect data from the threat of wild parties. Cryptography is the right method to secure data. One method that can be used is the Advanced Encryption Standard (AES). This method is an excellent classical cryptographic algorithm that can be used to identify data. AES algorithm is a symmetric ciphertext block that can encrypt and decrypt information quickly. Encryption changes data that can no longer be read called ciphertext; instead, decryption is changing the ciphertext data into the original form that we know as plaintext. The AES algorithm has several key models such as 128, 192, and 256 bits to encrypt and decrypt data on 128-bit message blocks. This study uses a 128-bit key. AES encryption results can be trusted as one of the fast and powerful encryption methods.

Keywords : AES, Encryption, Decryption, Algorithm

I. INTRODUCTION

In the digital age, information system security is a matter that must be considered its security, especially internet-based. Public and global internet networks are insecure [1]. When the data is sent from one computer to another on the internet, the data will fly in the air and not impossible to pass through some other computers, which means it will give an irresponsible person the opportunity to take over or intercept the data [2]–[4] Computers that have access to locked in a limited system will not be hacked. Access is limited, and the computer is not connected outside of the local network, the computer will be safe [5].

Many methods can be used to protect data. Advanced Encryption Standard is one algorithm that can be used to protect data. This algorithm is the development of the Data Encryption Standard (DES) encryption algorithm which is considered unsafe and can be hacked quickly using today's computer speed [6][7]. The new AES algorithm is also called the Rijndael algorithm. The criteria for selecting AES are based on three main criteria such as security, price, and algorithm characteristics along with their implementation [8]. Security is the most critical factor in the evaluation. AES uses the structure of the Substitution-Permutation Network which has a higher degree of parallelism, so it is expected to be faster than the Feistel network used. The use of the AES algorithm is expected to improve data security and protect users from data theft by wild parties.

II. THEORIES

2.1 Cryptography

Cryptography comes from Greek, consisting of two syllables, "crypto", and "graphia" [9]. "Crypto" means hiding, while "graphia" means writing. Cryptography is the study of mathematical techniques related to information security aspects, such as data confidentiality, data validity, data integrity, and data authentication. But not all aspects of information security can be solved by cryptography. Cryptography can also be interpreted as science or art to maintain the security of messages [10]. Cryptography has several security aspects including:

- Confidentiality (confidentiality), guarantees that certain parties can only access the data. Confidentiality aims to protect information from all parties who are not entitled to the information.
- Authentication is an identification carried out by each party that communicates with each other, meaning that some parties who communicate must identify with each other. Information obtained by a party from another party must be identified to ensure the authenticity of the information received.
- Integrity, ensuring that every message sent must arrive at the recipient without any part of the message being replaced, duplicated, tampered with, changed the order, and added. Data integrity aims to prevent information from being changed by parties who are not entitled to the information. To ensure the integrity of this data the user must have the ability to detect data manipulation by unauthorized parties. Data manipulation referred to here includes insertion, deletion, or data replacement.
- Nonrepudiation prevents the sender or recipient from denying that they have sent or received a message. If a message is sent, the recipient can prove that the message was indeed sent by the sender listed. Conversely, if a message is received, the sender can prove that the intended party has received the message.

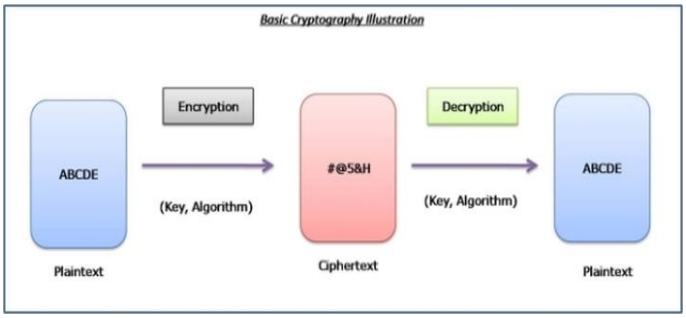

Figure 1. Basic cryptography illustration

Figure 1 [11] describes the cryptographic process taking place. The ABCD plaintext will be encrypted using the key so that it produces a ciphertext. Ciphertext will be sent to the recipient, and the recipient will decrypt the ciphertext using the decryption key it has. The decryption result is a plaintext that can be read and understood [12].

2.2 Advanced Encryption Standard

The Advanced Encryption Standard (AES) algorithm is one algorithm that can be used to encrypt data so that someone who has the encryption key can only read the original data. The example discussed this time is about the encryption and decryption of a sentence. This algorithm operates by using a state of byte type 4×4. A state is a matrix block consisting of 16 characters that will be input in the AES process. AES then repeats the transformation to convert plaintext to ciphertext according to the size of the byte used.

AES is a continuation of the standard encryption algorithm Data Encryption Standard (DES) whose validity period is considered overdue to security factors [13]. The development of computer speed is considered very dangerous to the DES, so that on March 2, 2001, the new Rijndael algorithm was established as AES. The Rijndael algorithm was later known as the Advanced Encryption Standard. After experiencing several standardization processes by NIST, Rijndael was later officially adopted as a cryptographic algorithm standard on May 22, 2002. In 2006, AES was

one of the most popular algorithms used in symmetric key cryptography. AES is a block cipher algorithm using permutation and substitution systems [14]. AES has three different key model, such as:

- AES-128 bit
- AES-192 bit
- AES-256 bit

This grouping of AES types is based on the length of the key used. The numbers behind the word AES describe the length of the key used in each type of AES. Besides, the difference between each of the AES is the number of rounds used. AES-128 uses ten rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds [15]. The outline of the Rijndael algorithm that operates on 128-bit blocks with 128-bit keys is described in the following figure.

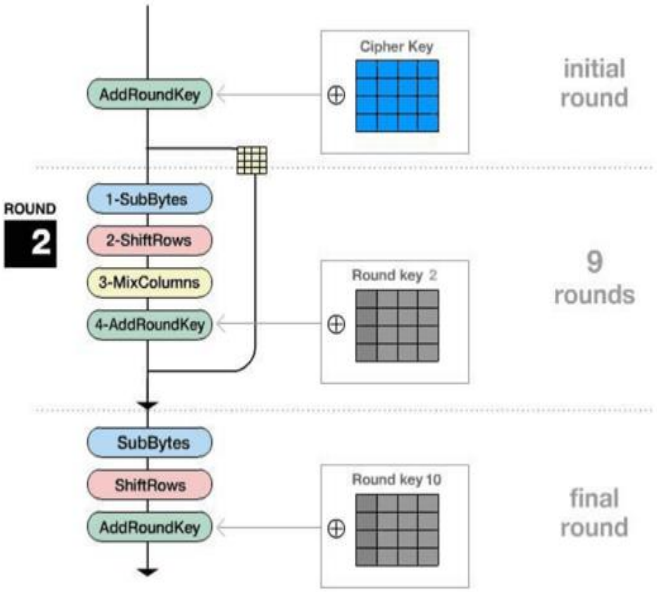

Figure 2. Sequence of the AES algorithm

Figure 2 describes the sequence of the AES algorithm process in performing the encryption process [11]. The process is explained as follows:

1. AddRoundKey: XOR between the initial state (plaintext) and the cipher key. This stage is also called the initial round.
2. Round as many times - 1 time. The process carried out in each round is:
   a. SubBytes: substitution of bytes using a substitution table (S-box).
   b. ShiftRows: shifts state array lines in wrapping.
   c. MixColumns: scrambles data in each column array state.
   d. AddRoundKey: do XOR between the state now round key.
3. Final round: the process for the last round:
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

III. METHODOLOGY

3.1 Add Round Key

Add Round Key is combining an existing text cipher with a cipher key cipher with an XOR connection. The chart can be seen in the following picture.

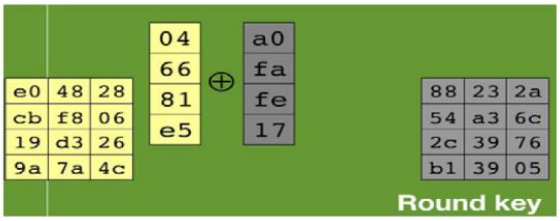

Figure 1. Add Round Key scheme

In Figure 1 on the left is the text cipher and the right is the round key. XOR is done per column such as column-1 text cipher in XOR with column-1 round key and so on.

3.2 Byte Sub

Byte Sub is an exchange of values in a matrix based on the S-Box list provided by default. Two tables become substitution tables. Each encryption and decryption has a different list of tables. Table 1 shows a list of S-Boxes when the Byte Sub encryption process is implemented. This table is different from the Sub Byte during the decryption process. For example, HEX A1 will be exchanged into HEX 32.

Table 1. List of S-Boxes for encryption

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table 2 shows a list of S-Boxes at the time of the Byte Sub decryption process implemented. For example, HEX 32 will be exchanged into HEX A1.

Table 2. List of S-Boxes for decryption

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

3.3 Mix Column

Mix Column is the last step in the AES stage. Mix Column is the most difficult step to do. Two stages must be done in this section, which part will be multiplied by the multiplication matrix and how to exchange the value in Galois Field. The multiplication matrix has two different values for the encryption and decryption process, and so does Galois Field which has two hexadecimal tables to be used in each encryption and decryption process.

Table 3. Encoding multiplication matrix (left) and decryption (right)

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

Table 3 is a matrix multiplication for the MixColomn process. Tables 4 and 5 are substitution exchanges in the MixColumn matrix (E-Table and L-Table).

Table 4. List of E-Table for the encryption process

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	03	05	0F	11	33	55	FF	1A	2E	72	96	A1	F8	13	35
1	5F	E1	38	48	D8	73	95	A4	F7	02	06	0A	1E	22	66	AA
2	E5	34	5C	E4	37	59	EB	26	6A	BE	D9	70	90	AB	E6	31
3	53	F5	04	0C	14	3C	44	CC	4F	D1	68	B8	D3	6E	B2	CD
4	4C	D4	67	A9	E0	3B	4D	D7	62	A6	F1	08	18	28	78	88
5	83	9E	B9	D0	6B	BD	DC	7F	81	98	B3	CE	49	DB	76	9A
6	B5	C4	57	F9	10	30	50	F0	0B	1D	27	69	BB	D6	61	A3
7	FE	19	2B	7D	87	92	AD	EC	2F	71	93	AE	E9	20	60	A0
8	FB	16	3A	4E	D2	6D	B7	C2	5D	E7	32	56	FA	15	3F	41
9	C3	5E	E2	3D	47	C9	40	C0	5B	ED	2C	74	9C	BF	DA	75
A	9F	BA	D5	64	AC	EF	2A	7E	82	9D	BC	DF	7A	8E	89	80
B	9B	B6	C1	58	E8	23	65	AF	EA	25	6F	B1	C8	43	C5	54
C	FC	1F	21	63	A5	F4	07	09	1B	2D	77	99	B0	CB	46	CA
D	45	CF	4A	DE	79	8B	86	91	A8	E3	3E	42	C6	51	F3	0E
E	12	36	5A	EE	29	7B	8D	8C	8F	8A	85	94	A7	F2	0D	17
F	39	4B	DD	7C	84	97	A2	FD	1C	24	6C	B4	C7	52	F6	01

Table 5. List of L-Table for the encryption process

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0		00	19	01	32	02	1A	C6	4B	C7	1B	68	33	EE	DF	03
1	64	4	E0	0E	34	8D	81	EF	4C	71	08	C8	F8	69	1C	C1
2	7D	C2	1D	B5	F9	B9	27	6A	4D	E4	A6	72	9A	C9	09	78
3	65	2F	8A	5	21	0F	E1	24	12	F0	82	45	35	93	DA	8E
4	96	8F	DB	BD	36	D0	CE	94	13	5C	D2	F1	40	46	83	38
5	66	DD	FD	30	BF	06	8B	62	B3	25	E2	98	22	88	91	10
6	7E	6E	48	C3	A3	B6	1E	42	3A	6B	28	54	FA	85	3D	BA

7	2B	79	0A	15	9B	9F	5E	CA	4E	D4	AC	E5	F3	73	A7	57
8	AF	58	A8	50	F4	EA	D6	74	4F	AE	E9	D5	E7	E6	AD	E8
9	2C	D7	75	7A	EB	16	0B	F5	59	CB	5F	B0	9C	A9	51	A0
A	7F	0C	F6	6F	17	C4	49	EC	D8	43	1F	2D	A4	76	7B	B7
B	CC	BB	3E	5A	FB	60	B1	86	3B	52	A1	6C	AA	55	29	9D
C	97	B2	87	90	61	BE	DC	FC	BC	95	CF	CD	37	3F	5B	D1
D	53	39	84	3C	41	A2	6D	47	14	2A	9E	5D	56	F2	D3	AB
E	44	11	92	D9	23	20	2E	89	B4	7C	B8	26	77	99	E3	A5
F	67	4A	ED	DE	C5	31	FE	18	0D	63	8C	80	C0	F7	70	07

3.4 Shift Rows

Shift Rows is a process that shifts or shifts each block/table element done per line. That is, the first line is not shifted, the second line is shifted by 1 byte, the third row is shifted 2 bytes, and the fourth row is shifted by 3 bytes. The shift seen in a block is a shift of each element to the left depending on how many bytes are displaced, each shift of 1 byte means to shift left once.

IV. RESULT AND DISCUSSION

This section discusses the results of encryption based on several AES processes that have been known previously. This encryption process is an action to convert plaintext to ciphertext. The illustration results of the encryption calculation are described as follows.

(Round 2 to 9 are skipped)

Round 10

==========

New State Matrix

[7A 93 09 7C]
[36 57 86 59]
[73 2B D6 30]
[8E 25 CF 15]

Sub Matrix

[DA DC 01 10]
[05 5B 44 CB]
[8F F1 F6 04]
[19 3F 8A 59]

Shift Row Matrix

[DA DC 01 10]
[5B 44 CB 05]
[F6 04 8F F1]
[59 19 3F 8A]

Key Matrix

[EE F0 42 35]
[C5 33 7C 52]
[91 B7 B0 2C]
[85 1C 9D 67]

Output Matrix Round 10

[34 2C 43 25]
[9E 77 B7 57]
[67 B3 3F DD]
[DC 05 A2 ED]

The illustration results of the decryption calculation are described as follows.

SM [0] = [34 9E 67 DC 2C 77 B3 05 43 B7 3F A2 25 57 DD ED]

State Matrix

[34 2C 43 25]
[9E 77 B7 57]
[67 B3 3F DD]
[DC 05 A2 ED]

Key [10] = [EE C5 91 85 F0 33 B7 1C 42 7C B0 9D 35 52 2C 67]

Key Matrix

[EE F0 42 35]
[C5 33 7C 52]
[91 B7 B0 2C]
[85 1C 9D 67]

Round 10

==========

New State Matrix

[DA DC 01 10]
[5B 44 CB 05]
[F6 04 8F F1]
[59 19 3F 8A]

Shift Row Matrix

[DA DC 01 10]
[05 5B 44 CB]
[8F F1 F6 04]
[19 3F 8A 59]

Sub Matrix

[7A 93 09 7C]
[36 57 86 59]
[73 2B D6 30]
[8E 25 CF 15]

Key Matrix

[E9 1E B2 77]
[1B F6 4F 2E]
[BC 26 07 9C]
[70 99 81 FA]

Round Key Matrix

[93 8D BB 0B]
[2D A1 C9 77]
[CF 0D D1 AC]
[FE BC 4E EF]

Multiplication Matrix

[0E 0B 0D 09]
[09 0E 0B 0D]
[0D 09 0E 0B]
[0B 0D 09 0E]

Mix Column Matrix

[04 FA 28 85]
[08 8F 17 50]
[5D 5B 83 5C]
[DE B3 51 B6]

(Round 9 to 2 are skipped)

Round 1

==========

New State Matrix

[76 63 76 F0]
[30 1B A4 01]
[12 30 63 20]
[FE AB 36 2B]

Shift Row Matrix

[76 63 76 F0]
[01 30 1B A4]
[63 20 12 30]
[AB 36 2B FE]

Sub Matrix

[0F 00 0F 17]
[09 08 44 1D]
[00 54 39 08]
[0E 24 0B 0C]

Key Matrix

[4E 72 6E 65]
[65 61 64 73]
[67 20 6F 69]
[61 49 6E 61]

Round Key Matrix

[41 72 61 72]
[6C 69 20 6E]
[67 74 56 61]
[6F 6D 65 6D]

The decryption calculation produces the same value as the state of the original message. It can be seen that the AES algorithm works well and quickly to perform cryptographic processes using 128-bit keys with a 4 x 4 matrix size.

V. CONCLUSION

AES or Rijndael algorithm as one of the essential algorithms certainly has various uses that have been applied or implemented in daily life which of course requires protection or concealment of information in the process. One example of using AES is file compression. The thing that is done is to encrypt the contents of the data using the AES method. The use of AES makes information protected and not hacked by wild parties. It also prevents information from being attacked by aspects that interfere with computer security. It is a big enemy in the world of computers and information because its nature is to damage and steal data.

VI. REFERENCES

[1] A. Lubis dan A. P. U. Siahaan, "Network Forensic Application in General Cases," IOSR J. Comput. Eng., vol. 18, no. 6, hal. 41–44, 2016.

[2] W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice Hall, 2005.

[3] V. Tasril, M. B. Ginting, Mardiana, dan A. P. U. Siahaan, "Threats of Computer System and its Prevention," Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, hal. 448–451, 2017.

[4] Hariyanto dan A. P. U. Siahaan, "Intrusion Detection System in Network Forensic Analysis and," IOSR J. Comput. Eng., vol. 18, no. 6, hal. 115–121, 2016.

[5] H. Ming dan S. LiZhong, "A New System Design of Network Invasion Forensics," in 2009 Second International Conference on Computer and Electrical Engineering, 2009, hal. 596–599.

[6] G. Singh dan Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," Int. J. Comput. Appl., vol. 6, no. 19, hal. 33–38, 2013.

[7] J. Daernen dan V. Rijrnen, The Design of Rijndael AES - The Advanced Encryption Standard. Berlin: Springer, 2002.

[8] A. P. U. Siahaan, How to Code: Advanced Encryption Standard in C#. Medan: Fakultas Ekonomi Universitas Panca Budi, 2018.

[9] A. Putera Utama Siahaan, E. Elviwani, dan B. Oktaviana, "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," in Proceedings of the Joint Workshop KO2PI and The 1st International Conference on Advance & Scientific Innovation, 2018.

[10] B. Forouzan, Cryptography and Network Security. New York, NY, USA: McGraw-Hill, 2006.

[11] Sukriadi Shafar, "Pengertian Dan Contoh Kriptografi dengan Proses Enkripsi dan Dekripsi," On Digital Forensics, 2016. [Daring]. Tersedia pada: http://ondigitalforensics.weebly.com/cryptography/pengertian-dan-contoh-kriptografi-dengan-proses-enkripsi-dan-dekripsi#.W7w6mxMzZZ0.

[12] Y. Kumar, R. Munjal, dan H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," Int. J. Comput. Sci. Manag. Stud., vol. 11, no. 3, hal. 60–63, 2011.

[13] N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards," Int. J. Secur. Its Appl., vol. 9, no. 7, hal. 241–246, Jul 2015.

[14] A. Arya dan M. Malhotra, "Effective AES Implementation.," Int. J. Electron. Commun. Eng. Technol., vol. 7, no. 1, hal. 01–09, 2016.

[15] S. S. Shirabadagi dan S. Nadagoud, "A new encryption methodology of aes algorithm using high speed s-box.," Int. J. Eng. Res. Electron. Commun. Eng., vol. 4, no. 7, hal. 37–42, 2017.