ISSN 2355-0082

Review on Realization of AES 256bit Encryption with Raspberry Pi

Erick Fernando[1], Surjandy[2], Muhamad Irsan[3], Hetty Rohayani AH[4], Fachruddin[5]
[1,2] Information Systems Department, School of Information Systems, Bina Nusantara University Jakarta, Indonesia 11480
[3] Information Technology Department, Universitas Islam Syekh Yusup (UNIS), Tangerang, 15117
[4]Information Technology Department, Computer science, Adiwangsa Jambi University Jambi, Indonesia
[5] Information Systems Department, STIKOM Dinamika Bangsa, Jambi, Indonesia
erick.fernando001@binus.ac.id
Surjandy@binus.ac.id[2]
hetty_mna@yahoo.com
mirsan@uni.ac.id
fachruddin@stikom-db.ac.id[5]

Accepted on 19 March 2019
Approved on 25 June 2019

***Abstract*—In this article, it aims to present the AES encryption on the Raspberry Pi mini pc. this application also aims to illustrate that this AES algorithm can be applied with small resources. This research was conducted with an experimental approach, which carried out the implementation process in mini pc hardware and xampp software (php, apache). This AES algorithm is tested by PHP programming with Apache web server with text data. The results of the study, that the AES algorithm can run well with a hard minimum, like raspberry mini pc with a very fast time in the process, speed in the process and a lot of text data. So, AES algorithm can be widely adopted for various applications from raspberry PI mini pc computers with strong practicality in information security and reliability.**

***Index Terms*—Algorithm AES, Encryption, Data security, Rasberry Pi**

I. INTRODUCTION

Nowadays, with the development of information technology makes information needs even greater. With these requirements, various devices such as computers, cellphones, and many other devices are used to produce, store and transmit information [1], [2]. As a result of this increase, making the security of information becomes very important for information privacy. Information privacy is sometimes closer to data privacy or data protection which is the relationship between collecting and distributing data around it [3]. Thus to protect this information from unauthorized users to access the data security process is needed. One solution offered is to encrypt their confidential data Encryption is a process of converting plain text messages (messages that can be understood by humans) into a cipher text message (a random message that cannot be understood by humans) and decryption is the process of changing back messages cipher text becomes plain text [4]. There are many encryption methods that have been created, for example RSA, Blowfish, Rijndael, DES, Serpent, RC4, etc. [1]. Each has its own way of encrypting messages. The rapid development of hardware and software provides a speed that allows computers to encode messages in an increasingly short time with a very complicated process that occurs behind it. One of the methods of data is done by encrypting that information. The National Institute of Standards and Technology (NIST) was developed in 2001 by Joan Daemen and Vincent Rijmen, an algorithm called Rijdael to publish the Advance encryption standard (AES) as an encryption standard [5], [6].

The AES algorithm is an algorithm that provides data security and process speed to encrypt data. Encrypting data blocks of 128 bits into 10, 12 and 14 rounds depends on the size of the key size used and has been carefully tested in many security applications [7], [8]. AES was built with the intention of securing government in various fields. The AES algorithm is designed to use a minimum cipher block from 128bit input blocks and supports 3-key-sizes, namely 128bit, 192bit, and 256bit key [8]. In this study will analyze the process of performance of the AES algorithm in a raspberry PI display. Where raspberry PI is a small pc device with limited capacity, so it can help workmanship or processors the things needed from the user with the desired data.

II. LITERATURE REVIEW

A. *Encryption and Description*

Encryption is a technology that is used to protect sensitive data by using a combination of private or public keys that can hide sensitive user data and activity from ciphertext [7]. While the decrypt is the process of returning the confidential data to its original data.

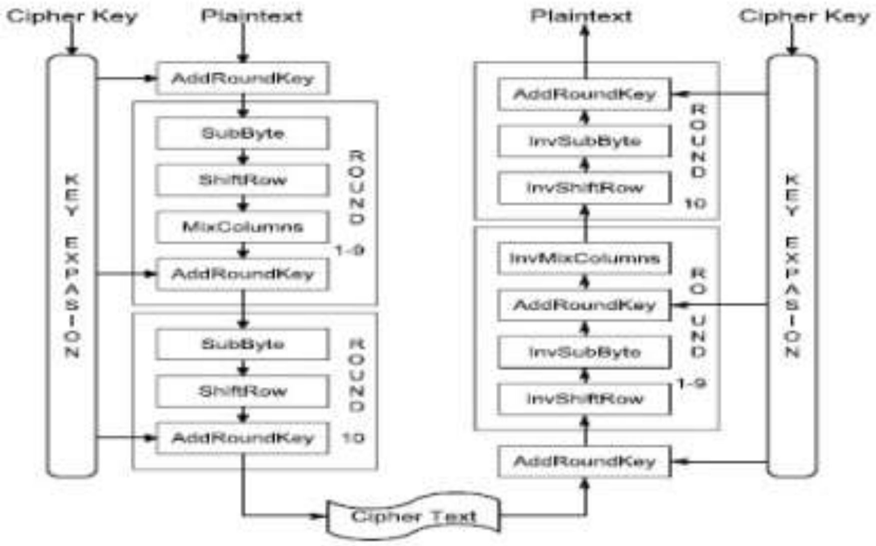


Fig 1 . AES Encryption and Description Standart [9]

B. Advance encryption standard (AES)

The AES algorithm is an algorithm that provides data security and process speed to encrypt data. Encrypting data blocks of 128 bits into 10, 12 and 14 rounds depends on the size of the key size used and has been carefully tested in many security applications [7], [8]. The AES algorithm is designed to use a minimum cipher block from 128bit input blocks and supports 3-key-sizes, namely 128bit, 192bit, and 256bit key [8].

The encryption process in the AES algorithm consists of 4 types of bytes transformation, namely SubBytes, ShiftRows, Mixcolumns and AddRoundKey. In the first stage of the encryption process, the input that has been copied into the state will undergo a byte transformation AddRoundKey. Furthermore, the state will undergo repeated SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations as much as Nr. This process that occurs in the AES algorithm is called a round function [10].

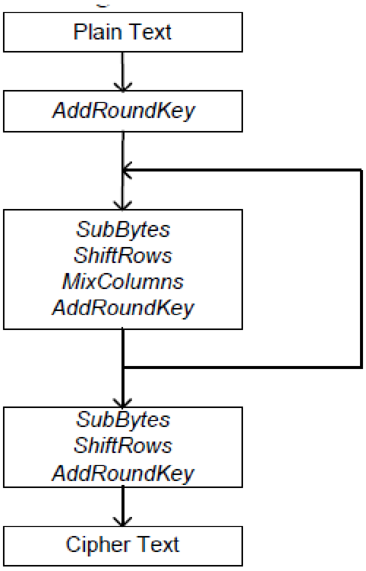


Fig 1. Diagram Alir Proses Enkripsi AES

The AES algorithm uses a surround function consisting of four different byte-oriented transformations. For encryption purposes, four rounds consist of [1]:

1. Substitute byte
2. Shift row
3. Mix columns
4. Add round key

While the decryption process itself is a reverse process of the encryption process consisting of [1]:

1. Inverse shift row
2. Inverse substitute byte
3. Add round key
4. Inverse mix columns

C. Raspberry PI board

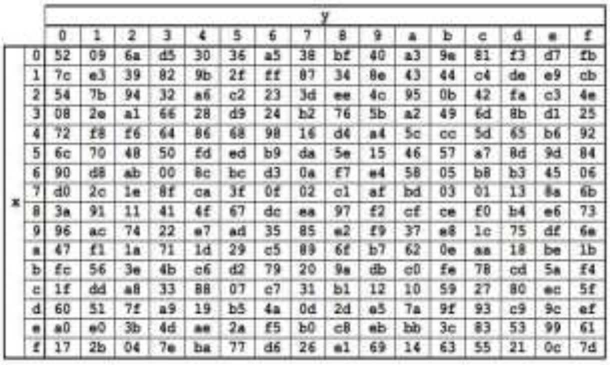
The Raspberry Pi is a mini-computer device the size of a credit card. The Raspberry Pi has a Broadcom

BCM2835 chip (SoC) system, which includes the ARM1176JZF-S 700 MHz processor (firmware includes a number of "Turbo" modes so users can try overclocking, up to 1 GHz, without affecting the warranty), GPU VideoCore IV, and originally shipped with 256 megabytes of RAM, then upgrading to 512MB which until now has grown even more rapidly. This allows this device to be used as an educational tool for people of all ages and skill levels. The interest in the Raspberry Pi device is extraordinary and has far exceeded expectations. Professional. IT, electronic experts and newcomers are all eager to 'put' their hands on this small device and everyone agrees, this device will become big and growing [11].

III. Methodology

In this study, the experimental approach was carried out, where the implementation was carried out and carried out testing directly on mini pc hardware, namely raspberry PI and xampp software. In the initial encryption process that occurs in the AES algorithm, among others:

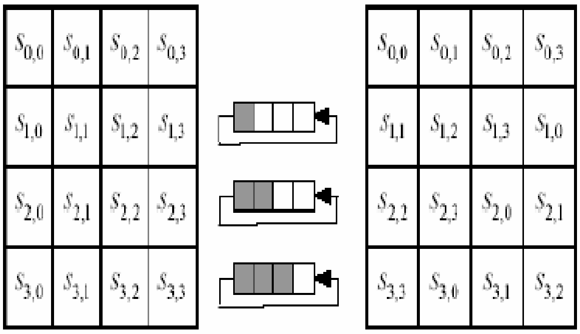
SubBytes is a byte transformation where each element in the state will be mapped using a substitution table (SBox).



		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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

Fig 2. *Rijndael S-boxes*

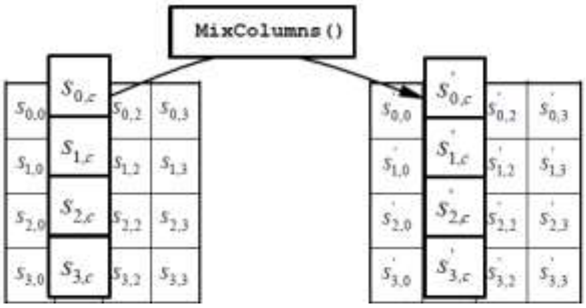
Transformation shiftrows is basically a process of shifting bits where the leftmost bit will be moved to the rightmost bit (bit rotation). This transformation is applied to line 2, row 3 and row 4. Line 2 will experience a bit shift once, while row 3 and row 4 each experience bit shifts twice and three times.



$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,1}$ $S_{1,2}$ $S_{1,3}$ $S_{1,0}$
$S_{2,2}$ $S_{2,3}$ $S_{2,0}$ $S_{2,1}$
$S_{3,3}$ $S_{3,0}$ $S_{3,1}$ $S_{3,2}$

Fig 3. *Transformasi ShiftRows*

MixColumns operates each element in a column in the state.



MixColumns()
$S_{0,0}$ $S_{0,c}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,c}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,c}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,c}$ $S_{3,2}$ $S_{3,3}$
$S'_{0,0}$ $S'_{0,c}$ $S'_{0,2}$ $S'_{0,3}$
$S'_{1,0}$ $S'_{1,c}$ $S'_{1,2}$ $S'_{1,3}$
$S'_{2,0}$ $S'_{2,c}$ $S'_{2,2}$ $S'_{2,3}$
$S'_{3,0}$ $S'_{3,c}$ $S'_{3,2}$ $S'_{3,3}$

Fig 4. *MixColumn Transformation*

AddRoundKey, In the process of AES encryption and decryption the AddRoundKey process is the same, a round key is added to the state with the XOR operation. Each round key consists of Nb word where each word will be summed with the word or corresponding column of the state.

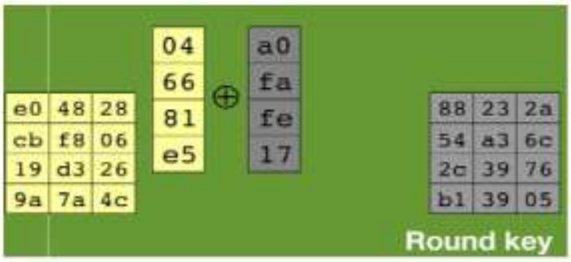


Fig 5. Add Round Key.

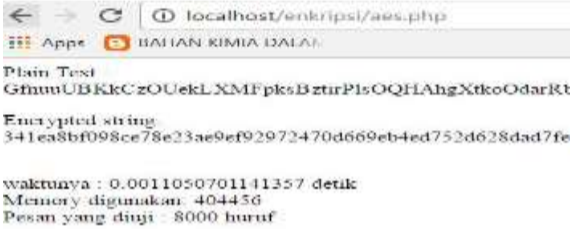
IV. Analysys And Results

In analyzing the analysis process using raspberry PI type B using PHP programming and Apache webserver. The process of analyzing the performance of the AES algorithm prepares 6 files that contain data sets with different sizes and contents, then the authors conduct experimental experiments based on complex criteria in crypto analysis according to Kaisar Siregar [12], which has 3 criteria: time, memory and data. Data to be used as input are 6 files with details as follows:

1. Data 1 is an 8 kb file containing a combination of uppercase (capital) and lowercase of 8,000 alphabet.
2. Data 2 is a 16 kb file containing a combination of uppercase (capital) and lowercase of 16,000 alphabet.
3. Data 3 is a 24 kb file containing a combination of uppercase (capital) and lowercase of 24,000 alphabet.
2. Data 4 is a 32 kb file containing a combination of uppercase (capital) and lowercase of 32,000 alphabet.
3. Data 5 is a 40 kb file containing a combination of uppercase (capital) and lowercase of 40,000 alphabet.
4. Data 6 is a file size of 47 kb containing a combination of uppercase (capital) and lowercase of 48,000 alphabet.

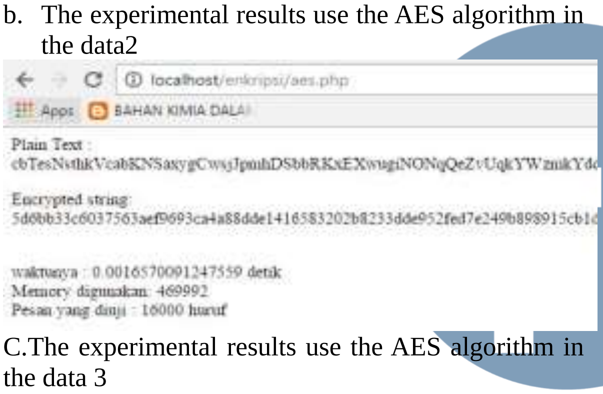
In implementation use data 1 as input into the AES algorithm to see how much speed and memory are used by each algorithm in encrypting data 1, data 2, data 3, data 4, data 5 and data 6. This aims to see how fast and how much each algorithm encrypts a message to determine the performance of each algorithm in encrypting a message. the implementation process can be as follows :

a. The experimental results use the AES algorithm in the data1



```
localhost/enkripsi/aes.php

Plain Text
GfnuuUBKkCzOUekLXMFpksBztirP1sOQHAhgXtkoOdarKt

Encrypted string
341ea8bf098ce78e23ae9ef92972470d669eb4ed752d628dad7fe


waktunya : 0.0011050701141357 detik
Memory digunakan  404456
Pesan yang diuji : 8000 huruf
```

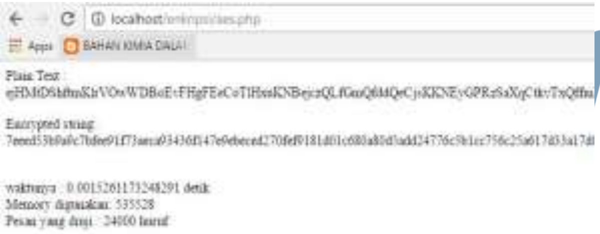
b. The experimental results use the AES algorithm in the data2



```
localhost/enkripsi/aes.php

Plain Text :
cbTesNsthkVcabKNSaxygCwsjJpmhDSbbRKxEXwugiNONqQeZvUqkYWzmkYdc

Encrypted string:
5d6bb33c6037563aef9693ca4a88dde1416583202b8233dde952fed7e249b898915cb1d


waktunya : 0.0016570091247559 detik
Memory digunakan: 469992
Pesan yang diuji : 16000 huruf
```

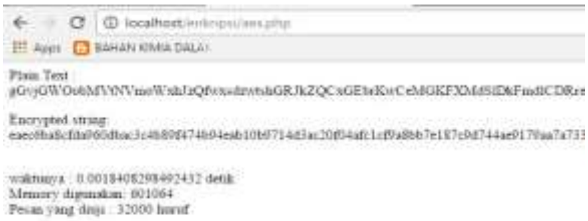
c. C.The experimental results use the AES algorithm in the data 3

d.



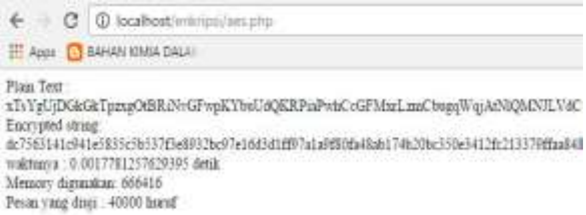
```
localhost/enkripsi/aes.php

Plain Text :
eHMtD6hfmKlrVOwWDBoEtFHgFEeCoTIHxsKNBejczQLfGmQ6MQeCjsKKNEyGPRzSaXyCtkvTxQffu

Encrypted string
7eeed53b0a0c7bdee91f73aea93436f147e9ebeced270fef9181d01c680a80d3add24776c9b1ec756c25a617d83a17d

waktunya : 0.0015261173248291 detik
Memory digunakan: 535528
Pesan yang diuji : 24000 huruf
```

e. D.The experimental results use the AES algorithm in the data4



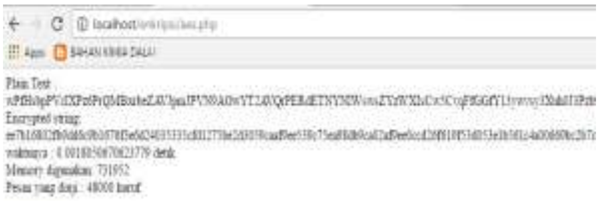
```
localhost/enkripsi/aes.php

Plain Text
gGvjGWOubMVYNVmoWshJzQfvxsdrwtshGRJkZQCxGEtaKurCeMGKFXMdSIDkFmdlCDRz

Encrypted string:
eaec8ba8cfda960dbac3c4b89f474b94eab10bf714d3ac20f04afc1cf9a8bb7e187c9d744ae9170aa7a733

waktunya : 0.0018408298492432 detik
Memory digunakan: 601064
Pesan yang diuji : 32000 huruf
```

f. E. The experimental results use the AES algorithm in the data5



```
localhost/enkripsi/aes.php

Plain Text :
xTsYgUjDGkGkTpzxgOtBRiNrGFwpKYbuUdQKRPiaPwhCcGFMxrLzmCbugqWqjAtNlQMNJLVdC
Encrypted string:
dc7563141c941e5835c5b537f3e8932bc97e16d3d1ff97a1a9f80fa48ab174b20bc350e3412fc213379ffaa84
waktunya : 0.0017781257629395 detik
Memory digunakan: 666416
Pesan yang diuji : 40000 huruf
```

g. The experimental results use the AES algorithm in the data6



```
localhost/enkripsi/aes.php

Plain Text
[illegible]
Encrypted string:
[illegible]
waktunya : 0.0018050670623779 detik
Memory digunakan: 731952
Pesan yang diuji : 48000 huruf
```

To make it easier to see the data the author will present the data above into the following table:

Table 1. Experment Result

Data	Speed (seconds)	Using memory (byte)
Data 1	0,001105	404.456
Data 2	0,001657	469.992
Data 3	0,001526	535.528
Data 4	0,001840	601.064
Data 5	0,001778	666.416
Data 6	0,001805	731.952
Average	**0,001619**	**568.235**

From the results of the implementation process and based on the results of the experiments conducted it can be concluded that

1. Ciphertext from the same letter in the plaintext produces a different letter output, for example in the image the results of point k above above in the plaintext we can see the letter "G" in the order of 9 and 11 produce 2 different letters on the ciphertext-output where the 9th "G" in the plaintext produces "1" and "G" in the 11th plaintext produces "9" in the 11th ciphertext, it shows us that even though the message (plaintext) has the same letter but not necessarily produce the same output, making it difficult for us to guess a message just by knowing the output (ciphertext) only without knowing the message key.
2. The time needed by the AES algorithm in encrypting a data tends to be more erratic on the magnitude of the data (messages) that are processed because in some of the above experimental results we can see that there are some data that process more messages but are faster than messages that fewer in number.

Memory usage in the AES algorithm is directly proportional to the number of messages tested where the memory needed will be greater along with the size of the message being tested.

V. Conclusion

This study resulted that the AES algorithm can be suitably implemented on raspberry PI one onther mini pc devices. This implementation process can be with high speed applications in real time. This process is carried out on the Ciphertext of the same letter in the plaintext resulting in different letters output, it shows us that even though the message (plaintext) has the same letter but does not necessarily produce the same output making it difficult for us to guess a message just by knowing the output (ciphertext) alone without knowing the message key. In this process, too, the time needed for the AES algorithm to encrypt data tends to be more erratic about the size of the data (messages) that are processed because in some of the experimental results we can see that there are more data processing messages but faster than with fewer messages. Memory usage in the AES algorithm is directly proportional to the number of messages tested where the memory needed will be greater along with the size of the message being tested. So the AES algorithm can be widely adopted for various applications from mini pc computers raspberry PI with strong practicality in information security and reliability

References

[1] G. Chaitanaya, B. Keerthi, A. Saleem, A. T. Rao, and K. T. P. S. Kumar, “An Image Encryption and Decryption using Chaos Algorithm,” *IOSR J. Electron. Commun. Eng. Ver. II*, vol. 10, no. 2, pp. 2278–2834, 2015.

[2] K. Wu, Y. Zhang, W. Cui, and T. Jiang, “Design and implementation of encrypted and decrypted file system based on USBKey and hardware code,” *AIP Conf. Proc.*, vol. 1839, no. May, 2017.

[3] M. G. Michael and K. Michael, *Uberveillance and the social implications of microchip implants : emerging technologies*. 2014.

[4] W. Stallings, *Cryptography and Network Security (2Nd Ed.): Principles and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1999.

[5] Y. R. A. Kannan, S. A. Prasad, and P. Varalakshmi, “Cognitive symmetric key cryptographic algorithm,” *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 85, no. PART 2, pp. 50–60, 2012.

[6] T. S. Ruprah, “Advance Encryption and Decryption Technique using Multiple Symmetric Algorithm,” *J. Inf. Secur. Res.*, vol. 7, no. 2, pp. 62–68, 2016.

[7] S. P. Singh and R. Maini, “Comparison of Data Encryption Algorithms,” *Int. J. Comput. Sci. Commun.*, vol. 2, no. 1, pp. 125–127, 2011.

[8] S. M. Seth and R. Mishra, “Comparative Analysis Of Encryption Algorithms For Data Communication,” vol. 4333, pp. 292–294, 2011.

[9] G. Berad, A. Jaggi, and V. Jagadale, “REVIEW ON IMPLEMENTATION OF AES ALGORITHM FOR,” no. 2, pp. 75–78, 2016.

[10] M. P. Widi, “Pengamanan Kunci Jawaban Sertifikasi CCNA Menggunakan Advanced Encryption Standard (AES) dan Mode Operasi Cipher Block Chaining,” pp. 1–9.

[11] E. Fernando, “Automatisasi Smart Home Dengan Raspberry Pi Dan Smartphone Android,” *Konf. Nas. Ilmu Komput.*, vol. 1, no. December 2014, pp. 1–5, 2014.

[12] K. Siregar, “Aplikasi algoritma Brute Force Dalam Proses Cryptanalysis,” *Makal. IF2251 Strateg. Algoritm.*, no. 40, 2008