PARAMETER
JURNAL MATEMATIKA, STATISTIKA DAN TERAPANNYA

e-ISSN. 2829-6303
Vol 04 No 2, August 2025
Page 261-274

Implementation of the Advanced Encryption Standard (AES) Algorithm to Protect Children Personal Data

Dyana Patty[1]*, Selvy Marchia Kololu[2], Novita Dahoklory[3], Zeth Arthur Leleury[4]

Mathematics Study Program, Science dan Technology Faculty, Pattimura University,
Ir. M. Putuhena street , Ambon, 97234, Maluku, Indonesia.

E-mail Correspondence Author: *dyanapatty57@gmail.com*

Abstract

The rapid development of information and communication technology is inseparable from data security issues. In today's digital age, one type of data that is vulnerable to cyber security threats is children's personal data. Protecting children's personal data is an important priority in safeguarding their privacy and digital security. This research applies AES-256 on a website to secure personal data within the database. AES-256 is a symmetric cryptographic and block-ciphertext algorithm that can encrypt and decrypt data/information with a key size of 256 bits, which can be used to secure data. Results demonstrate that AES-256 effectively maintains full name, NIK and password confidentiality and integrity, rendering the encrypted ciphertext difficult to interpret or access. This study provides a basis for advancing data security and related applications which strengthens the complexity of encrypted children's personal data against cryptanalysis attacks.

Keywords: *AES-256, cryptography, personal data*

: https://doi.org/10.30598/parameterv4i1pp261-274

Research Ariticle • *Open Acces*
Email: jurnalparameter@gmail.com
Homepage: https://ojs3.unpatti.ac.id/index.php/parameter

Submitted: June 2025
Accepted: August 2025

1. INTRODUCTION

According to Indonesia Law No. 27 Year 2022, personal data refers to information about an identified or identifiable individual, either alone or in combination with other information, directly or indirectly, through electronic or non-electronic systems. Under this law, one specific category of personal data that must be protected is children's data. The children's data that must be protected includes full name, parents' names, place and date of birth, address, gender, religion, phone number, health history, and photographs [1].

In today's digital age, where information and communication technology has developed rapidly, children's data has become one of aspects that vulnerable to cyber security threats [2],[3],[4]. There have been many incidents of child data misuse. For example, in 2000 in the United States, YouTube was fined $170 million for illegally collecting children's data without parental consent. A similar incident occurred in the United Kingdom in 2020, where the UK Data Protection Authority, the Information Commissioner's Office (ICO), imposed a fine of 12.7 million pounds sterling (approximately Rp236.7 billion) on TikTok for allowing approximately 1.4 million children under the age of 13 to use the platform. In Indonesia, one of the data breaches involving minors was the data leak at the Indonesian Child Protection Commission (KPAI) in 2021. The case began with the discovery of a file being sold on the RaidForums website titled "Leaked Database KPAI." Additionally, in 2022, a report by Narasi and Human Rights Watch (HRW) along with 14 media outlets from 23 countries titled "Children's Data Sold by Educational Apps" revealed how many edtech platforms worldwide secretly collect children's data and sell it to advertising companies.

In order to protect children's data from threats such as those mentioned above, data security is very important considering the number of attacks on computer systems and networks [5]. One of the most commonly used data security techniques is cryptography. Cryptography is a field of science and art that aims to store messages, data, or information securely. In cryptography, there is an encryption process that will change the original message (plaintext) into an unreadable and difficult to understand message (ciphertext) and to change the difficult to understand message (ciphertext) into the original message (plaintext) is used decryption techniques. This encryption and decryption process uses mathematical techniques that are adapted to the algorithm used. There are many cryptographic algorithms that can be used.

Based on the nature of the key, cryptographic algorithms are divided into two categories: symmetric-key and asymmetric-key. Symmetric cryptography is a data security method that uses a single key for both encryption and decryption. In this system, both the sender and receiver share the same key, which is used to convert the original information into an unreadable format and then revert it back to its original form in the same way. The use of a single key in symmetric cryptography makes it more efficient and faster than other methods, such as asymmetric cryptography.

One popular example of a symmetric-key cryptographic algorithm is the Advanced Encryption Standard (AES) [6],[7]. The AES encryption process involves several steps, including byte substitution, shift row, mix column, and add round key. Byte substitution involves replacing each byte of data with another byte from a predefined substitution table. Shift row involves shifting rows of data within a block. Mix column involves performing a linear operation on columns of data within a block. Finally, add round key involves a bitwise XOR operation between a data block and its corresponding encryption key.

The AES decryption process involves steps that are reversion of encryption steps. Using same decryption key, the encrypted data block can be restored to its original form. The algorithm has a data block length of 128 bits with variable key sizes of 128-bit (called AES-128), 192-bit (AES-192), and 256-bit (AES-256). The number of rounds to complete the process of encryption depends on key size: 10 rounds for AES-128; 12 rounds for AES-192; and 14 rounds for AES-256 [8],[9]. It is believed that longer key size makes higher cryptographic strength [10]. In other hand, higher level of complexity of a cryptographic algorithm needs greater computation power to process data structures.

The AES-256 algorithm is one of the most widely used encryption algorithms for securing data. AES-256 is based on a complex substitution and permutation system involving complex mathematical operations [11],[12],[13]. This algorithm is designed to provide a high level of security and has a cryptographic strength that can protect data from attacks and unauthorized access [14],[15]. Some applications of the AES-256 cryptographic algorithm include the 7-Zip data compression process, which encrypts the data using the AES-256 method, where the key is generated through a hash function. This combination protects information or data and prevents it from being easily damaged, especially by viruses, which are one of the biggest enemies in computer world because of their nature of destroying data. In addition, AES-256 is also applied to DiskCryptor software, which is useful for encrypting the entire contents of a disk/partition on a computer.

Previous research on AES-256 cryptography was conducted by Ega Shela Marsiani in 2022 [1], entitled "Implementation of the AES 256-BIT GCM Security System to Secure Personal Data." This research utilized the AES-256 cryptographic encryption and decryption method on Windows to protect personal data. In addition, in the same year, research on the AES-256 cryptographic algorithm was also conducted by Irfan Kurnia Nurhareza with the title "Application of the AES-256 Cryptographic Algorithm to Secure Web-Based Documents in Belendung Village" [13].

In this research, a web-based application was created implementing the AES 256 bit cryptographic algorithm to secure important documents, work documents, community data, letters and work results in Belendung Village so that there is no taking or theft of important documents and work reports by parties who want to misuse important documents, work documents, community data, letters and work results. In this research, the AES-256 algorithm, which is considered the most secure because it uses a 256-bit key length that is very difficult to penetrate by brute force attacks, will be implemented for the security of children's personal data such as full name, national identification number (NIK), and password protection on created website.

2. METHOD

According to [16], the AES algorithm uses substitution and permutation, as well as several rounds (repeated ciphers), where each round uses a different key called a round key. The AES algorithm defines key lengths of 128, 192, and 256 bits. The AES algorithm itself has three parameters, namely:

1. Plaintext: a 16-byte array that contains the input data.
2. Chipertext: a 16-byte array that contains the encryption result.
3. Key: a 32-byte array that contains the ciphering key (also called the cipher key).

Furthermore, AES uses four types of transformations, namely:

1. SubBytes, as a substitution transformation.
2. ShiftRows, as a permutation transformation.

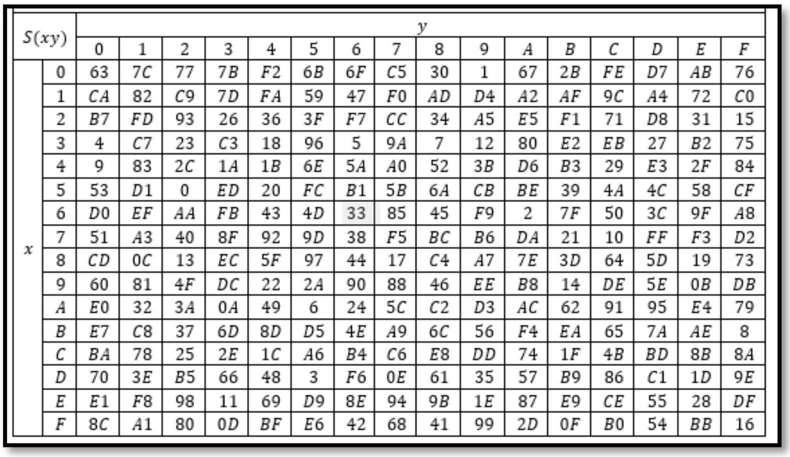
3. MixColumns, as a diffusion (mixing) transformation.
4. AddRoundkey as a key addition transformation.

Before entering the encryption-decryption process, there is a key expansion process in which operations are carried out to obtain the round keys, which is a key that used in each round of both the encryption and decryption processes. In this process, a Round Constant or Rcon is used, where Rcon is an array of constants used during the key expansion process to help generate round keys from the main key. The key expansion stage also involves a bit substitution (SubBytes), where hexadecimal bits are substituted with bytes from the S-box table. The steps of the key expansion process are explained as follows:

1. Determine the key that will be used in the encryption and decryption process.
2. Convert the key into its hexadecimal form.
3. Check the key length; if it is less than 32 bytes, apply PKCS#5 padding.
4. Insert the key into a 4 × 4 square matrix.
5. Divide the key into 4 blocks, which will be initialized as $w[i]$ where $i = 0, 1, 2, 3, \dots, 43$ to generate the complete expanded key.
6. Perform the RotWord process by taking the last block of round [i−1], shifting it left by one byte, substituting each byte with the corresponding value from the S-box table, then applying an XOR operation with the corresponding RCON value.
7. Perform an XOR between the first block of the previous round key and the first block of the new round key. The following blocks are then generated by XORing each block with the previous one in sequence.
8. Repeat the process until round key 14 is generated, where each round key will be used in every round of the encryption and decryption process.

Next, the AES-256 algorithm is divided into the encryption process, with the algorithm steps as follows:

1. The first step, known as the **initial round**, is to add the round key (round key 1) to the plaintext block using the XOR operation.
2. The main rounds are performed over 13 rounds, each of which includes the following four main transformations:
   a. Subbytes is a transformation that involves a substitution process with a lookup table called an s-box. The use of a lookup table as an extension to simplify the transformation process. The s-box lookup table can be seen in **Figure 1**. Substitution is performed based on the stateplain index value, then used to obtain a new value based on the similarity of the row and column indexes in the new stateplain.



S(xy)		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	1	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	4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
	4	9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	2	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	6	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	8
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	3	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	80	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 1. Substitution Box

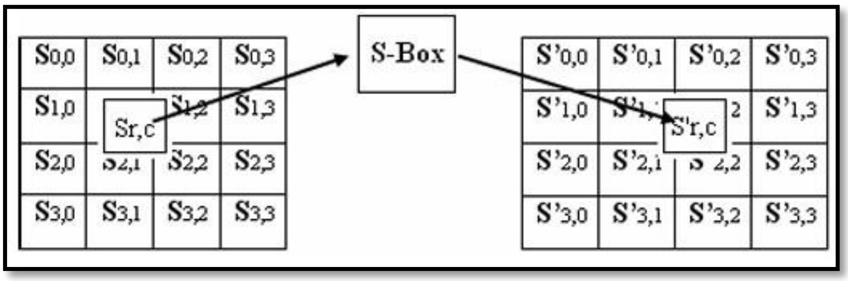
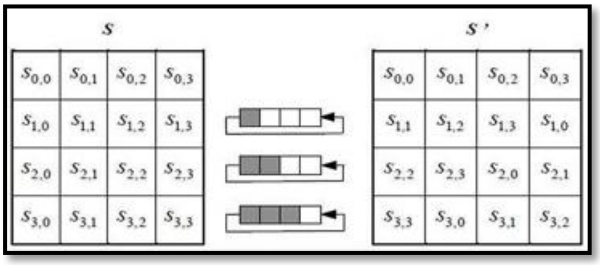


Figure 2. SubBytes Transformation

b. ShiftRows, a permutation transformation where each row in the state block is cyclically shifted to the left. The first row remains unchanged, the second row is shifted one position, the third row two positions, and the fourth row three positions. In this implementation, a modification is applied: the first row remains unchanged, the second row is shifted two positions, the third row three positions, and the fourth row one position.



s			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

s'			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

Figure 3. ShiftRows Transformation

c. MixColumns, a diffusion transformation where each column in the state matrix is operated on with a mix column matrix.

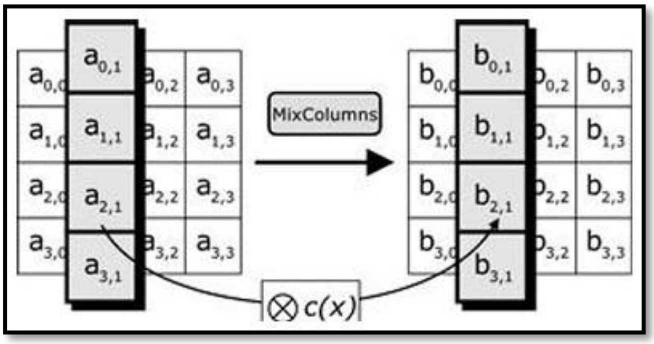


Figure 4. **MixColumns Transformation**

d. AddRoundKey, a key addition transformation where the state matrix is combined with the round key using the XOR operation.

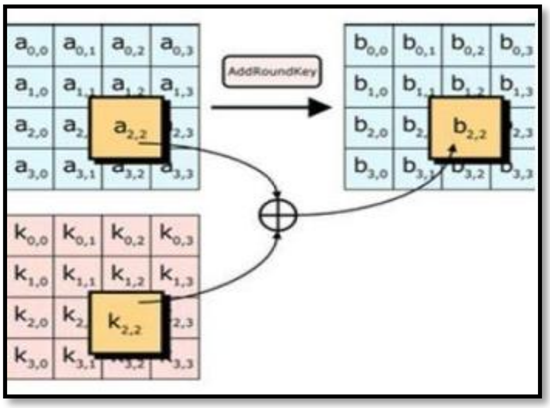


Figure 5. **AddRoundKey Transformation**

3. In the final round (the 14th round), only three transformations are applied in sequence: SubBytes, ShiftRows, and finally AddRoundKey — each of which has been explained in the previous steps.

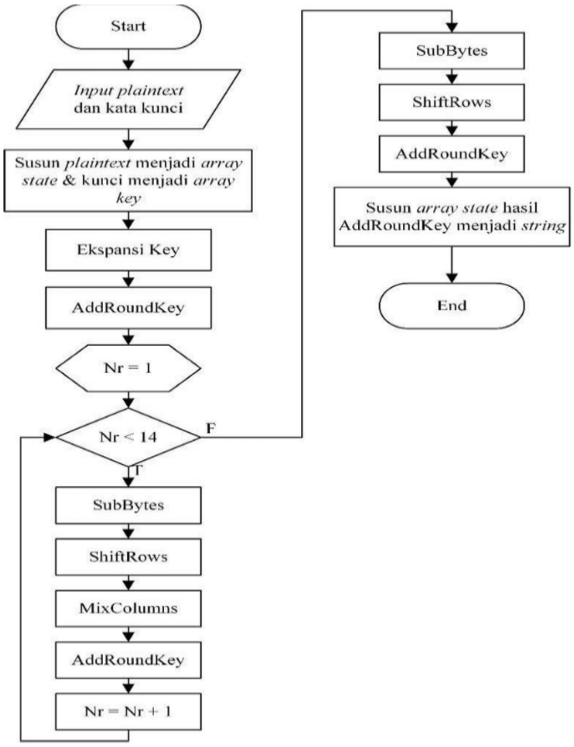

Start
Input plaintext dan kata kunci
Susun plaintext menjadi array state & kunci menjadi array key
Ekspansi Key
AddRoundKey
Nr = 1
Nr < 14
F
T
SubBytes
ShiftRows
MixColumns
AddRoundKey
Nr = Nr + 1
SubBytes
ShiftRows
AddRoundKey
Susun array state hasil AddRoundKey menjadi string
End

Figure 6. **Encryption Process Flowchart**

After the encryption process, a decryption process is carried out, the decryption process is implemented in the opposite direction of encryption to produce the inverse cipher. The byte transformations used in the inverse cipher are Inverse ShiftRows, Inverse SubBytes, Inverse MixColumns, and AddRoundKey. The sequence of the AES decryption process is not simply the reverse of encryption; rather, the order of operations is rearranged, even though the same key is used.

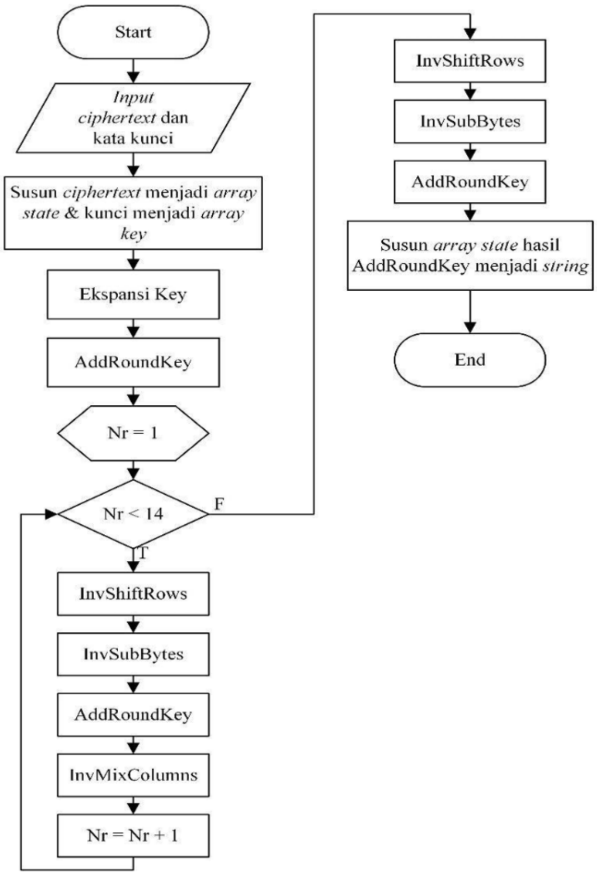

Start
Input ciphertext dan kata kunci
Susun *ciphertext* menjadi *array state* & kunci menjadi *array key*
Ekspansi Key
AddRoundKey
Nr = 1
Nr < 14
F
T
InvShiftRows
InvSubBytes
AddRoundKey
InvMixColumns
Nr = Nr + 1
InvShiftRows
InvSubBytes
AddRoundKey
Susun *array state* hasil AddRoundKey menjadi *string*
End

Figure 7. Decryption Process Flowchart

3. RESULTS AND DISCUSSION

The application of the AES cryptographic algorithm to data security aimed to improve the confidentiality of messages, specifically the child's full name, National Identification Number (NIK), username, and password. In this research, security was achieved using the AES-256 cryptographic algorithm, involving encryption and decryption processes.

3.1. Implementation of Algorithms

In this step, we demonstrated the application of the AES-256 encryption algorithm. Suppose the plaintext and key are chosen as follows:

Plaintext is "Negara Indonesia"

Key is "Indonesia cerdas pada tahun 2025"

The first step is to convert the plaintext and key to hexadecimal using the ASCII table, that results shown in Table 1 and Table 2.

Table 1. Conversion of Plaintext into Hexadecimal Numbers

N	e	g	a	r	a		I	n	d	o	n	e	s	i	a
4E	65	67	61	72	61	20	49	6E	64	6F	6E	65	73	69	61

Plaintext in hexadecimal is $4E$ 65 67 61 72 61 20 49 $6E$ 64 $6F$ $6E$ 65 73 69 65

Table 2. Conversion of Key into Hexadecimal Numbers

I	n	d	o	n	e	s	i	a		c	e	r	d	a	s
49	6E	64	6F	6E	65	73	69	61	20	63	65	72	64	61	73
	p	a	d	a		t	a	h	u	n		2	0	2	5
20	70	61	64	61	20	74	61	68	75	6E	20	32	30	32	35

Key in hexadecimal is 49 $6E$ 69 20 61 64 61 $6C$ 61 68 20 $6B$ 75 $6E$ 63 69

Before entering the Encryption-Decryption process, there is a key expansion process where operations are performed to obtain a Roundkey which is used in each round of the Encryption and Decryption process. In this process, a Round Constant (Rcon) is used. Rcon is an array of constants used during the key expansion process to help generate a round key from the primary key. The Rcon used in this research as shown in Table 3.

Table 3. Some RCON Values

Round Constant	=	Value
Rcon(1)	=	(01,0,0,0)
Rcon(2)	=	(02,0,0,0)
Rcon(3)	=	(04,0,0,0)
Rcon(4)	=	(08,0,0,0)
Rcon(5)	=	(10,0,0,0)
Rcon(6)	=	(20,0,0,0)
Rcon(7)	=	(40,0,0,0)
Rcon(8)	=	(80,0,0,0)
Rcon(9)	=	(1B,0,0,0)
Rcon(10)	=	(36,0,0,0)

Before starting encryption process, a key expansion process was performed, with at first search for Roundkey. Results of this calculation used for each round of the encryption process. After performed key expansion process, this research resulted 14 Roundkeys as follows :

Roundkey 0 : 496E646F6E657369612063657264617 3
Roundkey 1 : 207061646120746168756E2032303235
Roundkey 2 : 4C4DF24C222881254308E240316C8333
Roundkey 3 : E7208DA78600F9C6EE7597E6DC45A5D3
Roundkey 4 : 204B94CA026315EF416BF7AF7007749C
Roundkey 5 : B6E51F7930E5E6BFDE90715902D5D48A
Roundkey 6 : 2703EABD2560FF52640B08FD140C7C61
Roundkey 7 : 4C1B0F967CFEE929A26E9870A0BB4CFA
Roundkey 8 : C52AC75DE04A380F844130F2904D4C93
Roundkey 9 : 2CF8264A5006CF63F268571352D31BE9
Roundkey 10 : B385D95D53CFE152D78ED1A047C39D33
Roundkey 11 : 8CD67889DCD0B7EA2EB8E0F97C6BFB10
Roundkey 12 : EC8A134DBF45F21F68CB23BF2F08BE8C

Roundkey 13 : 99E6D6ED453661076B8E81FE17E57AEE
Roundkey 14 : 75503BBDCA15C9A2A2DEEA1D8DD65491

After found roundkey 1 to roundkey 14 and encryption steps were repeated for 14 rounds, it had resulted a ciphertext. With Matlab software, the ciphertext for this research was obtained as shown in **Table 4**.

Table 4. The results of encryption and conversion Hexadecimal to Base64

Plaintext	: Negara Indonesia
Key (32-byte)	: Indonesia cerdas pada tahun 2025
Ciphertext (Hex)	: 09C68083719E2C8D44D364282CACCB03F21914D20543F8512DDAB1AA8C0F9231
Ciphertext (Base64)	: CcaAg3GeLI1E02QoLKzLA/IZFNIFQ/hRLdqxqowPkjE=

3.2. Implementation on Website

In this research, the AES-256 cryptographic algorithm was implemented on website database to encrypt child's full name, National Identification Number (NIK) and password. On registration page, there were several important steps to ensure. After user entered the registration information, system performed several checks, such as ensured that the NIK was not already registered and confirmation that the password matches with user entered one.

1. NIK Check
   System first checked whether an entered NIK already existed in database. If an entered NIK was already registered, system displayed a message that NIK was already used. System checked NIK in database with followed code: **if($select_user->rowCount() > 0)**.
2. Username Check
   System first checked whether an entered username already existed in database. If an entered username was already registered, system displayed a message that username was already used. System checked username in database with same code as for NIK check: **if($select_user->rowCount() > 0)**.
3. Password Confirmation Check
   System also verified whether a password entered by the user matched with inputted password confirmation. In this part, system checked those inputs with followed code: **if($pass != $cpass)**.
4. Password Encryption
   Before saving password to the database, system encrypted an inputted password with followed code: **$encryptedPassword = encryptData($cpass, $key)**. This encryption stored a password in more secure form and made it invisible from its original form.
5. New User Storage
   After going through verification and encryption process, a new user's data (including encrypted password) was stored to database by system, with followed code: **$insert_user->execute(...)**.
6. Account Verification After Registration
   After successful registration, system verified a newly registered user with followed code: **$verify_user->execute(...)** and then automatically redirected them to main page if verification was successful.

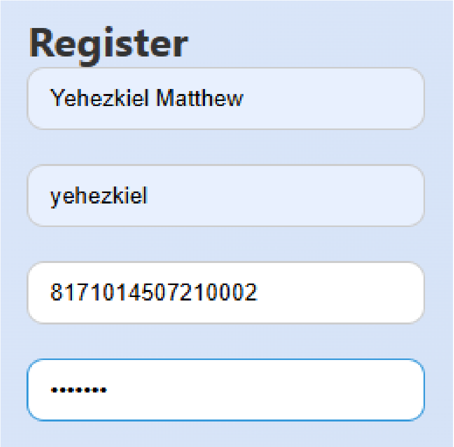
Next, on the login page, system performed a verification process to ensure that the logged-in user was a valid user. The key steps of this process as followed:

1. Database Check
   System checks whether an entered NIK existed in the database with followed code: **if($select_user->rowCount() > 0)**. If an entered NIK was not found, system displayed an error message.
2. Decrypt Encrypted Password in Database
   If user was found, system decrypted a password stored in database with function **decryptData()**.
3. Verify Input Password with Decrypted Password
   The user's entered password was compared with decrypted password with followed code: **if($decryptedPassword === $inputPass)**. If they were match, user was considered valid and redirected to the main page. If they didn’t match, an error message was displayed.

3.3. Program Trial

After its implementation on website, the program underwent testing to ensure its proper and smooth functioning. The testing process was divided into several stages: user registration, login, and checking user data stored in the database.

a. Registration Process
   On the main page of the website, users could select register menu to register and fill in their details, as shown in Figure 9. After registration of user data, system carried out a check and if an inputted NIK and username weren’t recorded in database, it would continue with checked similarity of password and confirmation of password, then encrypted a password and stored data in database.



Register

Yehezkiel Matthew

yehezkiel

8171014507210002

•••••••

Figure 9. Display of Completed Registration Page

b. Login Process
   After user registered an account on registration page and had access to website, user could perform login process by inputted the NIK and password data. After that, system checked user’s email in database and after it is confirmed that user’s email is in the database, the NIK and password in database will be decrypted before being matched with the NIK and password inputted by user. If decryption of the NIK and password in database was same as the NIK and password inputted by user, they count access their account and then automatically redirected to main page of the website.

c. Check in Database

While user has successfully registered, their data was automatically stored in database. This research aimed to ensure that personal data, such as full name, ID number, and password stored in database are encrypted. The research was considered successful if stored personal data was encrypted using the AES-256 algorithm and user could log in smoothly.

Table 5. Personal data

Full Name	Username	NIK	Password
Yehezkiel Matthew	Yehezkiel	8171014507210002	kiel123
Zephaniah Glory	Glory	8171010509210001	Glo32
John Phillip	John	8171012606200005	Jo578
Ester Rose	Ester	8171011109210010	Ester987

The personal data in **Table 5** was encrypted using the AES-256 cryptographic algorithm and the following data was obtained.

Table 6. Personal data in database after encryption

Fullname	Username	NIK	Password
oH3ryizbPVFdG9tAZYvNDxSHy2Zi88Dh9XW6/sH5/H8=	Yehezkiel	yA+Iskx9q0VgRdG4umR8ofIZFNIFQ/hRLdqxqowPkjE=	a6oj+AYP6Kc9hfC9xRqh7w==
lOrhVsdINoDQbp27zTwh3A==	Glory	wpV9RwGeDczy4nBRARAXg/IZFNIFQ/hRLdqxqowPkjE=	oKysj1mUeS+QRbFqKzc2Dg==
APrDEreGICDmMegCdmPtqw==	John	+DU14U0DOI4Ih1mMAR3QnvIZFNIFQ/hRLdqxqowPkjE=	vLX9LjvyE7fCIwJlr9ehJg==
crz7NjuVOg2ZVhI0NCtIPQ==	Ester	H4K88R5V3f7usbaaumRT8PIZFNIFQ/hRLdqxqowPkjE=	40Fd0QMr7A44G+TZn4MhnQ==

Based on **Table 6**, personal data had been encrypted into unintelligible random characters. This suggested that the security of databases containing personal data was significantly enhanced through implementation of cryptographic algorithms. By applied the AES-256 cryptographic algorithm, personal data of children, such as full names and NIK, are encrypted into complex characters and symbols, made it much difficult and required significant time and expertise to be hacked.

4. CONCLUSION

The conclusion of this study is that the implementation of the AES-256 cryptographic algorithm in protecting children's personal data successfully encrypts full names, NIK, usernames, and passwords used on websites, which are made into random characters that are not easily to understand. This research shows that the database that stores children's personal data becomes more secure when it has been applied to the AES-256 cryptographic algorithm. Furthermore, to improve the security of protecting children's personal data, the AES-256 cryptographic algorithm can be modified by changing the polynomial function in the finite field of Galoa and modifications to the mixcolumns. In addition, the AES-256 cryptographic algorithm can also be combined with other cryptographic algorithms such as RSA.

ACKNOWLEDGMENTS

We would like to express our appreciation to the anonymous reviewers for their valuable feedback that significantly enhanced the quality of our paper.

FUNDING INFORMATION

The authors declare no external funding. The authors themselves provided full support and funding for all activities related to this research.

AUTHOR CONTRIBUTIONS STATEMENT

First Author: Conceptualization, methodology, writing-original draft, data curation, validation. Second Author: methodology, software. Third Author: Formal analysis, draft preparation . Fourth Author: writing-review & editing, validation. All authors discussed the results and contributed to the final manuscript.

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

INFORMED CONSENT

This study does not involve any individual participant data, and no informed consent was required.

ETHICAL APPROVAL

There were no ethical issues with this research because it didn't involve experimentation on people or animals.

DATA AVAILABILITY

This study is based on hypothetical data used for simulation purposes only. No real-world data were used or analysed.

REFERENCES

[1] E. S. Marsiani *et al.*, "Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi," *Jurnal Rekayasa Komputasi Terapan*, vol. 1, no. 02, 2021, doi : 10.30998/jrkt.v1i02.4096.

[2] A. Di *et al.*, "Urgensi Perlindungan Data Pribadi Pada Sistem Elektronik Untuk Anak Di Bawah Umur Di Indonesia Serta Perbandingan Regulasi Dengan Uni Eropa (General Data Protection Regulation)," *Jurnal Esensi Hukum*, vol. 6, no. 2, pp. 105-124, 2024, doi : 10.35586/jsh.v6i2.412.

[3] W. Pratiwi, T. Diva Fortuna Hadi, A. Herian, K. Agustya Zahra Salsabilla, D. Satria Yudha Kartika, and U., "Sosialisasi Keamanan Data di Era Digital pada Anak-Anak Panti Asuhan Ulul Azmi Surabaya," *Jurnal Pengabdian Sosial*, vol. 1, no. 8, pp. 761-766, 2024, doi : 10.59837/749zpv32.

[4] G. Ayu Putu Vebyardani, "Perlindungan Data Anak, Regulasi, dan Solusi untuk Keamanan Media Digital Tiktok," *Jurnal Hukum, Administrasi Publik dan Negara*, vol. 2, no. 3, pp. 120–128, 2025, doi: 10.62383/hukum.v2i3.272.

[5] S. Oktavani *et al.*, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *Jurnal Media Informatika*, vol. 4, no. 2, pp. 97-101, 2023, doi : 10.55338/jumin.v4i2.435.

[6] F. Tita, A. Setiawan, and B. Susanto, "Construction Of Substitution Box (S-Box) Based On Irreducible Polynomials On Gf(28)," *Barekeng*, vol. 18, no. 1, pp. 0517–0528, Mar. 2024, doi: 10.30598/barekengvol18iss1pp0517-0528.

[7] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, no. 1, 2016, [Online]. Available: http://ejournal.unisba.ac.id

[8] E. M. De Los Reyes, A. M. Sison, and R. P. Medina, "Modified AES cipher round and key schedule," *Indonesian Journal of Electrical Engineering and Informatics*, vol. 7, no. 1, pp. 28–35, Mar. 2019, doi: 10.11591/ijeei.v7i1.652.

[9] C. Irawan and E. H. Rachmawanto, "Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA," *Seminar Nasional Multi Disiplin Ilmu*, Juli, 2021, pp. 567-573. Retrieved from https://www.unisbank.ac.id/ojs/index.php/sendi_u/article/view/8651

[10] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "Modified advanced encryption standard algorithm for information security," *Symmetry (Basel)*, vol. 11, no. 12, Dec. 2019, doi: 10.3390/SYM11121484.

[11] Saripa, "Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk," *Progressive Information, Security, Computer, and Embedded System,* vol. 2, no. 1, pp. 35-45, 2024, doi : 10.61255/pisces.v1i2.100.

[12] D. Putri Harum and S. Arifianto, "Improvisasi Algoritma Advanced Encryption Standard (AES) Dengan Melakukan Pemetaan S-Box Pada Modifikasi Mixcolumns," *Jurnal Repositor,* vol. 1, no. 2, pp. 95–104, 2019, doi : 10.22219/repositor.v1i2.30391.

[13] I. Kurnia Nurhareza and S. Siswanto, "Penerapan Algoritma Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi* (SENAFTI), vol. 1, no. 1, pp. 302-309, 2022, https://senafti.budiluhur.ac.id/senafti/article/view/269.

[14] F. Syafaat and A. Finandhita, "Implementasi Kriptografi AES-128 Pada Unmanned Aerial Vechile Dan Ground Control System," Bachelor thesis, Teknik Informatika, Universitas Komputer Indonesia, 2019.

[15] Y. Wiharto and Mufti, "Implementasi Advanced Encryption Standard 128 Sebagai Pengamanan Basis Data Obat-obatan Apotek," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 2, Aug. 2022, doi: 10.28932/jutisi.v8i2.4817.

[16] Warkim, Irvan Lewelusa, "Implementasi Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) Dengan Metode CBC (Chiper Block Chaining) Dan Pengecekan Error Detection Cyclic Redundancy Check,"*JurnalIlmu Komputer,* vol. 11, no. 2, September 2015, DOI: https://doi.org/10.47007/komp.v11i2.2233.