Modification of Advance Encryption Standard(AES) and Rivest–Shamir–Adleman(RSA) Algorithms for Data Authentication on Study Results Card

Karina Andriani[1], Roslina[2] and B. Herawan Hayadi[1]
[1] *Computer Science, Main Potential University, Medan, Indonesia*
[2] *Department of Computer Engineering, Politeknik Negeri Medan, Medan, Indonesia*

Keywords: AES and RSA Algorithms, Data Authentication.

Abstract: Authentication is a process carried out to validate the authenticity of data and the owner of the data. The method used to form an authentication system is cryptography. One of the cryptographic algorithms that are often used is the Advance Encryption Standard (AES) because it has been tested for its resistance to all kinds of attacks on data. Not only is it able to encrypt or encode data, but the AES algorithm is also able to decrypt or restore encrypted data so that the data can be read or understood again. Besides that, the RSA algorithm is a cryptographic algorithm that is often used for authentication. The RSA algorithm has a private key concept where the encryption and decryption keys are different so that it is stronger to serve as a data security algorithm. Therefore, modifications to the AES and RSA algorithms were made to produce a better authentication system. In this study, modifications were made to the AES and RSA algorithms for data security authentication on the study results card.

1 INTRODUCTION

In the digital era, it is convenient to falsify data and the identity of the data owner. Counterfeiting is carried out for various interests that benefit the perpetrator. Therefore, security is the solution to the threat of data forgery and the identity of the data owner by using modern security techniques such as cryptography. One of the data security techniques in the form of data authenticity validity is a digital signature. Digital Signature can be applied in verifying the authenticity of data and authenticating the authenticity of the owner of the data. Digital Signature is a cryptographic value that depends on the message and the sender. The way a Digital Signature works is almost the same as how a regular document ”signature” works (Amik and Cipta, 2021).

There are two algorithms in the Digital Signature system, namely the signing algorithm to sign a document M and generate a signature (sign) ρ, and the verify algorithm that returns true if the signature ρ belongs to the signer and for document M (Waruwu et al., 2020).

RSA is a cryptographic algorithm that is often used for making Digital Signatures because this algorithm produces two keys that are mathematically connected. Where the public key is used for the encryption process while the private key is used for the decryption process(Ahmed, 2022).RSA is a popular public-key cryptographic algorithm. This algorithm was found by three researchers from MIT (Massachusetts Institute of Technology) in 1976: Rivest, Shamir, and Adleman. The RSA algorithm uses a public key and a private key, where the public key can be known by many people to encrypt messages, while the private key can only be known by certain parties to decrypt messages. The security of this algorithm lies in the difficulty of factoring large integers into prime factors. This factoring decrease to obtain the private key. RSA's operating mechanism is convenient to understand and simple, but powerful (Pariddudin and Syawaludin, 2021).

AES Method The Advanced Encryption Standard (AES) method is an encryption method that uses a symmetric key with a key length of 128, 192, and 256 bits to encrypt and decrypt data in 128-bit blocks. The AES method that uses a block cipher system can perform symmetric key encryption operations with operating modes. In addition, AES has advantages in security, speed, and characteristics of the algorithm and

Andriani, K., Roslina, . and Hayadi, B.
Modification of Advance Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) Algorithms for Data Authentication on Study Results Card.
DOI: 10.5220/0012447000003848

In *Proceedings of the 3rd International Conference on Advanced Information Scientific Development (ICAISD 2023)*, pages 211-217
ISBN: 978-989-758-678-1

its implementation (Allan, 2020).

With the collaboration of the Hybrid Cryptosystem, the RSA-AES algorithm can increase the effectiveness and capabilities of the algorithm in securing data, especially in producing Digital Signatures which function to maintain the authenticity of Study Result Card data.

2 METHOD

2.1 Stage of Research

At this stage of the study, which starts from the analysis of problem how to modified AES and RSA to secure the data of study result card, then conducted literature studies to modify the two algorithms, namely as follows:

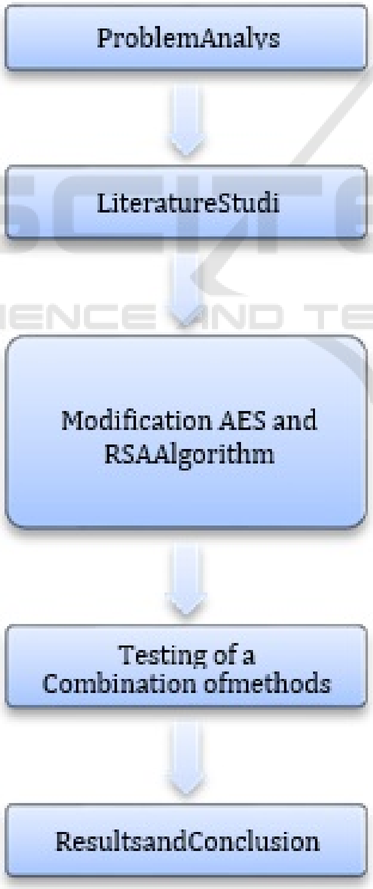

ProblemAnalys
LiteratureStudi
Modification AES and RSAAlgorithm
Testing of a Combination ofmethods
ResultsandConclusion

Figure 1: Stages of research.

From these results, it can be seen what the conclusions of the combination of these 2 algorithms are in authenticating the authenticity of the data on the study results card and the security of ownership of the data. From the results of this combination, this algorithm modification can be used in other data security to obtain a better level of security.

2.2 AES (Advanced Encryption Standard) Algorithm

AES uses 5 units of data size: bits, bytes, words, blocks, and states. The bit is the smallest unit of data, namely the value of the binary system digits. While bytes are 8 bits, words are 4 bytes (32 bits), blocks are 16 bytes (128 bits) and the state is a block that is arranged as a 4x4 byte matrix. The following image describes the AES data unit(Siringoringo, 2020). The following is the arrangement of the AES algorithm steps(Azanuddin, 2022):

1. Transform plaintext and key into hexadecimal numbers
2. Arrange the plaintext and key into a 4x4 state arrays
3. Performs an expansion on the selected key
4. Do AES encryption transformation process with SubBytes, ShiftRows, MixColumns, and AddRoundKey
5. To return the ciphertext to the original message, decrypt it using the InvSubBytes, InvShiftRows, InvMixColumns, and InvAddRoundKey processes.

The following is an overview of the encryption and decryption process with the AES algorithm (Sodikin and Hidayat, 2020):

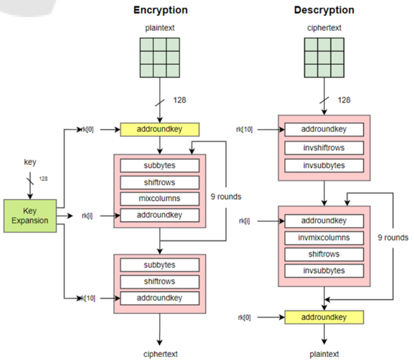


Figure 2: Encryption and decryption of AES.

SubByte doing by substituting each byte in the Array state, the example, $S[i,j] = xy$ is a hexadecimal digit and the value is $S[i,j]$, then the substitution value expressed by $S[i,j]$ is an element in the S-box that is the intersection of the x line with the y column (Azhari et al., 2022).

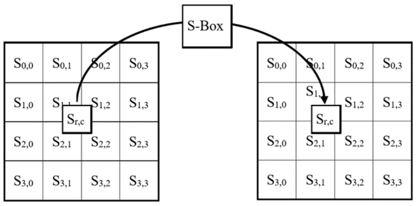

S-Box
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S_{r,c}$
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S_{r,c}$

Figure 3: SubByte transformation.

ShiftRow is a process in which each row of the status matrix is given a cyclic shift to the right according to its position (M et al., 2022).

MixColumn in the AES algorithm process by performing polynomial multiplication between the last state and the following matrix (Haris and Lydia, 2023):

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

AddRoundkey is performed by performing an XOR operation on each value of the input block with the value of the key block in the same position (Haris and Lydia, 2023).

2.3 RSA (Rivest Shamir Addleman) Algorithm

Rivest Shamir Adleman's algorithm is a method that has different keys (encryption and decryption keys). The RSA method is known as a cryptographic method that uses the concept of public key cryptography (Gea et al., 2021). The following is a schematic of the RSA algorithm (Kota and Aissi, 2022):

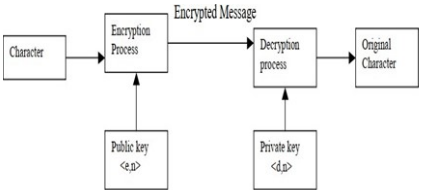


Figure 4: RSA Algorithm Schematic.

Following are the steps of the RSA algorithm:

1. Generate a public key (e) and a private key (d) by choosing two very large primenumbers, the two number = p and q
2. Multiply p and q, n = p * q .
3. Generate a public key, which is relatively prime to the ”totient” function $\varphi(n) = (p-1)(q-1)$
4. Generate a private key, which is the multiplicative inverse of emod $\varphi(n)$. Note that the public key is $< e, n >$ and private key is $< d, n >$
5. Encrypt a message with following formula:

$$c = memodn \tag{1}$$

$$m = cdmodn \tag{2}$$

6. Decrypt the cipher textwith following formula:

2.4 Authentication With Digital Signature

The Digital Signature functions as a tool for the authenticity of electronic information and verification of the identification of the signer. Information and communication technology has certainly changed the pattern of people's behavior and also human civilization globally. In addition, the world has become borderless because developments in the field of information technology have resulted in and also caused significant social changes to take place rapidly (Qisthina and Neyman, 2021).

The scheme of the Digital Signature for the study result card authentication is as follows:

1. Stages on digital signature

   a. The data on the study results card is taken, for example Name (secret)
   b. Define a key, for example NIRM (secret)
   c. The data is encrypted with the AES algorithm
   d. The result of encryption (Cipherteks-AES) is then encrypted again with RSA using the private-RSA key. At this stage, an RSA private key must be generated with the selected data and an RSA Public key that is interrelated with the private key
   e. The result of encryption with RSA (this is the Digital signature)

2. Verification stage

   a. Digital Signature taken
   b. Then decrypt it using the RSA's Public key
   c. The result of this description is code
   d. Code Decryption with AES: The results are in the form of a name and Nirm
   e. If Name and nirm = value on KHS then the data is valid

3 RESULTS AND DISCUSSION

3.1 Message Encryption Process With The AES Algorithm

In the AES algorithm, a file will first be divided into 1 block of 128 bits to be processed first with a key length of 128 bits, 129 bits, or 256 bits, so that the sizes of plaintext and ciphertext will be different because, during the encryption process, the division of blocks is less of 128 bits will be padded to meet the standard block size of the AES algorithm.

The sequence of bits is numbered sequentially from 0 to n-1 where n is the sequence number. The data sequence of 8 bits sequentially is referred to as a byte where this byte is the basic unit of operations to be performed on a block of data. The number of n-bits that exist depends on the key length = 128 bits, $0 \leq n < 16$; key length = 192 bits, $0 \leq n < 24$; key length = 256 bits, $0 \leq n < 32$.

Each process in this algorithm will transform 10 rounds. Each round uses a different round key which is obtained during the key expansion process. This is intended to increase security so that this algorithm is not easy to solve by cryptanalysts.

3.1.1 Key Expansion

In the process of encryption and description of the AES algorithm, it is necessary to have 10 roundkey keys for each round.In this case, key is taken from the study results card, namely NIRM, then change the key to hexadecimal form and arrange it into a 4 x 4 state array as follows:

02	00	02	00
00	02	00	02
04	06	00	01
02	03	04	05

After the keys are arranged as above, the key expansion process will be carried out to get the roundkey state. Here is the process to get round 1 key:

a. Take the fourth column from RoundKey 0

b. The RotWord function is performed by moving the top bit to the bottom bit.

c. SubBytes transformation is performed with s-boxes

d. XOR with column 1 Roundkey 0

e. XOR with constant Rcon

In contrast to searching for results in column 1, searching for results in columns 2, 3, and 4 only requires an XOR process from the results of the previous column with the column values being searched. And so on to produce Roundkey 1 as follows:

74	74	76	76
7C	7E	7E	7C
6F	69	69	68
61	62	66	63

To get the next RoundKey result, repeat the same process as above. Because in this case using 128-bit AES with a key length of 128 bits, 10 RoundKeys are needed. The following are the search results for all of the RoundKeys 1 to 10:

- RoundKeys 1

74	74	76	76
7C	7E	7E	7C
6F	69	69	68
61	62	66	63

- RoundKeys 2

66	12	64	12
39	47	39	45
94	FD	94	FC
59	5B	5D	3E

- RoundKeys 3

0C	1E	7A	68
89	CE	F7	B2
26	DB	4F	B3
90	AB	F6	C8

- RoundKeys 4

33	2D	57	3F
E4	2A	DD	6F
CE	15	5A	E9
D5	7E	88	40

- RoundKeys 10

48	53	19	86
72	C4	76	98
D5	12	43	E2
EA	71	7B	6E

3.1.2 Encryption

In the encryption process, the plaintext and key are taken. In this case, the plaintext is taken in the form of the name on the study result card and NIRM or Roundkey 0.

Name : Khoril Khomis (Change to hexadecimal 4x4 state array):

48	68	6F	69
72	69	6C	4B
68	6F	6D	69
73	01	02	03

NIRM : 2020020246 (Change to hexadecimal 4x4 state array):

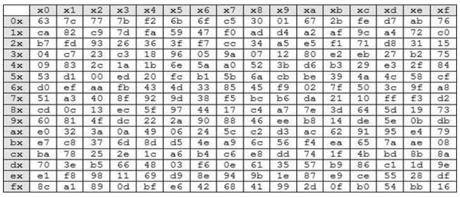
02	00	02	00
00	02	00	02
04	06	00	01
02	03	04	05

After getting the state of the plaintext and key, the AddroundKey transformation process is carried out by XOR it to get the State Initial Round. The following is the result of the XOR process between plaintext and RoundKey 0 :

49	68	6D	69
72	6B	6C	49
6C	69	6D	68
71	2	6	6

a. SubBytes Transformation

SubBytes are done by transforming the two numbers of hexadecimal digits with the S-box table :



	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 5: S-Box.

The following is the result of the initial round state transformation with the S-box :

3B	45	3C	F9
40	7F	50	3B
50	F9	3C	45
A3	77	6F	6F

Then the results of SubBytes will then be processed with shiftRow

b. ShiftRow

ShiftRow is a process in which each row of the status matrix is given a cyclic shift to the right according to its position. The following is the process for getting the results of the ShiftrRow transformation.

The result of ShiftRow below will taken to next step MixColumns:

3B	45	3C	F9
7F	50	3B	40
3C	45	50	F9
6F	A3	77	6F

c. MixColumns Process

MixColumns is done by multiplying polynomials between Shift Row's resulting states and predetermined polynomial matrix :

1. $\{3B\}x\{02\} = \{X^5+X^4+X^3+X+1\}.\{X\}$
   $= \{X^6+X^5+X^4+X^2+X\}$
   $= 01110110$
   $= 76$
2. $\{7F\}x\{03\}$
   $= \{x^6+x^5+x^4+x^3+x^2+x+1\}.\{x+1\}$
   $= \{x^7+1\}$
   $= 10000001$
   $= 81$
3. $\{3C\}x1 = 3C$
4. $\{6F\}x1 = 6F$

R1.0=76 XOR 81XOR3CXOR6F = A4
Do the next multiplication to get the MixColumn result as follows:

A4	9C	12	BF
EE	89	CD	6
8D	63	3E	E1
D0	87	D5	77

This state result to be continue for next step, AdRoundkey

d. AddRoundkey After getting the state from the MixColumns transformation, the next step is to carry out the AddroundKey transformation process. AddRoundKey is done using an XOR operation between the resulting state of Mixcolumn and Roundkey 1. This is the result of AddRoundkey :

After getting the value from the AddRoundkey state, the SubBytes – ShiftRows – MixCollumns process is carried out 9 times again bypassing the

D0	E8	64	C9
92	F7	B3	7A
E2	A	57	89
B1	E5	B3	14

state value from the AddroundKey which was obtained from the process above. But in the 10th round, the MixCollumns process is not used, just do the SubBytes – ShiftRows – AddroundKey process. The following is the result of the ciphertext from the encryption process which is also the result of the 10th round Addroundkey process.

EB	DD	9A	BC
9B	86	EC	27
E4	C5	F9	B0
B0	82	AE	3D

The results of the message encryption with AES will be modified with the RSA encryption algorithm at a later stage.

3.2 Modification AES With RSA Algorithm

At this stage, the results of encryption with the previous AES algorithm will be encrypted with the RSA algorithm. To do this, the Ciphertext resulting from AES encryption must be converted to a decimal number first.

Encrypted messages with AES: AEBC193A19C7F7FCF8442777866FE97C
Message is converted to decimal: 174188255825199247252248683911913411123312 4
Then, the message is processed with the RSA algorithm. The following is the encryption process with the RSA algorithm:

3.2.1 RSA Key Generator

- Take two prime numbers for the values of p and q
  P = 137
  Q = 131

- Calculate modulus value (n)
  n = p x q
  n = 137 × 131
  n = 17947

- Calculate modulus value (m)
  m = (p - 1) × (q - 1)
  m = (137 - 1) × (131 - 1)
  m = 136 × 130
  m = 17680

- Choosing e which is relatively prime to m with the condition that it meets the Greater Common Divisor (GCD) means that the greatest dividing factor for the values of e and m is one. To determine this value, the Euclidean algorithm is used as follows:
- gcd(e,m)=1

  Euclidean Algorithm Formula
  $r_0 = q_1 r_1 + r_2, 0 < r_2 < r_1$
  $r_1 = q_2 r_2 + r_3, 0 < r_3 < r_2$
  $r_n = ...$

  gcd(e, 17680) = 1
- $r_0 = 3, r_1 = 17680$

  $r_0 = q_1 r_1 + r_2$
  3 = 0.17680 + 3
  $r_1 = 17680, r_2 = 3$
  $r_1 = q_2 r_2 + r_3$
  17680 = 5893.3 + 1
  $r_2 = 3, r_3 = 1$
  $r_2 = q_3 r_3 + r_4$
  3 = 3.1 + 0

- then the value of e is 3, e = 3
- Determining the value of d : e×d mod m=1
  3×11787 mod 17680=1
  d = 11787

- Public Key
  $K_{public} = (e, n)$
  $K_{public} = (3, 17947)$

- Private Key
  $K_{private} = (e, d)$
  $K_{private} = (3, 11787)$

3.2.2 RSA Encryption

To encrypt messages with the RSA Algorithm, the first 3 digits of the message above are taken, namely 174. Then, the plaintext is encrypted with the following formula:

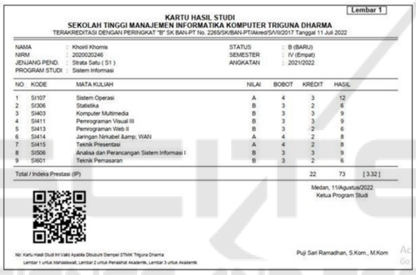
$C = m^e \ modn$
$C = 1743^3 mod 17947$
$C = 9553$

3.2.3 RSA Decryption

Here is the result of the decryption of the message above:
$M = C^d mod n$
$M = 9553^{11787} mod 17947$
$M = 174$

3.3 Authentication Message on Study Result Card

The message that is used as a digital signature in the form of a QR-Code is the name and registration number (NIRM) which is encrypted with the AES algorithm, then the results of the encryption are encrypted again with the AES algorithm using a public keys. The message is placed on the study results card. For authentication, the public key RSA algorithm is used which generates the AES message again, then decrypts it again to get the original message.



Lembar 1

KARTU HASIL STUDI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA KOMPUTER TRIGUNA DHARMA
TERAKREDITASI DENGAN PERINGKAT "B" SK BAN-PT No. 2265/SK/BAN-PT/Akred/S/VII/2017 Tanggal 11 Juli 2022

NAMA	: Khoiril Khomis	STATUS	: B (BARU)
NIRM	: 2020020246	SEMESTER	: IV (Empat)
JENJANG PEND.	: Strata Satu (S1)	ANGKATAN	: 2021/2022
PROGRAM STUDI	: Sistem Informasi		

NO	KODE	MATA KULIAH	NILAI	BOBOT	KREDIT	HASIL	
1	SI107	Sistem Operasi	A	4	3	12	
2	SI306	Statistika	B	3	2	6	
3	SI403	Komputer Multimedia	B	3	3	9	
4	SI411	Pemrograman Visual III	B	3	3	9	
5	SI413	Pemrograman Web II	B	3	2	6	
6	SI414	Jaringan Nirkabel &amp; WAN	A	4	2	8	
7	SI415	Teknik Presentasi	A	4	2	8	
8	SI506	Analisa dan Perancangan Sistem Informasi I	B	3	3	9	
9	SI601	Teknik Pemasaran	B	3	2	6	
Total / Indeks Prestasi (IP)					22	73	[3.32]

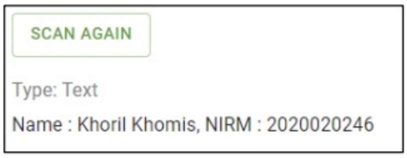
Medan, 11/Agustus/2022
Ketua Program Studi

Puji Sari Ramadhan, S.Kom., M.Kom

Nb: Kartu Hasil Studi Ini Valid Apabila Dibubuhi Stempel STMIK Triguna Dharma
Lembar 1 untuk Mahasiswa, Lembar 2 untuk Penasihat Akademik, Lembar 3 untuk Akademik

Figure 6: QR-Code On Study Result Card.

The following is a message that has been authenticated by scanning the QR-Code that is already on the study result card.



Type: Text

Name : Khoril Khomis, NIRM : 2020020246

Figure 7: Date Verification Of Study Result Card.

4 CONCLUSIONS

Modification of the AES and RSA algorithms makes it possible to authenticate data on study results cards. This modification is made to protect the data owned by the card owner so that it cannot be modified. For data authentication, decryption using RSA is a bit complicated because of the large number of messages resulting from AES encryption, which slows down the decryption computation due to the large exponential value. However, the security of this algorithm is very strong because the message value cannot be predicted easily.

REFERENCES

Ahmed, M. (2022). Digital signature with rsa public key cryptography for data integrity in sose-based e-government systems. *Int. J. Manag. Technol. Soc. Sci*, 7(1):59–70,.

Allan, J. (2020). Keamanan file digital.

Amik, M. and Cipta, D. (2021). Penerapan qr code untuk media pelayanan absensi.

Azanuddin (2022). Implementasi keamanan citra menggunakan.

Azhari, M., Mulyana, D., Perwitosari, F., and Ali, F. (2022). Implementasi pengamanan data pada dokumen menggunakan algoritma kriptografi advanced encryption standard (aes. *J. Pendidik. Sains dan Komput*, 2(01):163–171,.

Gea, F., Nasution, Z., and Hartama, D. (2021). Bees : Bulletin of electrical and electronics engineering implementasi algoritma rsa untuk keamanan data kredit di pt bank perkreditan rakyat solider pematangsiantar.

Haris, M. and Lydia, M. (2023). Pengamanan pada citra digital dengan menggunakan modifikasi blok data algoritma aes - rijndael.

Kota, C. and Aissi, C. (2022). Implementation of the rsa algorithm and its cryptanalysis.

M, G., Hadiana, A., and Sabrina, P. (2022). Kriptografi untuk enkripsi ganda pada gambar menggunakan algoritma aes (advanced encryption standard) dan rc5 (rivest code 5. *Informatics Digit Expert*, 4(1):25–32,.

Pariddudin, A. and Syawaludin, M. (2021). Penerapan algoritma rivest shamir adleman untuk meningkatkan keamanan virtual private network.

Qisthina, S. and Neyman, S. (2021). Pengamanan internet of things untuk tanda tangan digital menggunakan algoritme elgamal signature scheme security of the internet of things (iot) for digital signature using the.

Siringoringo, R. (2020). Analisis dan implementasi algoritma rijndael (aes) dan kriptografi rsa pada pengamanan file.

Sodikin, L. and Hidayat, T. (2020). Analisa keamanan e-commerce menggunakan metode aes algoritma. *Teknokom*, 3(2):8–13,.

Waruwu, T., Kurniasih, N., and Turban, M. (2020). Sistem pendukung keputusan pemilihan pemenang lomba balita sehat dengan menerapkan metode weighted aggerated sum product assessment (waspas) pada posyandu desa karang anyar.