International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

Super Encryption of the Hill Cipher Method and the AES Method for Security of Employee Salary Data

Ervina Br Sitepu [1] , Achmad Fauzi [2] , Rahmadani [3]

[1,2] Information System, STMIK Kaputama, Binjai Indonesia
[3] Computer Systems, Faculty of Science and Technology,
Development Panca Budi University, Medan, Indonesia

E-mail address:
ervinabrstp85@gmail.com (Ervina Br Sitepu), fauzie.kaputama@gmail.com (Achmad Fauzi), rahm4dani@gmail.com (Rahmadani)

*Corresponding author: ervinabrstp85@gmail.com

Received: July 10, 2023; **Accepted** : December 17,2023 ; **Published** : January 23, 2024

Abstract: Data security is a security system that is needed to protect data in systems, networks and other digital components. In a unit or agency such as the South Binjai sub-district office, the management of employee salary data is done digitally, namely via a computer. However, in this increasingly sophisticated digital era, it can cause many irresponsible individuals to easily wiretapping the company's data so that it can be easily accessed by other parties, as well as employee salary data which contains a lot of data. important. In order to avoid unwanted things such as theft of personal data by irresponsible persons, a security system is needed that can maintain the confidentiality of data and secure data. Therefore, in this case, a security system is needed that can maintain the confidentiality of data and secure employee salary data. With that there are many algorithms that can be used in securing employee salary data. And the algorithm used is hill cipher and AES algorithm. The hill cipher algorithm is an encryption-decryption algorithm that uses a transformation matrix. The AES algorithm is a symmetric block ciphertext that can encrypt and decrypt information. The use of these two algorithms can further strengthen the security of employee salary data. From the results of the trials carried out, the sample data used containing employee salary data was successfully secured with both hill cipher and AES algorithms.

Keywords : AES Algorithm, Data, Hill Cipher, Cryptography.

1. Introduction

Data security (data security) is the process carried out to protect data from unauthorized access, misuse, or unwanted changes. In simple terms, data security is a security system that is needed to protect data in systems, networks and other digital components. The South Binjai Sub-District Office is a unit or agency consisting of a place for employees/employees and operations

DOI: 10.52362/ijiems.v3i1.1219

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

for managing paperwork (finances and so on) led by the Head of the sub-district in the field of government to assist the City of Binjai in administering government, public services and community empowerment in the sub-district. The South Binjai sub-district office has an organizational structure consisting of sub-district heads, secretaries, government sections, general sub-divisions, finance sub-divisions, etc. Where each of these structures has its own roles and duties.

Almost all jobs in the sub-district office use computers, especially in managing employee salary data. However, in today's increasingly sophisticated digital era, there are many irresponsible individuals who find it easy for them to wiretapping the company's data so that it can be easily accessed by other parties. This can cause losses for the unit/agency itself. At the South Binjai Sub-District Office, the salaries received by employees each month are in accordance with the UMR that has been set. Salary data managed at the sub-district office is only salary data for daily freelance workers (TLH) or what is also known as honorarium. Employee salary data at the South Binjai Sub-District Office are inputted and made into a file containing several employee identities such as account numbers and nominal salary amounts. Where later the file or document will be sent to the Bank, and it is the Bank that will process the payroll of the employees at the South Binjai Sub-District Office according to the existing data. However, here the employee salary data document has not undergone an encryption process or is still in plaintext form. This of course will make it easier for unauthorized parties to manipulate the employee salary data if the data is still in plaintext form.

The employee salary data not only contains the nominal amount of salary that needs to be secured, but also contains employee personal data which is also confidential, such as account numbers, employment serial numbers (NUP), employee intensive types and other identities that also need to be hidden. To prevent undesirable things from happening, such as theft of personal data by irresponsible persons. Therefore, in this case, a security system is needed that can maintain the confidentiality of data and secure employee salary data. With that there are many algorithms that can be used in securing employee salary data. And the algorithm used is the Hill Cipher algorithm and the AES (Advanced Encryption Standard) Algorithm, each of which has weaknesses and strengths, including the weakness in the Hill Cipher algorithm is that if the attacker is able to get the original message and password that uses the same key then the attacker will automatically get the original message. Therefore, to strengthen and cover the weaknesses of the Hill Cipher algorithm, the AES (Advanced Encryption Standard) algorithm will be added here. Thus, by combining the two super encryption algorithms, it can be further strengthened so that security is even more guaranteed.

To strengthen the background of the problem, the author includes journals related to cryptography In this research it was conducted at Bank Sampoerna which is in the city of Padang Sidempuan. Encryption and decryption processes performed on the Bank's database were successfully carried out. The original database (plaintext) can be encrypted into an encoded database (ciphertext) and can be decrypted into the original database again. The Hill Cipher algorithm method using the ASCII code has been implemented in inputting bank customer financial data using a range of data according to bank regulations (Hasibuan et al., 2022). The next research adaptation is (Nabila Qomariah, Azanuddin, Vina Winda Sari, 2018, STMIK

DOI: 10.52362/ijiems.v3i1.1219

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

Triguna Dharma). In the research that has been done in designing and evaluating the implementation of salary data cryptography at the Siti Rahma Primary Clinic, using the AES method was successfully implemented. AES implementation is done with binary or hexsa, encrypted data cannot be read before the data is decrypted or converted into plaintext so that the data can be read again (Suci et al., 2018). As for further research (Muhammad Fadlan, Haryansyah, Rosmin, 2021, STMIK PPKIA). Based on the results of the research that has been done, this study shows that the proposed super encryption model through a combination of autokey cipher algorithms and column transposition is able to provide a better level of security. The proposed model also shows a very good level of accuracy in terms of the results of the encrypted data decryption process which are the same as the initial data. Of the 5 trial data that have been carried out, it has an accuracy rate of 100%. This shows that the entire trial data after going through the decryption process proposed in this study is able to return to the initial data form before being encrypted (Muhammad Fadlan et al., 2021)

2. Literature

There are several previous studies which are used as references in enriching the study material of this research. One of the studies using the AES algorithm was conducted (Dian Widyawan, Imelda, 2021) in his research it can be concluded that the application of cryptography with the AES method can secure important documents in the National Transportation Safety Committee, the AES-128 bit algorithm is successful applied. To secure files, encryption is carried out so that only people who have the key can decrypt the files (Di et al., 2021).

Subsequent research, namely research (Alfina Rachmayanti and Wirawan, 2022) in her research shows that the AES encryption method can provide maximum results so that the AES method can be applied to Smart health care to protect patient data sent using the IoT network.

The next research, namely research (Fadlullah Fadlullah et al, 2023) in his research it can be concluded that testing the encryption and decryption process using the AES algorithm can be applied to encrypt passwords, so that passwords cannot be easily read by other users. In addition, the password is also not easy to crack.

Subsequent research, namely research using the Hill Cipher algorithm, which was carried out (Ocha Gusti Awang Aritonang et al, 2019) from his research it can be concluded that the Hill Cipher method can be used to secure cashier employee salary data so that privacy regarding data about employee salaries at PT. Matahari Department Store Plaza Medan Fair is safe so data does not fall into irresponsible parties. This cryptographic design has a good level of security because it has two security keys, namely the public key and the private key.

The next research, namely research (Patmawati Hasan et al, 2020) in her research, it can be concluded that the results of the accuracy level that was tested five times on different plaintexts obtained an accuracy rate of 100%, that is, no differences were found in the results of encryption or decryption.

And further research, namely research (Yusna Warni Hasibuan et al, 2022) from this study it can be concluded that the encryption and decryption processes carried out on the original database (plaintext) can be encrypted into an encoded database (ciphertext) and can be decrypted

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

into the original database again. From the results of encryption calculations using the Hill Cipher method which has been combined with the ASCII Code, it produces resilience in securing data security that is safe to use.

3. Methods

3.1. Problem Analysis

The problem that will be solved by using this system is the security of employee salary data in the .doc format which you want to keep confidential. In this payroll system, text data in files will be secured using the Hill Cipher and AES algorithms, where text files will be secured by Hill Cipher and AES symmetric keys which will be combined. This key will initially be encrypted using the Hill Cipher algorithm and then encrypted again using the AES algorithm. Then the key that will be generated later will use two security keys, namely the hill cipher algorithm and AES.

3.2. Calculation Analysis of Hill Chiper Super Encryption and AES

1. **Hill Cipher encryption process.**

Plaintext (Hill Cipher): NILAMARLENANANST

Key (Hill Cipher): $\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}$

$$\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}\times\begin{bmatrix}78\\73\end{bmatrix}=\begin{bmatrix}10283\\11101\end{bmatrix}(mod\ 256)=\begin{bmatrix}43\\93\end{bmatrix}$$

$$\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}\times\begin{bmatrix}76\\65\end{bmatrix}=\begin{bmatrix}9621\\10369\end{bmatrix}=\begin{bmatrix}149\\129\end{bmatrix}$$

$$\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}\times\begin{bmatrix}77\\65\end{bmatrix}=\begin{bmatrix}9692\\10443\end{bmatrix}=\begin{bmatrix}220\\203\end{bmatrix}$$

$$\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}\times\begin{bmatrix}82\\76\end{bmatrix}=\begin{bmatrix}10762\\11616\end{bmatrix}=\begin{bmatrix}10\\96\end{bmatrix}$$

$$\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}\times\begin{bmatrix}69\\78\end{bmatrix}=\begin{bmatrix}9969\\10800\end{bmatrix}=\begin{bmatrix}241\\48\end{bmatrix}$$

$$\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}\times\begin{bmatrix}65\\78\end{bmatrix}=\begin{bmatrix}9685\\10504\end{bmatrix}=\begin{bmatrix}213\\8\end{bmatrix}$$

$$\begin{bmatrix}71 & 65\\74 & 73\end{bmatrix}\times\begin{bmatrix}83\\84\end{bmatrix}=\begin{bmatrix}11353\\12274\end{bmatrix}=\begin{bmatrix}89\\242\end{bmatrix}$$

CIPHERTEXT

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

43 93 149 129 220 203 10 96 241 48 213 8 213 8 89 242
2B 5D 95 81 DC CB 0A 60 F1 30 D5 08 D5 08 59 F2

2. The encryption process with the AES algorithm.

At this stage the encryption process for ciphertext_1 is generated by the Hill Cipher algorithm.
Plaintext (AES): 2B 5D 95 81 DC CB 0A 60 F1 30 D5 08 59 F2
Key (AES): 4B 41 52 59 41 57 41 4E 4B 41 4E 54 4F 52 42 53

$$\begin{bmatrix} 4B & 41 & 4B & 4F \\ 41 & 57 & 41 & 52 \\ 52 & 41 & 4E & 42 \\ 59 & 4E & 54 & 53 \end{bmatrix}\begin{bmatrix} 4A & 0B & 40 & 0F \\ 6D & 3A & 7B & 29 \\ BF & FE & B0 & F2 \\ DD & 93 & C7 & 94 \end{bmatrix}\begin{bmatrix} ED & E6 & A6 & A9 \\ E4 & DE & A5 & 8C \\ 9D & 63 & D3 & 21 \\ AB & 38 & FF & 6B \end{bmatrix}\begin{bmatrix} 8D & 6B & CD & 64 \\ 19 & C7 & 62 & EE \\ E2 & 81 & 52 & 73 \\ 78 & 40 & BF & D4 \end{bmatrix}$$

$$\begin{bmatrix} AD & C6 & 0B & 6F \\ 96 & 51 & 33 & DD \\ AA & 2B & 79 & 0A \\ 3B & 7B & C4 & 10 \end{bmatrix}\begin{bmatrix} 7C & BA & B1 & DE \\ F1 & A0 & 93 & 4E \\ 60 & 4B & 32 & 38 \\ 93 & E8 & 2C & 3C \end{bmatrix}\begin{bmatrix} 73 & C9 & 78 & A6 \\ F6 & 56 & C5 & 8B \\ 8B & C0 & F2 & CA \\ 8E & 66 & 4A & 76 \end{bmatrix}\begin{bmatrix} 0E & C7 & BF & 19 \\ 82 & D4 & 11 & 9A \\ B3 & 73 & 81 & 4B \\ AA & CC & 86 & F0 \end{bmatrix}$$

$$\begin{bmatrix} 36 & F1 & 4E & 57 \\ 31 & E5 & F4 & 6E \\ 3F & 4C & CD & 86 \\ 7E & B2 & 34 & C4 \end{bmatrix}\begin{bmatrix} B2 & 43 & 0D & 5A \\ 75 & 90 & 64 & 0A \\ 23 & 6F & A2 & 24 \\ 25 & 97 & A3 & 67 \end{bmatrix}\begin{bmatrix} E3 & A0 & AD & F7 \\ 43 & D3 & B7 & BD \\ A6 & C9 & 6B & 4F \\ 9B & 0C & AF & C8 \end{bmatrix}$$

ROUND KEY

Round Key 0

$$\begin{bmatrix} 4B & 41 & 4B & 4F \\ 41 & 57 & 41 & 52 \\ 52 & 41 & 4E & 42 \\ 59 & 4E & 54 & 53 \end{bmatrix}$$

Round Key 1

$w[0] = 4B\ 41\ 52\ 59$
$w[1] = 41\ 57\ 41\ 4E$
$w[2] = 4B\ 41\ 4E\ 54$
$w[3] = 4F\ 52\ 42\ 53$

=== process for w[4] ===
byte shift left from w[3]:
$w[3] = 52\ 42\ 53\ 4F$

Byte Substitution (S-Box):
$w[3] = 00\ 2C\ ED\ 84$

Added spin constants (01; 00; 00; 00)

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

$g(w[3]) = 01\ 2C\ ED\ 84$

=== End process for w[4] ===
$w[4] = w[0] \oplus g(w[3]) = 4B\ 41\ 52\ 59 \oplus 01\ 2C\ ED\ 84 = 4A\ 6D\ BF\ DD$
$w[5] = w[1] \oplus w[4] = 41\ 57\ 41\ 4E \oplus 4A\ 6D\ BF\ DD = 0B\ 3A\ FE\ 93$
$w[6] = w[2] \oplus w[5] = 4B\ 41\ 4E\ 54 \oplus 0B\ 3A\ FE\ 93 = 40\ 7B\ B0\ C7$
$w[7] = w[3] \oplus w[6] = 4F\ 52\ 42\ 53 \oplus 40\ 7B\ B0\ C7 = 0F\ 29\ F2\ 94$
Add Round Key 0

$$\begin{bmatrix} 2B & DC & F1 & D5 \\ 5D & CB & 30 & 08 \\ 95 & 0A & D5 & 59 \\ 81 & 60 & 08 & F2 \end{bmatrix} \oplus \begin{bmatrix} 4B & 41 & 4B & 4F \\ 41 & 57 & 41 & 52 \\ 52 & 41 & 4E & 42 \\ 59 & 4E & 54 & 53 \end{bmatrix} = \begin{bmatrix} 60 & 9D & BA & 9A \\ 1C & 9C & 71 & 5A \\ C7 & 4B & 9B & 1B \\ D8 & 2E & 5C & A1 \end{bmatrix}$$

ROUNDS 1
Sub Bytes 1

$$\begin{bmatrix} 60 & 9D & BA & 9A \\ 1C & 9C & 71 & 5A \\ C7 & 4B & 9B & 1B \\ D8 & 2E & 5C & A1 \end{bmatrix} = \begin{bmatrix} D0 & 5E & F4 & B8 \\ 9C & DE & A3 & BE \\ C6 & B3 & 14 & AF \\ 61 & 31 & 4A & 32 \end{bmatrix}$$

Shift Rows 1

$$\begin{bmatrix} D0 & 5E & F4 & B8 \\ DE & A3 & BE & 9C \\ 14 & AF & C6 & B3 \\ 32 & 61 & 31 & 4A \end{bmatrix}$$

Mix Column 1

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} D0 & 5E & F4 & B8 \\ DE & A3 & BE & 9C \\ 14 & AF & C6 & B3 \\ 32 & 61 & 31 & 4A \end{bmatrix} = \begin{bmatrix} E4 & 8C & DD & 2D \\ 79 & 88 & F3 & 1F \\ 70 & 1B & 8E & 87 \\ C5 & 2C & 1D & 68 \end{bmatrix}$$

Add Round Key 1

$$\begin{bmatrix} E4 & 8C & DD & 2D \\ 79 & 88 & F3 & 1F \\ 70 & 1B & 8E & 87 \\ C5 & 2C & 1D & 68 \end{bmatrix} \oplus \begin{bmatrix} 4A & 0B & 40 & 0F \\ 6D & 3A & 7B & 29 \\ BF & FE & B0 & F2 \\ DD & 93 & C7 & 94 \end{bmatrix} = \begin{bmatrix} AE & 87 & 9D & 22 \\ 14 & B2 & 88 & 36 \\ CF & E5 & 3E & 75 \\ 18 & BF & DA & FC \end{bmatrix}$$

Generated ciphertext: F8 64 75 EE D6 0A 11 51 38 30 CF F6 E2 07 0F 9D

4. Results And Discussion

After the encryption process is complete, the ciphertext will no longer be understood,

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

therefore the decryption process must be carried out.

1. **The first decryption step will be carried out with the AES algorithm.**

Ciphertext (AES): F8 D6 38 E2 64 0A 30 07 75 11 CF 0F EE 51 F6 9D

Key (AES): 4B 41 52 59 41 57 41 4E 4B 41 4E 54 4F 52 42 53

ROUNDS 1

Add Round Key 10

$$\begin{bmatrix} F8 & 64 & 75 & EE \\ D6 & 0A & 11 & 51 \\ 38 & 30 & CF & F6 \\ E2 & 07 & 0F & 9D \end{bmatrix} \oplus \begin{bmatrix} E3 & A0 & AD & F7 \\ 43 & D3 & B7 & BD \\ A6 & C9 & 6B & 4F \\ 9B & 0C & AF & C8 \end{bmatrix} = \begin{bmatrix} 1B & C4 & D8 & 19 \\ 95 & D9 & A6 & EC \\ 9E & F9 & A4 & B9 \\ 79 & 0B & A0 & 55 \end{bmatrix}$$

Inverse Shift Rows 1

$$\begin{bmatrix} 1B & C4 & D8 & 19 \\ EC & 95 & D9 & A6 \\ A4 & B9 & 9E & F9 \\ 0B & A0 & 55 & 79 \end{bmatrix}$$

Inverse Sub Bytes 1

$$\begin{bmatrix} 1B & C4 & D8 & 19 \\ EC & 95 & D9 & A6 \\ A4 & B9 & 9E & F9 \\ 0B & A0 & 55 & 79 \end{bmatrix} = \begin{bmatrix} 44 & 88 & 2D & 8E \\ 83 & AD & E5 & C5 \\ 1D & DB & DF & 69 \\ 9E & 47 & ED & AF \end{bmatrix}$$

Plaintext (AES): 2B 5D 95 81 DC CB 0A 60 F1 30 D5 08 59 F2

Key (AES): 4B 41 52 59 41 57 41 4E 4B 41 4E 54 4F 52 42 53

2. **After being decrypted with AES, the next step is the decryption process using the Hill Cipher algorithm.**

Ciphertext (Hill Cipher): 2B 5D 95 81 DC CB 0A 60 F1 30 D5 08 D5 08 59 F2

43 93 149 129 220 203 10 96 241 48 213 8 213 8 89 242

Key (Hill Cipher): "SALARY"

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

$$\begin{bmatrix}71 & 65\\ 74 & 73\end{bmatrix}^{-1} = \frac{1}{373} \times \begin{bmatrix}73 & -65\\ -74 & 71\end{bmatrix} mod\ 256 = \begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}43\\ 93\end{bmatrix} = \begin{bmatrix}78\\ 73\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}149\\ 129\end{bmatrix} = \begin{bmatrix}76\\ 65\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}220\\ 203\end{bmatrix} = \begin{bmatrix}77\\ 65\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}10\\ 96\end{bmatrix} = \begin{bmatrix}82\\ 76\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}241\\ 48\end{bmatrix} = \begin{bmatrix}69\\ 78\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}213\\ 8\end{bmatrix} = \begin{bmatrix}65\\ 78\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}213\\ 8\end{bmatrix} = \begin{bmatrix}65\\ 78\end{bmatrix}$$

$$\begin{bmatrix}5 & 227\\ 30 & 75\end{bmatrix} \times \begin{bmatrix}89\\ 242\end{bmatrix} = \begin{bmatrix}83\\ 84\end{bmatrix}$$

78 73 76 65 77 65 82 76 69 78 65 78 65 78 83 84

Plaintext (Hill Cipher): NILAMARLENANANST

5. Conclusion

in this research, with the existence of a data security system using the hill cipher algorithm and the aes algorithm, it can help to secure the confidentiality of text data so that it reaches the recipient in the same confidentiality as before. With this security system, it can minimize data theft by irresponsible persons. This data security system can secure employee data in the form of letters or numbers, such as the sample that has been successfully secured, namely the employee's name Nila Marlena Nst. This data security system will secure data by first encrypting the data using the Hill Cipher algorithm, then re-encrypting it with the AES algorithm. After the encryption process is complete, the data can no longer be understood by ordinary people. After that, the description process is carried out, namely returning the code in the form of original data by doing a description with the AES algorithm then a description with the Hill Cipher algorithm. The use of these two algorithms makes the level of data security higher so that its security is not easily damaged.

DOI: 10.52362/ijiems.v3i1.1219

International Journal of Informatics, Economics, Management and Science (IJIEMS)
http://journal.stmikjayakarta.ac.id/index.php/ijiems
E-ISSN: 2809-8471 (online), **P-ISSN:** 2809-9281 (Print)
DOI: 10.52362/ijiems.v3i1.1219
Volume 3, Issue 1, January 2024, pp. 29-37

References

[1] Computer Networking Book - Google Search (p. 228). (2018). DEEPUBLISH.
[2] Munir's book.pdf (p. 644). (2019). Bandung Informatics.
[3] Fadlullah, F., Tahir, M., Bintari, BP, Dewi, ML, Ilmy, MF, Ardiansyah, R., Informatics, PP, Madura, UT, & Telang, JR (2023). Implementation of AES Algorithm in Information System Login Authentication. 1(2).
[4] Gusti, O., Aritonang, A., Anwar, B., Kom, S., Kom, M., & Taufik, F. (2019). "Implementation of Cryptography Using the HILL CIPHER Method for Data Security of Cashier Employee Salaries at PT. Matahari Department Store Plaza Medan Fair ". 30, 1–15.
[5] Hasibuan, YW, Veronica, RB, Mathematics, J., Semarang, UN, Gunungpati, KS, & Article, I. (2022). How to Cite. 11(1), 54–68.
[6] Hidayat, A., & Alawiyah, T. (2013). Text Encryption and Decryption using Hill Cipher Algorithm with Rectangle Matrix Key. 9(1), 39–51.
[7] Cryptography Cryptography & Confidentiality, K. (2006). Chapter 2 theoretical basis.
[8] Kromodimoeljo, S. (2009). Cryptographic Theory and Applications. In Zeitschrift fur die Gesamte Hygiene und Ihre Grenzgebiete (Vol. 30, Issue 6).
[9] Problem, R. (n.d.). Implementation of Cryptography Using the Advanced Encryption Standard (AES) Algorithm with the CBC (Chipher Block Chaining) Method and Checking for Error Detection.
[10] Munir, R. (2004). Advanced Encryption Standard (AES) Department of Informatics Engineering , Bandung Institute of Technology 13. Advanced Encryption Standard (AES).
[11] Muhammad Fadlan, Haryansyah, & Rosmini. (2021). Data Security through the Autokey Cipher Super Encryption Model and Column Transposition. Journal of RESTI (System Engineering and Information Technology), 5(6), 1113–1119.
[12] Sitorus, NT (2021). Payroll Data Security for Naori Tigadolok Office Employees Using Einsten Encryption. Journal of Informatics Dialectics (Detika), 2(1), 1–6.
[13] Standard, AE, Aes, A., Aes, A., Standard, AE, Standard, DE, Des, T., Feistel, K., Aes, S., Network, SP, & Spn, K. (2001). AES Algorithm Encryption (Advanced Encryption Standard).
[14] Studies, P., Informatics, T., & Sukabumi, UM (2018). Study of Advanced Encryption Standard (AES).
[15] Wastito, GH (2018). Chapter II Basic Theory. Journal of Chemical Information and Modeling, 53(9), 1689–1699.
[16] Zacky. (2016). AES Algorithm Encryption (Advanced Encryption Standard) - Cryptography & Computer Networks.