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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

Security of Employee Salary Data Using the ElGamal Algorithm By Utilizing the Diffie-Hellman Algorithm Key Generator

Barru Indakholasy [1] , Akim Manaor Hara Pardede [2] , Husnul Khair [3]

[1,2,3] Information System, STMIK Kaputama, Binjai Indonesia

E-mail address:
barruindakholsy2@gmail.com (Barru Indakholasy), akimmhp@live.com (Akim Manaor Hara Pardede), husnul.khair@gmail.com (Husnul Khair)

*Corresponding author : barruindakholasy2@gmail.com

Received: July 11, 2023; **Accepted** : December 18, 2023 ; **Published** : January 23, 2024

Abstract: Data security is something that is very important for companies or organizations, one of which is the South Binjai District Office. Almost all work in the South Binjai sub-district office uses a computer, especially in processing data stored in the form of data files on storage media without encoding. In today's digital era, many irresponsible parties find it easy to tap company data so that it can be easily accessed and there is also some *software* that can be easily used to crack *passwords.* One of the data that needs to be kept confidential is employee salary data. To overcome these problems, a security system is needed to secure text data. The cryptographic method is regarding encryption techniques in which plaintext is scrambled using an encryption key to become ciphertext which is applied in data security systems. The Diffie-Hellman algorithm is a key exchange algorithm, this algorithm is limited to the key exchange process, so it must require another algorithm for the encryption and decryption process such as the ElGamal algorithm. The use of these two algorithms can strengthen the level of data security. From the results of trials conducted, the sample data used containing the word "KARYAWAN" was successfully secured with both diffie-helman and ElGamal algorithms.

Keywords : Diffie-Hellman Algorithm, Data, ElGamal, Cryptography.

1. Introduction

Data security is something that is very important for companies or organizations because there is so much data that must be secured. The South Binjai Sub-District Head Office is one of the government organizations that assists the City of Binjai in the performance of its administrative regional technical implementation led by the Sub-District Head. At the South Binjai Sub-District Office there is a sub-district organizational structure consisting of the Sub-District Head, Secretary, Government Section, Empowerment Section, Peace and Order Section, General Sub-Division, and Finance Sub-Division, all of which have their respective duties or roles. Almost all work in the South Binjai sub-district office uses computers, especially in

DOI: 10.52362/ijiems.v3i1.1221

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

processing data stored in the form of data files. But in today's digital era, many irresponsible parties are easy to tap the company's data so that it can be easily accessed by other parties and there is also some software that can be easily used to crack passwords, this will be very detrimental to the company and endanger the person sending or receiving the data message. Each data is stored in a storage medium without any data encryption so that it is possible for crimes to leak, manipulate, misuse, damage data or information at the South Binjai Sub-District Office.

At the South Binjai Sub-District Office there are various types of data that need to be kept confidential. One of them is employee salary data. Employee salary data at the South Binjai Sub-District Office are managed by the Finance Sub-Division. Salary data that is managed is salary data for honorary employees or daily casual workers (Non-PNS). The salary received by the daily freelance workers at the South Binjai Sub-district Office is in accordance with the UMR received every month. Employee salary data is input which contains the employee's identity, account number and nominal salary amount, which later the data will be submitted to the Bank, and the Bank will process payroll according to the data. However, the salary data has not undergone an encryption process or is still in plaintext form. This of course will make it easier for unauthorized parties to read and manipulate employee salary data if the data is still in plaintext form.

In this case a security system is needed to secure the text of employee salary data at the South Binjai Sub-district Office. A good security system so that the data contained on the computer becomes more secure. The employee salary data is not only the nominal number of the salary that is important to secure, but the employee salary data also contains confidential identities such as the employee's NUP (Employee Serial Number) which needs to be hidden and there are account numbers which really need to be secured as well. Document data is written and printable media used as evidence and information. To secure important and confidential document data, a method is needed to secure data or information using cryptographic methods.

Cryptography is the science of encryption techniques in which plaintext is scrambled using an encryption key to become ciphertext. Cryptography has various methods, in this study the authors used the ElGamal algorithm by utilizing the Diffie-Hellman algorithm key generator. The Diffie-Hellman algorithm is a key exchange algorithm, this algorithm is limited to the key exchange process, so it must require another algorithm for the encryption and decryption process. The effectiveness of the Diffie-Hellman algorithm is the difficulty in calculating discrete logarithms. If in the process of distributing the secret key is wrong, then the information will be easily accessed by other parties during the transmission. The ElGamal algorithm is used for the encryption and decryption processes.

The research entitled Combining Diffie-Hellman and Blowlfish as a Document Security System in 2021, using Diffie-Hellman in sending keys (Key Exchange) was successfully carried out with an average time of 0.405 seconds (Alice) and 0.395 seconds (Bob) from five attempts. which is conducted. The time difference that occurs is due to a delay when sending data through the network. Encryption and decryption with the Blowfish algorithm were also successfully implemented. Encryption time with the smallest document (2.192MB) takes 0.129 seconds and an additional 138 bytes of ciphertext (Rizka, 2021).

Research conducted in 2019 implemented the implementation of the ElGamal asymmetric

DOI: 10.52362/ijiems.v3i1.1221

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

cryptographic algorithm with key generator modifications for encryption and decryption of color images. The ElGamal algorithm is implemented in image security. The modifications to the key generator that were made resulted in a good key match. There is a difference in the comparison of the similarities between the original image and the image after it has been encrypted, while there is no difference in the comparison of the similarities between the original image and the image after it has been decrypted (Indahwati & Prihanto, 2020).

A study in 2022, applying the Quicksort algorithm to generate the ElGamal algorithm for securing document files. By randomizing and sorting values for key formation based on the ElGamal method. The encryption process can be carried out and the results of taking the encryption by carrying out the decryption process can be carried out properly using the ElGamal algorithm based on keys that have been modified with the Quicksort algorithm (Al-Amansyah, 2022).

2. Literature

In this section, the results of previous research will be explained which can be used as a reference in this research topic. This previous research is expected to be able to explain and provide references for writers in completing this research. In the following, some of the selected studies will be explained.

In the research conducted by Fifit Alfiah, Rio Sudarji, Dzakwan Taqiyyuddin Al Fatah (2020) entitled Cryptographic Applications Using the Java Desktop-Based ElGamal Algorithm at Pt. Indo Trada Nissan Jatake vehicle at Raharja University. In this study at Pt. Wahana Indo Trada Nissan Jatake wants to innovate in applying the latest technology to secure information/message data that will be sent via e-mail. There is a lot of important and confidential data such as customer identity data and financial reports. Therefore cryptography is used to be a security system. By implementing the ElGamal algorithm in the form of a desktop-based application that is easy for users to understand and use. The ElGamal algorithm is part of the asymmetric algorithm, the encryption and decryption processes each use a different key (Alfiah et al., 2020).

In research conducted by Ahmad Ihsanudin and Achmad Solichin (2018) entitled Application of the DES Algorithm, Vernam Cipher and Diffie-Hellman to Secure New Student Registration Data at Budi Luhur University. In this study, we looked at the activities of accepting new students at Budi Luhur University, where the registration administration process was carried out in various ways, usually registration was done manually or came directly to the registration section. If dozens or hundreds of students come on the same day, there will definitely be long queues and of course they cannot all be accommodated in the room. This certainly requires a solution to anticipate this with a data security solution to avoid data theft, which is to prevent it from being disseminated for use by irresponsible parties. The DES and Vernam Cipher algorithms with the Diffie-Hellman algorithm key generation are used to secure data. The DES algorithm uses an internal key generated from an external key, in the encryption process using a stream cipher method originating from XOR between plaintext bits and key bits (Ihsanudin & Solichin, 2018).

Luthfiatun Nisa, Tutuk Indriyani and Maretha Ruswiansari conducted a study entitled Image

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

and Text Encryption Applications Using the Diffie-Hellman and ElGamal Algorithms. This study discusses the combination of the Diffie-Hellman and ElGamal algorithms to secure text messages and images. From the research results, for 10 text files with a size of 10 Kb to 100 Kb, an average encryption time of 119.9 ms, a decryption of 248.3 ms, and a throughput of 600.96 Kbps were obtained. Meanwhile for image files with a size of 100x100 pixels to 1000x1000 pixels, an average encryption time of 2623.4 ms was obtained, 4349.5 ms for decryption, an MSE value of 213.95 with a percentage decrease of 27.67%, and a Peak value. The Signal to Noise Ratio (PSNR) is 173.27 dB with a percentage increase of 1.94%. In addition, from the results of the avalanche effect test, the percentage of bit shifts in files is 85.18% and in image files is 84.46% (Nisa et al., 2020).

Research conducted in 2018 implemented the use of the Diffie-Hellman and ElGamal algorithms in an Android-based fingerprint image security application. The encrypted image is a fingerprint image with a size of 120 x 230 pixels. The encryption process produces an image cipher measuring 460 x 360 pixels or 2 times the size of the original image, then decrypted to produce the original image. Of the 30 samples tested using a 16-bit key, the results of encryption and decryption were successful with an average encryption time of 102.482 seconds and an average decryption time of 34.151 seconds. The length of time in the encryption and decryption process is affected by the size of the image and the size of the key. The larger the image size, the longer the encryption process will take and if the number of key size bits used is greater for exchange and key generation, the encryption and decryption process will take longer (Yalisa et al., 2018).

3. Methods

3.1. Problem analysis

Developments in the field of online technology as it is today have made it possible for everyone to exchange information through public networks without any distance and time limitations. It is also possible for data leaks to occur during the process of exchanging information. To be able to reduce threats that occur in the exchange of confidential information in a data communication process, it can be done by coding the information to be stored or sent quickly and accurately.

3.2. Application of the Method

Key Generation Using the Diffie-Hellman Algorithm

The Diffie-Hellman algorithm is used for key generation which will later be used in the encryption and decryption process using the ElGamal algorithm. The key exchange process stage uses the Diffie-Hellman algorithm, the process begins when the sender and recipient of the message exchange keys with each other by agreeing on the same prime p and random integer g values. The sender chooses a random number (a) then calculates it using the formula: ***A=g^a mod p*** and the recipient chooses a random number (b) then calculates it using the formula: ***B=g^b mod p*** .

p = 331

g = 5

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

a = 41 (private) : sender
b = 43 (private) : recipient
A=g^a mod p=5^41 mod 331=302
B=g^b mod p=5^43 mod 331=268
Ya=B^a mod p=268^41 mod 331=234
Yb =A^b mod p=302^43 mod 331=234
Yes = Yb = Yprivat : x (private key)

Calculating the value of the public key y :
y =g^x mod p=5^234 mod 331=56

Encryption and Decryption process using the ElGamal algorithm
The results of the private key and public key from the Diffie-Hellman algorithm will be called to be used as a key in the ElGamal Encryption and Decryption process. The results of the public key from the Diffie-Hellman algorithm will be used to encrypt plaintext with the ElGamal algorithm, while the private key will be used to decrypt the ciphertext with the ElGamal algorithm.

Private Key (x) = 234 and Public Key (y) = 56.

Encryption Process
p = 331
g = 5
x = 234
y =g^x mod p=5^234 mod 331=56
Plaintext : KARYAWAN
Plaintext will be cut into character blocks and converted into ASCII numbers.

Table 1. Plaintext conversion to ASCII numbers

Character	plaintext m_i	ASCII
K	m_1	75
A	m2 _	65
R	m_3	82
Y	m_4	89
A	m_5	65
W	m_6	87
A	m_7	65
N	m_8	78

Next is to determine the random value k, where $1 \leq k \leq p - 1$.

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

Table 2. Plaintext Random Values

Character	plaintext m $_i$	ASCII	Key k $_i$
K	m $_1$	75	17
A	m2 _	65	17
R	m $_3$	82	17
Y	m $_4$	89	17
A	m $_5$	65	17
W	m $_6$	87	17
A	m $_7$	65	17
N	m $_8$	78	17

Then calculate c_1 = ***g^ k mod p and c2 = y^k × m (mod p) .***

For K(75)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 75\ (mod\ 331)$
$c_2 = 305$
$\boldsymbol{c = (195, 305\ )}$

For A(65)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 65\ (mod\ 331)$
$c_2 = 154$
$\boldsymbol{c = (195\ , 154)}$

For R(82)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 82\ (mod\ 331)$
$c_2 = 179$

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

$\boldsymbol{c} = (\mathbf{195}, \mathbf{179})$

For Y(89)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 89\ (mod\ 331)$
$c_2 = 53$
$\boldsymbol{c} = (\mathbf{195}, \mathbf{53})$

For A(65)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 65\ (mod\ 331)$
$c_2 = 154$
$\boldsymbol{c} = (\mathbf{195}, \mathbf{154})$

For W(87)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 87\ (mod\ 331)$
$c_{52} = 89$
$\boldsymbol{c} = (\mathbf{195}, \mathbf{89})$

For A(65)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 65\ (mod\ 331)$
$c_2 = 154$
$\boldsymbol{c} = (\mathbf{195}, \mathbf{154})$

For N(78)
$c_1 = g^k mod\ p = 5^{17}\ mod\ 331 = 195$
$c_2 = y^k \times m\ (mod\ p)$
$c_2 = 56^{17} \times 78\ (mod\ 331)$
$c_2 = 251$
$\boldsymbol{c} = (\mathbf{195}, \mathbf{251})$

Ciphertext results :
(195, 305), (195, 154), (195, 179), (195, 53), (195, 154), (195, 89), (195, 154),$(\mathbf{195}, \mathbf{251})$

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

4. Results And Discussion

Decryption Process

Decrypt the ciphertext results by performing calculations with the formula:

$$\boldsymbol{m = c_2 \times c_1^{p-1-x}\ (mod\ p)}$$

p = 331

x = 234

C = (195, 305)

$m = c_2 \times c_1^{p-1-x}\ (mod\ p)$

$m = 305 \times 195^{331-1-234} \text{mod } 331$

$m = 305 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 75}$

C = (195, 154)

$m = c_2 \times c_1^{p-1-x}\ (mod\ p)$

$m = 154 \times 195^{331-1-234} \text{mod } 331$

$m = 154 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 65}$

C = (195, 179)

$m = c_2 \times c_1^{p-1-x}\ (mod\ p)$

$m = 179 \times 195^{331-1-234} \text{mod } 331$

$m = 179 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 82}$

C = (195, 53)

$m = c_2 \times c_1^{p-1-x}\ (mod\ p)$

$m = 53 \times 195^{331-1-234} \text{mod } 331$

$m = 53 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 89}$

C = (195, 154)

$m = c_2 \times c_1^{p-1-x}\ (mod\ p)$

$m = 154 \times 195^{331-1-234} \text{mod } 331$

$m = 154 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 65}$

DOI: 10.52362/ijiems.v3i1.1221

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

C = (195, 89)

$m = c_2 \times c_1^{p-1-x} \ (mod\ p)$

$m = 89 \times 195^{331-1-234} \text{mod } 331$

$m = 89 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 87}$

C = (195, 154)

$m = c_2 \times c_1^{p-1-x} \ (mod\ p)$

$m = 154 \times 195^{331-1-234} \text{mod } 331$

$m = 154 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 65}$

C = (195, 251)

$m = c_2 \times c_1^{p-1-x} \ (mod\ p)$

$m = 251 \times 195^{331-1-234} \text{mod } 331$

$m = 251 \times 195^{96} \text{mod } 331$

$\boldsymbol{m = 78}$

After getting the value m, **the results of the description** are:

75 65 82 89 65 87 65 78

The decryption results are converted to character form to:

Table 3. Description results converted into characters

Plaintext ASCII code	Character
75	K
65	A
82	R
89	Y
65	A
87	W
65	A
78	N

KARYAWAN

(Return to the initial plaintext form).

5. Conclusion

DOI: 10.52362/ijiems.v3i1.1221

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.v3i1.1221
Volume 3, Issue 1, January 2024, pp. 38-47

in this research, with a data security system using the ElGamal algorithm by utilizing the Diffi-Hellman algorithm key generator, it can help employees of the Binjai Sub-district Office in the process of sending data without fear of irresponsible parties taking access to the data. Even if an irresponsible party wants to access employee salary data, they cannot use the data because the data is no longer in plaintext form so that it cannot be read by anyone. The use of the two ElGamal and Diffi-Hellman algorithms makes the level of data security higher than security systems in general. This data security system secures data by performing a key generation process using the Diffie-Hellman algorithm, then carrying out the encryption and description process using the ElGamal algorithm, then the secured data returns to its initial plaintext form or original data. This data security system can secure employee data in doc format both letters and numbers such as samples that have been successfully secured, namely data in the form of letters that read "KARYAWAN".

References

[1] Al-Amansyah, AA (2022). Implementation of the Quicksort Algorithm for Generating Elgamal Algorithm Keys in Securing Document File Data. Bulletin of Artificial Intelligence, 1(1), 17–24.
[2] Alfiah, F., Sudarji, R., & Al Fatah, DT (2020). Cryptographic Application Using Elgamal Algorithm Based on Java Desktop at Pt. Wahana Indo Trada Nissan Jatake. ADI Digital Business Interdisciplinary Journal, 1(1), 22–34.
[3] Erick, K. (2011). Quickly Proficient in Visual Basic 2010. CV Andi Offset.
[4] Ihsanudin, A., & Solichin, A. (2018). SKANIKA VOLUME 1 NO. MARCH 1 2018 60 Application of the DES Algorithm, Vernam Cipher and Diffie-Hellman to Secure New Student Registration Data on. 1(1), 60–67.
[5] Indahwati, N., & Prihanto, A. (2020). Application of Elgamal Asymmetric Cryptographic Algorithm with Key Generation Modification to Color Image Encryption and Decryption. Journal of Informatics and Computer Science (JINACS), 1(02), 97–103.
[6] Munir, R. (2019). CRYPTOGRAPHY (SECOND EDition). Bandung Informatics.
[7] Nisa, L., Indriyani, T., & Ruswiansari, M. (2020). Image and Text Encryption Applications Using Diffie-Hellman and ElGamal Algorithms. Journal of Technology and Management, 1(1), 8–17.
[8] Rizka, M. (2021). The combination of Diffie Hellman and Blowfish as a Document Security System. Infomedia Journal, 6(2), 86.
[9] Setiawan, R. (n.d.). Flowcharts Are: Functions, Types, Symbols, and Examples. August 4, 2021.
[10] Singh, R., & Kumar, S. (2012). Elgamal's Algorithm in Cryptography. International Journal of Scientific & Engineering Research, 3(12), 3–6.
[11] Yalisa, N., Arhami, M., & Azhar, A. (2018). Elgamal Algorithm with Diffie Hellman Key Exchange on Android-Based Fingerprint Image Security Applications. Proceedings of the National Seminar …, 2(1), 1–7.

DOI: 10.52362/ijiems.v3i1.1221