ISSN No:-2456-2165

Diffie-Hellman Based Hill Cipher Key Generation on End-to-end Encryption Key Share

Andysah Putera Utama Siahaan
Faculty of Science and Technology
Universitas Pembangunan Panca Budi, Medan, Indonesia

Abstract:- Data leakage is a frequent occurrence due to security system vulnerabilities. The key is the most valuable object in the encryption and decryption process. The Hill Cipher algorithm also has a key in the form of several decimal numbers placed in a square matrix. This key exchange will result in system security vulnerabilities. This study uses the Diffie-Hellman technique in key exchange where the key sent by the sender to the recipient is in the form of a number which is the component that forms the actual key value. The results of the study stated that the key generation using the Diffie-Hellman algorithm was successfully used by the Hill Cipher algorithm even though in the generation process it produced several values that did not have the appropriate determinant.

Keywords:- *Hill Cipher, Diffie-Hellman, End-to-end, Encryption, Decryption*

I. INTRODUCTION

Computer security is very important to note. In sending data, there is the main thing that must be considered, namely the security of the data. Sending data over the internet can cause data leaks. Sending data that does not have security will cause harm to the sender and recipient of the message. Data leaks often cause great losses, especially if the data sent has a very important meaning.

Data transmission can be done using cryptographic techniques [1]. There are many algorithms that can be used to transmit data. One of the algorithms that can be used in data transmission is the Hill Cipher algorithm. This algorithm is a classic algorithm that uses a square matrix in the encryption and decryption process. The Hill Cipher algorithm encryption process requires four values for the 2 x 2 matrix and nine values for the 4 x 4 matrix. Each value will be used for the encryption process and the inverse of that value will be used for the decryption process.

The vulnerability of the Hill Cipher algorithm is that if the key is distributed to the recipient, it will have the potential to cause data leakage so that the key distribution process is one way that is not recommended.

The Diffie-Hellman algorithm is an algorithm that can be used to exchange keys without providing real numbers or without having to distribute the original key between the sender and recipient of the message [2]. The technique used by the Diffie-Hellman algorithm is similar to the Three-pass Protocol technique. It performs the encryption and decryption process without having to exchange keys at all [3], while the technique used by the Diffie-Hellman algorithm is that keys can be exchanged in a secret way using mathematical calculations.

II. LITERATURE REVIEW

A. Cryptography

Cryptography is the art of writing messages in the form of ciphers or arranged in the form of characters that cannot be understood. Cryptography has two processes, namely encryption, and decryption. Encryption is the process of transforming plaintext into ciphertext so that the message can no longer be understood while decryption is the process of returning the ciphertext to plaintext so that it can be read and understood again in its form and content [4].

B. Hill Cipher

Hill cipher is a cryptographic algorithm that is polygraphic substitution based on linear algebra. Hill cipher uses modulo operation to perform encryption and decryption processes depending on the limitation of the number of characters used. Hill Cipher algorithm is often used for the use of modulo 26 according to the number of letters from A to Z. Each letter will be replaced with an index of 0 to 25. In performing encryption, each block of n letters will be formed in a square matrix of 2 x 2 or 3 x 3 or n × n and will then be multiplied by the value of each generated key. To decrypt the message, each block is multiplied by the reciprocal of the matrix used for encryption [5].

C. Diffie-Hellman

The Diffie-Hellman algorithm is one of the cryptographies for exchanging decimal numbers without having to give the lift to each sender and recipient. Both the sender and the recipient will perform a mathematical calculation whose results are public and private. Values that are public will be returned to the sender or recipient to search for the next value. The last calculation will get the same value between sender and receiver. This value will be used as a key in the encryption and decryption process [6].

Diffie–Hellman key exchange is a method of generating and exchanging keys used for secure cryptographic techniques over public networks or the internet. This technique was one of the first public key protocols devised by Ralph Merkle and named after Whitfield Diffie and Martin Hellman [7].

ISSN No:-2456-2165

Table 1. Diffie-Hellman Schematic

Sender	Receiver
N	G
X	Y
$A = G^X \text{ Mod } N$	$B = G^Y \text{ Mod } N$
$K = B^X \text{ Mod } N$	$K = A^Y \text{ Mod } N$

Key generation using the Diffie-Hellman algorithm can be seen in table 1. The sender determines the value of N, the receiver determines the value of G as a public number which will then be exchanged. The sender determines the value of X and the receiver determines the value of Y which is private. The values of X and Y will be held by the sender and receiver respectively. The sender and receiver will determine the values of A and B based on the modulo exponential calculation. The final calculation of the exponential modulo will produce a value of K where this number will be the same for the sender and receiver.

III. RESEARCH METHODOLOGY

This research has several parts that were carried out to get the results. There are several important parts that will be explained related to the stages of research.

A. Research Flowchart

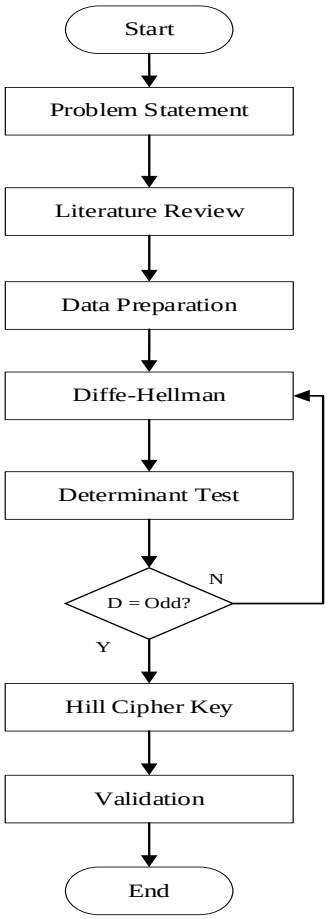

Fig 1. Research Flowchart

This study has several stages that will be passed in determining the numbers to be used in the Hill Cipher algorithm. The flow of the research can be seen in Figure 1. This flow explains that data preparation is done by taking a random decimal value to be tested and processed using the Diffie-Hellman algorithm. The key results obtained will be tested using the Hill Cipher algorithm whether the value has obtained the appropriate determinant value. This process is repeated 4 times to get the Hill Cipher key with a 2 x 2 matrix. Key validation is done by determining whether the generated key has the appropriate determinant and has an inverse key.

B. Research Type

This research is quantitative where this research uses discrete data and continuum data, such as the data obtained in the form of numbers generated by a computer randomly. This data is used as test data from the calculation of the Diffie-Hellman algorithm in looking at the key exchange process and the encryption and decryption process on the Hill Cipher algorithm.

C. Data Collection Technique

The data used in this study uses random decimal numbers. The number is limited from 0 to 255 according to the number of characters in the ASCII table. This is so that no value of the process results will exceed the capacity that has been determined by the ASCII table.

IV. RESULTS AND DISCUSSION

A. Results

Testing is done by trying to generate four numbers that will be used by the Hill Cipher algorithm. The matrix used is 2 x 2.

Table 2. Hill Cipher Key (Generation 1)

	Sender	Receiver	
N	253	49	G
X	10	83	Y
A	100	246	B
K	243	243	K
N	198	45	G
X	180	82	Y
A	45	45	B
K	45	45	K
N	92	204	G
X	23	14	Y
A	20	4	B
K	4	4	K
N	201	240	G
X	121	128	Y
A	171	33	B
K	96	96	K

Key generation results using the Diffie-Hellman technique generate $K = \begin{bmatrix} 243 & 45 \\ 4 & 96 \end{bmatrix}$. The search for the determinant is carried out based on the key that has been

generated is $D = (243 * 96) - (4 * 45) = 23148$. The resulting determinant is an even value so it cannot be used for the Hill Cipher algorithm decryption process because it does not have the correct inverse key.

Table 3. Hill Cipher Key (Generation 2)

	Sender	**Receiver**	
N	196	37	G
X	181	209	Y
A	121	53	B
K	81	81	K
N	158	182	G
X	33	49	Y
A	78	24	B
K	78	78	K
N	170	205	G
X	117	233	Y
A	35	35	B
K	35	35	K
N	72	101	G
X	172	200	Y
A	25	49	B
K	49	49	K

The results of key generation using the Diffie-Hellman technique in the second experiment is $K = \begin{bmatrix} 81 & 78 \\ 35 & 49 \end{bmatrix}$ The search for the determinant is carried out based on the key that has been generated is $D = (81 * 49) - (78 * 35) = 1239$. The resulting determinant is odd so that it can be used for the decryption process of the Hill Cipher algorithm because it has the correct inverse key. The inverse key obtained is $Ki = \begin{bmatrix} 55 & 158 \\ 107 & 23 \end{bmatrix}$

B. Discussion

In determining the key to be used by the Hill Cipher algorithm, it takes several tries to get an odd-valued determinant. There are four items that are determined during the Diffie-Hellman algorithm process, namely N, G, X and B, the results of the exponential modulo process will produce the same value of K between the sender and receiver. This K value will then be entered into each part of the Hill Cipher matrix. If the four values do not produce the appropriate determinant, then the key generation process will be repeated from the beginning and determine the four values to be entered into the Hill Cipher matrix.

V. CONCLUSION

Hill Cipher key generation using the Diffie-Hellman algorithm is very helpful for the sender and recipient of the message in avoiding key exchange. Diffie-Hellman is able to reduce the potential for data leaks that can occur due to keys distributed directly through the internet network.

REFERENCES

[1]. D. Kurnia, H. Dafitri, A. P. U. Siahaan, Sugianto, and Mardiana, "RSA 32-bit Implementation Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, pp. 279–284, Jul. 2017, doi: 10.23883/IJRTER.2017.3359.UXAIW.

[2]. A. Kamsyakawuni, Fanani, A. Husnan, and A. Riski, "Pengamanan Citra dengan Algoritma Diffie-Hellman dan Algoritma Simplified Data Encryption Standard (S-DES)," *J. Ilm. Mat. dan Pendidik. Mat.*, vol. 10, no. 2, pp. 63–80, 2018.

[3]. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 1149–1152, 2016.

[4]. A. I. Permana, T. Tulus, and Z. Situmorang, "Combination of One Time Pad Cryptography Algorithm with Generate Random Keys and Vigenere Cipher with EM2B KEY," in *International Conference on Management, Business, Applied Science, Engineering and Sustainability Development*, 2020, doi: 10.4108/eai.3-8-2019.2290723.

[5]. J. R. Paragas, A. M. Sison, and R. P. Medina, "A New Variant of Hill Cipher Algorithm using Modified S-Box," *Int. J. Sci. Technol. Res.*, vol. 8, no. 10, pp. 615–619, 2019.

[6]. Purwadi, H. Jaya, and A. Calam, "Aplikasi Kriptografi Asimetris dengan Metode Diffie-Hellman dan Algoritma ElGamal untuk Keamanan Teks," *J. Ilm. Saintikom*, vol. 13, no. 3, pp. 183–196, 2014.

[7]. W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory.*, vol. 22, no. 6, pp. 644–654, 1976.