Hadamard Matrix on Cryptographic Problems

Salman Al Farizi[1], Mashuri Mashuri[1], Bambang Hendriya Guswanto[*1]

[1]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, Jenderal Soedirman University, Jl. Dr. Soeparno 61, Purwokerto 53123, Indonesia*
**Corresponding author. Email: bambang.guswanto@unsoed.ac.id*

ABSTRACT
The application of matrices to cryptographic problems, especially with Hill Chiper algorithm, needs an invertible matrix as a key and a plaintext's difuser. One of the invertible matrices is a Hadamard matrix (***H***). The Hadamard matrix is applied to cryptographic problems with Hill Chiper algorithm by modifying encryption and decryption processes with the help of Hadamard matrix properties and modulo operation. The Hill Chiper algorithm requires two keys, namely public and private keys. By using the Hadamard matrix as a public key, the encryption process can be shortened by eliminating the process of checking of the reverse key matrix. Any character can also be used as a private key provided the number of characters doesn't exceed the square of the Hadamard matrix order.

Keywords : *Hadamard matrix, encryption, decryption, Hill Chiper*

1. INTRODUCTION

Matrices can be applied in the cryptographic problems. One of the cryptographic algorithms that uses a matrix is the Hill Chiper algorithm. This algorithm uses the matrix as a key to transform plaintext into ciphertext at an encryption process. Then, in the decryption process, ciphertext is multiplied by the inverse of the key matrix to return it to plaintext [1]. This means that the matrix is used as a key and difuser in the Hill Cipher. The condition for a matrix used in this algorithm is that it must have an inverse under multiplication operation.

One of matrices that has an inverse is the Hadamard matrix. This matrix is a square matrix whose entries are either $+1$ or -1 and whose rows are mutually orthogonal [2],[3]. The absolute value of the determinant of the matrix is $n^{n/2}$ where n is the order of the matrix [4]. Since the Hadamard matrix is an invertible matrix, it can be used as a key matrix in the Hill Cipher algorithm.

The modification of the Hill Chiper algorithm using the Hadamard matrix makes the algorithm more complex [5]. However, the Hill Chiper algorithm still can be destroyed through cryptanalysis such as brute force attack, plaintext attack, and ciphertext attack [6]. Therefore, the authors modify the Hill Chiper algorithm by employing modulo operation and the properties of the Hadamard matrix. This modification makes the encryption and decryption processes require two keys, namely the public and private key. The public key in this modification uses the Hadamard matrix. Thus the computer program associated with the algorithm can be shortened since the process to check the invertibility of the public key matrix is not required. Besides, any character can be input as a private key. This makes the algorithm even more difficult to destroy.

2. RESULTS AND DISCUSSION

The encryption process makes plaintext in the form of characters as input and produces ciphertext in the form of characters as output. The decryption process is the opposite of the encryption process. Both processes require the American Standard Code of Information Interchange (ASCII) to convert characters to decimal code and vice versa. The ASCII codes are limited, there are only 256 characters. Thus, the encryption process is modified as follows:

$$\boldsymbol{C} = (\boldsymbol{H} \cdot \boldsymbol{P}) + (\boldsymbol{K} \cdot \boldsymbol{e}) \bmod m$$

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \left(\begin{pmatrix} h_{11} & \dots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{n1} & \dots & h_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} + \begin{pmatrix} k_{11} & \dots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{n1} & \dots & k_{nn} \end{pmatrix} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \right) mod\ m. \quad (1)$$

Through the definition of the Hadamard matrix, the inverse of the matrix is known as $\frac{1}{n}\boldsymbol{H_n}^{\boldsymbol{T}}$, so that the decryption process is expressed as

$$\begin{aligned} \boldsymbol{C} &= (\boldsymbol{H}\cdot\boldsymbol{P})+(\boldsymbol{K}\cdot\mathbf{e})\bmod m \\ \boldsymbol{C}-(\boldsymbol{K}\cdot\mathbf{e})\bmod m &= (\boldsymbol{H}\cdot\boldsymbol{P})\bmod m \\ \boldsymbol{H^{-1}}\cdot\boldsymbol{C}-(\boldsymbol{K}\cdot\mathbf{e})\bmod m &= \boldsymbol{H^{-1}}\cdot(\boldsymbol{H}\cdot\boldsymbol{P})\bmod m \\ \left(\frac{\mathbf{1}}{\boldsymbol{n}}(\boldsymbol{H^{T}})\cdot(\boldsymbol{C}-(\boldsymbol{K}\cdot\mathbf{e}))\right)\bmod m &= \boldsymbol{I}\cdot\boldsymbol{P} \\ \boldsymbol{P} &= \left(\frac{\mathbf{1}}{\boldsymbol{n}}(\boldsymbol{H^{T}})\cdot(\mathbf{C}-(\boldsymbol{K}\cdot\mathbf{e}))\right)\bmod m \end{aligned}$$

$$\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \left(\frac{1}{n} \begin{pmatrix} h_{11} & \dots & h_{n1} \\ \vdots & \ddots & \vdots \\ h_{1n} & \dots & h_{nn} \end{pmatrix} \left(\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} - \begin{pmatrix} k_{11} & \dots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{n1} & \dots & k_{nn} \end{pmatrix} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \right) \right) mod\ m \qquad (2)$$

where

$\boldsymbol{C}$	: the chipertext,
$\boldsymbol{P}$	: the plaintext,
$\boldsymbol{H}$	: the Hadamard matrix,
$\boldsymbol{K}$	: the private key,
$\boldsymbol{e}$	: the generator,
m	: the number of ASCII that's used,
n	: the order of the Hadamard matrix that's used,
$\boldsymbol{I}$	: the identity matrix,
$\boldsymbol{H^{-1}}$	: the inverse of the Hadamard matrix,
$\boldsymbol{H_n}^{\boldsymbol{T}}$	: the transpose of the Hadamard matrix.

The Hill Chiper algorithm modification using the Hadamard matrix involves modulo operations. The modulo operation only applies to integers [1]. In the decryption process, this algorithm uses the inverse of the Hadamard matrix as the inverting key of the ciphertext. Therefore, $\frac{1}{n}\ mod\ m$ in equation (2) can be expressed as the modulo m inverse of n symbolized by $n^{-1}\ mod\ m$. It is satisfied when n and m are relatively prime. The further condition of this algorithm is that the number of characters used as the private key isn't more than n^2.

2.1. Encryption on the Hill Chiper Algorithm Using the Hadamard Matrix

The following is an encryption process using a Hadamard matrix of order 2×2 as a public key and 255 characters in ASCII code. For example, given plaintext

"**Matematika Unsoed**"

with

"**mtk2**"

is as the private key and

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is as the Hadamard matrix. The encryption process is carried out in the following way.

2.1.1. Validating the Order of the Hadamard Matrix and the Number of ASCII Used are Relatively Prime

Since 4 < 255, the greatest common divisor of 4 and 255 symbolized by *gcd*(4,255) can be written as *gcd*(255, 4). Then, using Euclid's algorithm, we get

$$255 = 127 \cdot 2 + 1,$$
$$2 = 2 \cdot 1 + 0.$$

It means that *gcd*(2, 255) = *gcd*(255, 1) = 1. Therefore, 4 and 255 are relatively prime. The modified Hill Chiper algorithm can be used.

2.1.2. Representing the Private Key as a 2×2 Matrix

The number of characters in the private key is 4, so that the number of entries in the matrix of order 2×2 is 4. Then, the private key is represented as the matrix

$$\begin{pmatrix} m & t \\ k & 2 \end{pmatrix}.$$

2.1.3. Converting Every Character in the Private Key to be Decimal Number

Each character is converted to be decimal number, so that we get

$$\begin{pmatrix} 109 & 116 \\ 107 & 50 \end{pmatrix}.$$

2.1.4. Spliting the Plaintext into 2×1 Blocks

Each block consists of 2 characters since the Hadamard matrix used is a matrix of order 2×2. Then, the obtained matrices $\boldsymbol{P_1}$, $\boldsymbol{P_2}$, $\boldsymbol{P_3}$, $\boldsymbol{P_4}$, $\boldsymbol{P_5}$, $\boldsymbol{P_6}$, $\boldsymbol{P_7}$, $\boldsymbol{P_8}$, and $\boldsymbol{P_9}$ are

$$\begin{pmatrix} M \\ a \end{pmatrix}, \begin{pmatrix} t \\ e \end{pmatrix}, \begin{pmatrix} m \\ a \end{pmatrix}, \begin{pmatrix} t \\ i \end{pmatrix}, \begin{pmatrix} k \\ a \end{pmatrix}, \begin{pmatrix} Space \\ U \end{pmatrix}, \begin{pmatrix} n \\ s \end{pmatrix}, \begin{pmatrix} o \\ e \end{pmatrix}, \text{ and } \begin{pmatrix} d \\ Space \end{pmatrix}$$

respectively. The number of characters in "**Matematika Unsoed**" is 17. Consequently, when they are divided into 2×1 blocks, there are 9 blocks with 1 incomplete block. Here, incomplete blocks are filled with "space" as dummy characters.

2.1.5. Converting Every Character in Plaintext to be a Decimal Number

Each character is converted to be a decimal number. Then, we get

$\begin{pmatrix}77\\97\end{pmatrix}, \begin{pmatrix}116\\101\end{pmatrix}, \begin{pmatrix}109\\97\end{pmatrix}, \begin{pmatrix}116\\105\end{pmatrix}, \begin{pmatrix}107\\97\end{pmatrix}, \begin{pmatrix}32\\85\end{pmatrix}, \begin{pmatrix}110\\115\end{pmatrix}, \begin{pmatrix}111\\101\end{pmatrix}$, and $\begin{pmatrix}100\\32\end{pmatrix}$.

2.1.6. Encrypting Each Plaintext Block One by One

The eencryption is done through the following calculation.

$$C_1 = \left((H_2 \cdot P_1) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}144\\137\end{pmatrix}$$

$$C_2 = \left((H_2 \cdot P_2) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}187\\172\end{pmatrix}$$

$$C_3 = \left((H_2 \cdot P_3) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}176\\169\end{pmatrix}$$

$$C_4 = \left((H_2 \cdot P_4) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}191\\168\end{pmatrix}$$

$$C_5 = \left((H_2 \cdot P_5) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}174\\167\end{pmatrix}$$

$$C_6 = \left((H_2 \cdot P_6) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}87\\104\end{pmatrix}$$

$$C_7 = \left((H_2 \cdot P_7) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}195\\152\end{pmatrix}$$

$$C_8 = \left((H_2 \cdot P_8) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}182\\167\end{pmatrix}$$

$$C_9 = \left((H_2 \cdot P_9) + (K \cdot e_2)\right) \bmod 255 = \begin{pmatrix}102\\225\end{pmatrix}$$

That calculation obtained ciphertext block C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, and C_9, namely

$\begin{pmatrix}144\\137\end{pmatrix}, \begin{pmatrix}187\\172\end{pmatrix}, \begin{pmatrix}176\\169\end{pmatrix}, \begin{pmatrix}191\\168\end{pmatrix}, \begin{pmatrix}174\\167\end{pmatrix}, \begin{pmatrix}87\\107\end{pmatrix}, \begin{pmatrix}195\\152\end{pmatrix}, \begin{pmatrix}182\\167\end{pmatrix}$, and $\begin{pmatrix}102\\225\end{pmatrix}$

respectively.

2.1.7. Converting Each Number in the Chipertext Matrices to be Characters

Each number in C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, and C_9 is converted to a character. Then, the ciphertext block becomes

$\begin{pmatrix}‰\end{pmatrix}, \begin{pmatrix}»\\¬\end{pmatrix}, \begin{pmatrix}°\\©\end{pmatrix}, \begin{pmatrix}¿\\¨\end{pmatrix}, \begin{pmatrix}®\\§\end{pmatrix}, \begin{pmatrix}W\\h\end{pmatrix}, \begin{pmatrix}Ã\\˜\end{pmatrix}, \begin{pmatrix}¶\\§\end{pmatrix}$, and $\begin{pmatrix}f\\á\end{pmatrix}$.

Thus, we get the ciphertext "**‰»¬°©¿¨®§WhÃ˜¶§fá**" as the result of encryption of "**Matematika Unsoed**".

The encryption process using Matlab is done as shown in **the Figure 1**.

```
Command Window
>> Encrypt
INPUT YOUR TEXT PLEASE : Matematika Unsoed
THE ORDER OF MATRIX : 2
THE MODULO OPERATION : 255
INPUT THE PRIVATE KEY : mtk2

ans =

‰»¬°©¿¨®§WhÃ˜¶§fá
```

Figure 1 Encryption process using Matlab

The program instructs to input the encrypted plaintext. Then, by inputting "Matematika Unsoed", the program is ordered to input the order of the Hadamard matrix, the private key, the modulo operation, and the Hadamard matrix used. The user input 2 as the order of the matrix, "mtk2" as the private key, and 255 as the modulo operation number. The user also inputs

$$\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

as the Hadamard matrix used. Then, the program displays

"**‰»¬°©¿¨®§WhÃ˜¶§fá**".

Thus, we get the ciphertext "**‰»¬°©¿¨®§WhÃ˜¶§fá**" from plaintext "Matematika Unsoed".

2.2. Decryption on the Hill Chiper Algorithm Using the Hadamard Matrix

The following is a decryption process using a Hadamard matrix of order 2×2 as a public key and 255 characters in ASCII code. For example, given ciphertext

"**‰»¬°©¿¨®§WhÃ˜¶§fá**"

with

"**mtk2**"

is as the private key and

$$H_2 = \begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

is as the Hadamard matrix used. The decryption process is carried out in the following way.

2.2.1. Representing the Private Key as a 2x2 Matrix

The private key is represented by the matrix

$$\begin{pmatrix} m & t \\ k & 2 \end{pmatrix}.$$

2.2.2. Converting Every Character in the Private Key to be a Decimal Number

Each character is converted to be a decimal number, so that we get

$$\begin{pmatrix} 109 & 116 \\ 107 & 50 \end{pmatrix}.$$

2.2.3. Finding the Inverse of the $\boldsymbol{H_2}$ mod 255 Matrix

Based on equation (2), the inverse of $\boldsymbol{H_2}$ mod 255 can be expressed as

$$\begin{aligned} \boldsymbol{H_2}^{-1} \bmod 255 &= \tfrac{1}{2}\left(\boldsymbol{H_2}^{T}\right) \bmod 255 \\ &= 2^{-1}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \bmod 255. \end{aligned} \quad (3)$$

In the encryption process, 2 and 255 are relatively prime so that the inverse of 2 mod 255 exists. To find the inverse of 2 mod 255, $gcd(2, 255) = 1$ is expressed in a linear combination using Euclid's algorithm, namely

$1 = 255 \cdot (1) - (127) \cdot (2)$

$= (255) \cdot (1) + (2) \cdot (-127).$

We get 1 mod 255 ≡ 2 (−127) + 255 (1) mod 255. This shows that 1 mod 255 ≡ 2 (−127) mod 255. Therefore, the inverse of 2 mod 255 is −127. Thus, the inverse of the Hadamard matrix can be expressed as

$$\begin{aligned} \tfrac{1}{2}\left(\boldsymbol{H_2}^{T}\right) \bmod 255 &= (-127)\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \bmod 255 \\ &= \begin{pmatrix} -127 & -127 \\ -127 & 127 \end{pmatrix} \bmod 255 \\ &= \begin{pmatrix} 128 & 128 \\ 128 & 127 \end{pmatrix}. \end{aligned}$$

2.2.4. Spliting Chipertext into 2×1 Blocks

The Ciphertext is respectively grouped into matrices $\boldsymbol{C_1}$, $\boldsymbol{C_2}$, $\boldsymbol{C_3}$, $\boldsymbol{C_4}$, $\boldsymbol{C_5}$, $\boldsymbol{C_6}$, $\boldsymbol{C_7}$, $\boldsymbol{C_8}$, and $\boldsymbol{C_9}$, namely

$\begin{pmatrix} \\ ‰ \end{pmatrix}, \begin{pmatrix} » \\ ¬ \end{pmatrix}, \begin{pmatrix} ° \\ © \end{pmatrix}, \begin{pmatrix} ¿ \\ ¨ \end{pmatrix}, \begin{pmatrix} ® \\ § \end{pmatrix}, \begin{pmatrix} W \\ h \end{pmatrix}, \begin{pmatrix} Ã \\ ˜ \end{pmatrix}, \begin{pmatrix} ¶ \\ § \end{pmatrix}$, and $\begin{pmatrix} f \\ á \end{pmatrix}$.

The number of characters of "**‰»¬°©¿¨®§WhÃ˜¶§fá**" is 18. Thus, when they are divided into 2×1 blocks, there are 9 ciphertext blocks.

2.2.5. Converting Each Character to be a Decimal Number

Each character that's in the chipertext is converted to be a decimal number, namely

$\begin{pmatrix} 144 \\ 137 \end{pmatrix}, \begin{pmatrix} 187 \\ 172 \end{pmatrix}, \begin{pmatrix} 176 \\ 169 \end{pmatrix}, \begin{pmatrix} 191 \\ 168 \end{pmatrix}, \begin{pmatrix} 174 \\ 167 \end{pmatrix}, \begin{pmatrix} 87 \\ 104 \end{pmatrix}, \begin{pmatrix} 195 \\ 152 \end{pmatrix}, \begin{pmatrix} 182 \\ 167 \end{pmatrix}$, and $\begin{pmatrix} 102 \\ 225 \end{pmatrix}$.

2.2.6. Decrypting Each Plaintext Block One by One

The decryption is done through the following calculation.

$$\boldsymbol{P_1} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_1 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 97 \\ 77 \end{pmatrix}$$

$$\boldsymbol{P_2} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_2 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 116 \\ 101 \end{pmatrix}$$

$$\boldsymbol{P_3} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_3 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 109 \\ 97 \end{pmatrix}$$

$$\boldsymbol{P_4} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_4 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 116 \\ 105 \end{pmatrix}$$

$$\boldsymbol{P_5} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_5 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 107 \\ 97 \end{pmatrix}$$

$$\boldsymbol{P_6} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_6 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 32 \\ 85 \end{pmatrix}$$

$$\boldsymbol{P_7} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_7 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 110 \\ 115 \end{pmatrix}$$

$$\boldsymbol{P_8} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_8 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 111 \\ 101 \end{pmatrix}$$

$$\boldsymbol{P_9} = \left(\left(\frac{1}{2}H_2^{\,T}\right)\left(C_9 - (K \cdot e_2)\right)\right) \bmod 255 = \begin{pmatrix} 100 \\ 32 \end{pmatrix}$$

The plaintext blocks $\boldsymbol{P_1}$, $\boldsymbol{P_2}$, $\boldsymbol{P_3}$, $\boldsymbol{P_4}$, $\boldsymbol{P_5}$, $\boldsymbol{P_6}$, $\boldsymbol{P_7}$, $\boldsymbol{P_8}$, and $\boldsymbol{P_9}$ are obtained, namely

$\begin{pmatrix} 77 \\ 97 \end{pmatrix}, \begin{pmatrix} 116 \\ 101 \end{pmatrix}, \begin{pmatrix} 109 \\ 97 \end{pmatrix}, \begin{pmatrix} 116 \\ 105 \end{pmatrix}, \begin{pmatrix} 107 \\ 97 \end{pmatrix}, \begin{pmatrix} 32 \\ 85 \end{pmatrix}, \begin{pmatrix} 110 \\ 115 \end{pmatrix}, \begin{pmatrix} 111 \\ 101 \end{pmatrix}$, and $\begin{pmatrix} 100 \\ 32 \end{pmatrix}$

respectively.

2.2.7. Converts Each Number in the Matrix to Characters

Each number in $\boldsymbol{P_1}$, $\boldsymbol{P_2}$, $\boldsymbol{P_3}$, $\boldsymbol{P_4}$, $\boldsymbol{P_5}$, $\boldsymbol{P_6}$, $\boldsymbol{P_7}$, $\boldsymbol{P_8}$, and $\boldsymbol{P_9}$ is converted to be characters, so that the plaintext blocks $\boldsymbol{P_1}$, $\boldsymbol{P_2}$, $\boldsymbol{P_3}$, $\boldsymbol{P_4}$, $\boldsymbol{P_5}$, $\boldsymbol{P_6}$, $\boldsymbol{P_7}$, $\boldsymbol{P_8}$, and $\boldsymbol{P_9}$ become

$\begin{pmatrix} M \\ a \end{pmatrix}, \begin{pmatrix} t \\ e \end{pmatrix}, \begin{pmatrix} m \\ a \end{pmatrix}, \begin{pmatrix} t \\ i \end{pmatrix}, \begin{pmatrix} k \\ a \end{pmatrix}, \begin{pmatrix} Space \\ U \end{pmatrix}, \begin{pmatrix} n \\ s \end{pmatrix}, \begin{pmatrix} o \\ e \end{pmatrix}$, and $\begin{pmatrix} d \\ Space \end{pmatrix}$,

respecetively. Thus, the plaintext "**Matematika Unsoed**" is obtained as the result of the decryption of

“ **‰»¬°©¿¨®§WhÃ˜¶§fá**”.

The decryption using Matlab is carried out as shown in **the Figure 2**.

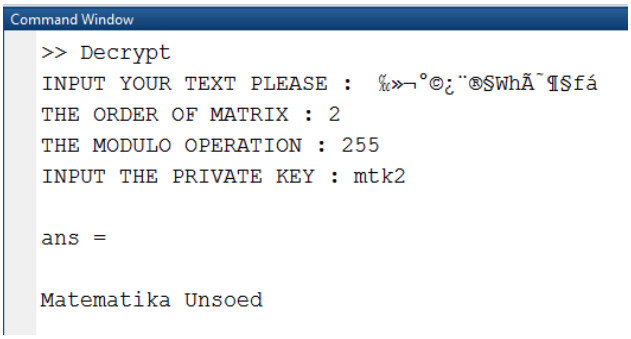

Figure 2 Decryption Process using Matlab

The program instructs to input the decrypted chipertext. Then, by inputting “**‰»¬°©¿¨®§WhÃ˜¶§fá**”, the program is ordered to input the order of the matrix, the private key, the modulo operation, and the Hadamard matrix used. The user input 2 as the order of the matrix, “mtk2” as the private key, and 255 as the modulo operation number. The user also input

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

as the Hadamard matrix used. Then, the program displays “Matematika Unsoed”. Thus, we get the plaintext “Matematika Unsoed” from chipertext “ **‰»¬°©¿¨®§WhÃ˜¶§fá**”.

3. CONCLUSION

The encryption-descryption process of the Hill Chiper algorithm is simpler by using the Hadamard matrix as a public key because of the invertibility of the matrix.

The computation of the encryption-descryption process using the computer program gives the same results as that using manual computation. It means that the computer program gives accurate results.

The computer program can’t compute the empty space that’s symbolized by the ASCII code of 0. In other side, the ASCII code of number 1 – 31 can’t be printed as a character. Thus, for future works, the number of 32 has to be added as a base number for every chipertext or plaintext that’s obtained through the encryption or the decryption process.

AUTHORS’ CONTRIBUTIONS

The first author, SAF CONCEIVED of the presented ideas and DEVELOPED the hadamard matrix and the Hill Chiper theory. SAF also DESIGNED the computational solution of cryptographic problem using Hill Chiper algorithm and performed the computations. The second, MM, and the third author, BHG, VERIFIED the analytical method and ENCOURAGED the first author to investigate the Hadamard matrix role in the encryption and the decryption process. In other side, MM and BHG GUIDED and PROVIDED suggestions for each stage of research. All authors discussed the results and contributed to the final version.

ACKNOWLEDGMENTS

This work was supported by Jenderal Soedirman University through Institutional Research Scheme [grant number : T/458/UN23.18/PT.01.03/2021].

REFERENCES

[1] R. Munir, Cryptography. Bandung: Informatika Bandung, 2019.
[2] K.J. Horadam, Hadamard Matrices and Their Aplication. Princeton: Princeton University Press, 2007.
[3] S.S. Agaian, Hadamard Matrices and Their Aplication. Berlin: Springer, 1985.
[4] J. Steepleton, Construction of Hadamard matrices. *Trace: Tennessee Research and Creative Exchange*, 2019.
[5] S. Kumari, H. Mahato, Encryption based on Conference Matrix. Cornell University: arXiv:1912.10757v1. 1, 2019.
[6] C. Koukovinos, D.E. Simos, Encryption Scheme based on Hadamard Matrices with Circulant Cores. Journal of Applied Mathematics and Bioinformatics. Vol. 3, no. 1, 2013, pp. 17-41.