Keyword Security Implementation Based on Hill Cipher Optimized Using Genetic Algorithms

Mayang Arinda Yudantiar[1]*, Purwanto[2], Sri Winarno[3]
[1,2,3]Informatics Department, Universitas Dian Nuswantoro, Indonesia
[1]mayangarinda1@gmail.com*; [2]mypoenk@gmail.com; [3]sri.winarno@dsn.dinus.ac.id
*corresponding author

ABSTRACT

In the process of exchanging data and information, the most important task is to maintain data and information security and reach out to interested parties. One way this can be achieved is through encryption, a process better known as cryptography. Cryptography can scramble messages so that, even if intercepted, the message cannot be immediately read. One example of an encryption algorithm is the Hill Cipher. The Hill Cipher uses an m-by-m-sized matrix as the key for the encryption and decryption process, making it a challenging algorithm to crack. The key provided for the Hill Cipher encryption and decryption process cannot be arbitrary. The keys with mismatched determinants cannot be used, as they can prevent the encrypted message from being restored to its original form. Optimization can be carried out to overcome these obstacles using a genetic algorithm. Genetic algorithms can determine the keys to encrypt and decrypt the Hill Cipher. A key with the appropriate composition for the Hill Cipher will be obtained through the genetic algorithm's evaluation function. This research aims to enhance message security by using the correct composition to generate Hill Cipher encryption and decryption keys. The research results indicate that out of 10 tests conducted with different lengths of original text, eight succeeded, while two failed to complete the encryption and decryption process.

Keywords: Cryptography, Symmetric Key, Hill Cipher, Matrix Optimization, Genetic Algorithm.

Article History		
Received : Sept, 06th 2023	Accepted : Nov, 16th 2023	Published : Nov, 12th 2023

I. INTRODUCTION

One of the most important parts of an information system is the availability of data and information. So, today's society competes to get as much data and information as possible. This resulted in the flow of information exchange processes between communities to increase. However, it cannot be denied that many dangers arise from exchanging information. For example, the rise of information theft and wiretapping means that information is no longer confidential because it can fall into the hands of unauthorized parties. Once the importance of exchanging information must be accompanied by efforts to maintain information security, one widely used way is to encrypt or encode the information. This method is known as cryptography. According to [1], cryptography is defined as the art or science of maintaining message security, whereas, according to [2], cryptography refers to the science that studies methods related to information security. [3] cryptography is a method for maintaining the confidentiality of messages by converting text into encoded text with a special format whose contents are difficult to understand or even completely incomprehensible. Many cryptographic algorithms, including the Hill Cipher, can be applied to the encryption process. Hill cipher is a symmetrical algorithm classified as a classic algorithm, and hill cipher is a substitution cipher with matrix multiplication [4]. The working process principle of Hill Cipher is to compare plaintext and ciphertext in both negative and positive directions [5]. Encryption is carried out by exchanging the key matrix for a plaintext matrix, and decryption is accomplished by exchanging the inverse key matrix for ciphertext [6]. However, using the Hill Cipher still has a lot of downsides. One of them is giving the key to the matrix for the encryption and decryption process cannot be arbitrary because it will result in the text being unable to be returned to its original form. In general, to avoid key mismatches in Hill Cipher can be done with genetic algorithms.

A genetic algorithm is defined as computer software used to simulate the evolutionary process, where each population produces chromosomes randomly and allows these chromosomes to develop based on the laws of evolution, which are expected to produce better chromosomes [7][8][9]. According to [10], a genetic algorithm is a computational algorithm inspired by evolutionary theory, which is then adopted into a computer algorithm to help complete the search for values or solutions in optimization problems. This optimization problem has been widely applied, especially in securing data or information.

Research topics discussing the implementation of Genetic Algorithms, Hill Cipher, and their combinations have been carried out by several previous researchers, including research conducted by [11], which discusses how to solve the Sudoku game by

implementing genetic algorithms. Furthermore, a study [12] examines using Hill Cipher for the encryption and decryption process using rectangular matrix keys. The research [13] discusses text data security by applying Hill Cipher to Telephone Codes and the Five Modulus Method. The topic of Hill Cipher algorithm hybrid cryptography as the development of symmetric key cryptography [14] discusses how to secure student academic grades using the Hill Cipher hybrid algorithm. The publication [15] wrote about optimizing genetic algorithms for population service affairs using genetic algorithms. Then, a discussion of the genetic algorithm for predicting the time and cost of a construction project [16]. The research [17] discusses the application of genetic algorithms and Hill Cipher for data encoding.

II. METHOD

A. Data Collection Methods

Data collection methods are the methods used by researchers to obtain data to support their research activities. This method is oriented towards data sources obtained through main or supporting methods [18]. The data obtained to support this research comes from secondary data in the form of books, journals, and proceedings that discuss the implementation of the Hill Cipher algorithm and genetic algorithms. Data is obtained from several important documents for testing, which will be attempted to carry out the encryption and decryption process.

B. Hill Cipher Algorithm

In the Hill Cipher algorithm, the encoding process involves using strategies in conjunction with plaintext. In contrast, the decoding process involves inversible text intended for use with cipher text [19]. The symbols for identifiers are in plain and cipher text, each with 29 characters. Each block of plain text is used in the Hill Cipher encryption process. This particular block is identical in size to the key material [20].

Hill cipher, a polyalphabetic cipher, can be categorized as a block cipher because the text to be processed will be divided into blocks of a certain size. According to [21], the Hill Cipher algorithm uses a key as a size m by m matrix to carry out the encryption and decryption process. Several matrix theories proposed by Hill Cipher include multiplication between matrices and inversing matrices [22].

C. Hill Cipher Encryption Technique

The Hill Cipher encryption process Figure 1. The encryption process in Hill Cipher is carried out block by block of plaintext. Each block is the same size as the key matrix. Before dividing the text into rows of blocks, the plaintext is first converted to numbers, for example, A=0, B=1, and Z=25, where the illustration is in Figure 2.

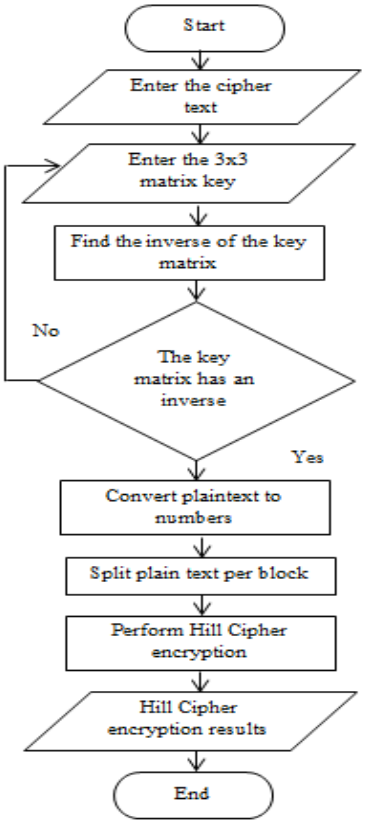

Fig.1. Illustration of Encryption Process

DOI: http://dx.doi.org/10.25139/ijair.v5i2.6907

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fig.2. Number Conversion Table

Mathematically, the encryption process in Hill Cipher is as Equation (1) [23], where the *C* variable is a ciphertext (encoded text), the *K* variable is a key, and the *P* variable is a plaintext (original text).

$$C = K * P \tag{1}$$

To clarify the Hill Cipher encryption process, the following is an example of a case and its solution.

Plaintext: UDINUS

Convert to number: 20 3 8 13 20 18

The keywords presented in matrix form are as $\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}$

The subsequent steps in the encryption process are carried out for each block based on the outcomes of converting the integers and determining the key matrix. These phases are as follows:

UD :

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 3 \end{bmatrix} = \begin{bmatrix} (4*20)+(3*3) \\ (3*20)+(3*3) \end{bmatrix} = \begin{bmatrix} 89 \\ 69 \end{bmatrix}$$

MOD : 89 mod 26=11=L

69 mod 26=17=R

IN :

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} (4*8)+(3*13) \\ (3*8)+(3*13) \end{bmatrix} = \begin{bmatrix} 71 \\ 63 \end{bmatrix}$$

MOD : 71 mod 26=19=T

63 mod 26=11=L

US :

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 18 \end{bmatrix} = \begin{bmatrix} (4*20)+(3*18) \\ (3*20)+(3*18) \end{bmatrix} = \begin{bmatrix} 134 \\ 114 \end{bmatrix}$$

MOD : 134 mod 26=4=E

114 mod 26=10=K

From this process, it is found that the plaintext UDINUS is encrypted to **LRTLEK**

D. Hill Cipher Decryption Technique

The technique of decrypting information using the Hill cipher is exactly the same as the process of encrypting it. However, to proceed, the key matrix needs to be inverted. The flow of the decryption procedure is depicted in Figure 3.

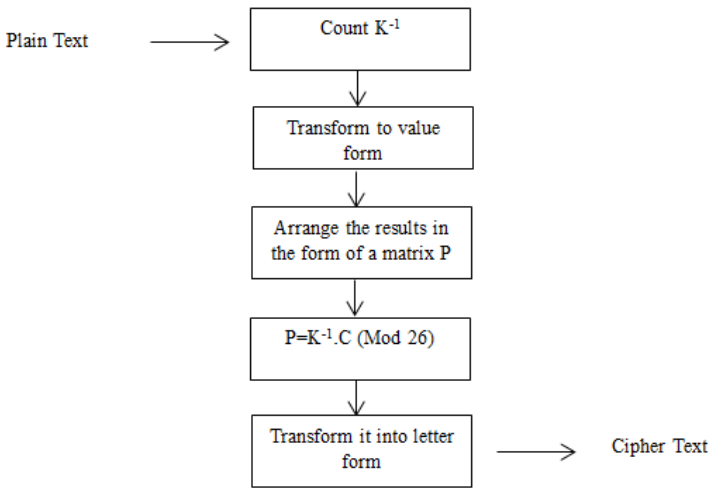

Fig.3. Decryption Process Flow

Mathematically, the decryption process on the Hill cipher can be derived from the Equation [24].

$$P = K^1 * C \ mod \ 26 \quad (2)$$

The following is a list of several examples of instances and possible solutions that have been supplied to make the application of the decryption function in the Hill Cypher more clear:

Cipher Text: **LRTLEK**

Key :

Calculating the determinant using the key yields the following result: determinant K = (4*3) - (3*3) = 3. After obtaining this value, an inverse modulo can be constructed as follows:

3-1 mode 26

= 3X=1 mod 26

=3X=1+26K

=X=(1+26k)/3

Then look for Find k = n so that the result x is an integer

k=0 X=(1+26*0)/3=1/3 (result is not an integer)

k=1 X=(1+26*1)/3=9 (result is an integer).

From these results, the inverse of 3 mod 26 is equivalent to 9 mod 26, which is 9, so the search for the inverse matrix is carried out as:

$$K^{-1} = 9\begin{bmatrix} 3 & -3 \\ -3 & 4 \end{bmatrix} = \begin{pmatrix} 27 & -27 \\ -27 & 36 \end{pmatrix} \text{mod} 26 = \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix}$$

The decryption process per block is carried out below based on the inverse matrix.

LR :

$$\begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 11 \\ 17 \end{bmatrix} = \begin{bmatrix} (1*11) + (25*17) \\ (25*11) + (10*17) \end{bmatrix}$$

$$= \begin{bmatrix} 436 \\ 445 \end{bmatrix}$$

= 436 mod 26 = 20=**U**

= 445 mod 26=3=**D**

TL :

$$\begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 19 \\ 11 \end{bmatrix} = \begin{bmatrix} (1*19) + (25*11) \\ (25*19) + (10*11) \end{bmatrix}$$

$$= \begin{bmatrix} 294 \\ 585 \end{bmatrix}$$

= 294 mod 26 = 8=**I**

= 585 mod 26=13=**N**

EK :

$$\begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 4 \\ 10 \end{bmatrix} = \begin{bmatrix} (1*4) + (25*10) \\ (25*4) + (10*10) \end{bmatrix}$$

$$= \begin{bmatrix} 254 \\ 200 \end{bmatrix}$$

= 254 mod 26 = 20=**U**

= 200 mod 26=18=**S**

The MOD function above is used to find the remainder of the division results, where *X* is the value of the matrix addition result, and *Y* is the length value of the character conversion value with Hill Cipher. The result of the decryption process is plain text: **UDINUS.**

E. Genetic Algorithm

Genetic algorithms utilize various patterns of thought derived from natural evolution to solve a problem [25]. The term "genetic algorithms" can also refer to a strategy for solving optimization issues based on natural selection. This refers to strategies that mirror the progression of biology throughout time [26]. Utilizing the evaluation function with genetic algorithms allows for determining the key required for encryption and decryption in Hill Cypher. At the same time, Hill Cipher is an

algorithm that will execute the key for the encryption and decryption process. In general, the stages of solving using the genetic algorithm are in Figure 4.

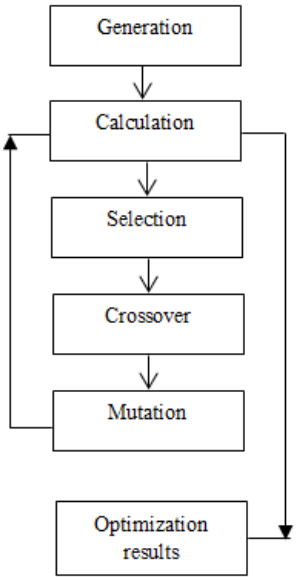

Fig.4. The GA Algorithm Process Flow

III. RESULT AND DISCUSSION

This study aims to analyze how the genetic algorithm optimization process determines the data security key with Hill Cipher.

A. Population Testing

In the Hill Cipher key matrix, there are nine chromosomes. Of these chromosomes, each gene has a value range from 0 to 255, which is of type byte. This value is obtained randomly and placed in each cell in the key matrix.

$$\begin{bmatrix} K_i{}^{10} & K_i{}^{11} & K_i{}^{12} \\ K_i{}^{20} & K_i{}^{21} & K_i{}^{22} \\ K_i{}^{30} & K_i{}^{31} & K_i{}^{32} \end{bmatrix}$$

The information shown up top gives an outline of how chromosomes are constructed using the Hill Cypher matrix key as a starting point. The key, which is in the form of a three-by-three matrix, will be transformed into a one-dimensional vector, and each chromosome will have nine genes.

B. Fitness Value

The fitness value is determined immediately after the current genes are populated with random numbers. The fitness value can be obtained by calculating the determinant. The main provision of this value is $F = 1$, where the determinant of the key matrix must have a value of $D = 1$. Equation (3) calculates the fitness value, where the F variable is the fitness and the D variable is the determinant.

$$F = D \tag{3}$$

C. Testing

The testing procedure is conducted to locate suitable values that are entered into the nine cells comprising the Hill Cypher key matrix. Initialization is the first stage, and its purpose is to establish several parameters that will later serve as initial determinants.

Generation: 30
Population size: 25
Crossover level: 0.8
Mutation level: 0.5

As can be observed from the information above, there are a total of 25 populations. The creation of random values will be repeated 25 times for each population. There will be nine rounds of random generation while the population is maintained. The

number of chromosomes utilized equals the value 9. 225 values will be generated in this initial stage using this value as the starting point. Table I displays the generation results up to this point in the process.

TABLE I
TEST RESULTS OF 25 POPULATIONS

K10	K11	K12	K20	K21	K22	K30	K31	K32
107	84	165	79	69	184	96	183	52
65	86	135	47	224	116	213	112	9
223	37	40	43	5	140	100	215	33
174	195	135	196	220	37	108	144	43
31	232	46	145	120	234	196	242	63
190	54	141	128	118	179	151	108	43
90	64	85	24	242	106	154	178	244
172	124	120	93	193	80	73	183	132
215	82	161	62	103	13	79	165	164
147	47	77	212	45	112	249	18	80
213	7	241	195	245	196	244	25	119
196	92	112	59	55	190	44	191	27
134	29	216	72	198	76	196	7	131
168	214	80	10	104	173	1	114	177
145	20	91	221	73	79	149	137	73
50	89	246	142	168	108	85	116	244
119	141	61	167	254	239	66	77	65
40	187	243	193	58	195	14	154	172
190	168	210	137	178	63	5	146	173
139	26	47	226	179	242	187	137	228
162	80	212	61	102	13	76	163	164
45	178	243	183	57	192	14	145	171
195	90	110	56	55	180	43	190	26
170	123	120	95	193	82	72	181	130
60	85	125	47	223	115	213	112	8

The population formed according to the criteria in Table I is then utilized in several procedures, including the calculation of fitness values, probabilities, and cumulative probabilities. This procedure needs to be carried out to determine how close the population is to the solution that is anticipated to be found. The outcomes of the calculations are presented in Table II.

TABLE II
FITNESS, PROBABILITY, AND CUMULATIVE PROBABILITY CALCULATIONS

F	P	PK
1	0,0002542	0,0003652
59	0,0221674	0,02374
211	0,0765982	0,1003273
228	0,0869248	0,168443
9	0,0032571	0,1906501
76	0,0277775	0,2184076
150	0,0547545	0,2731921
186	0,0644328	0,3421249
203	0,0741417	0,4152666
174	0,06355	0,4878167
241	0,1780205	0,5668371
84	0,0303967	0,5974516
0	0	0,5975164
152	0,055515	0,6530314
172	0,0628196	0,715851
188	0,0686263	0,7843412
223	0,0814463	0,8659606
169	0,0617239	0,9276844
2	0,0007305	0,9284149
196	0,0715851	1
152	0,055515	0,6314530
172	0,0628196	0,785115
188	0, 814463	0,7845142
223	0,0633686	0,8596066
169	0,0361729	0,9842764

From the selection, crossover, and mutation values calculation results, a series of selection, crossover, and mutation processes will be used when the cumulative probability value calculation process is complete. Each of these processes will form the last population that occurs after the changes that occur. The results of the population that has undergone the genetic algorithm process are in Table III.

DOI: http://dx.doi.org/10.25139/ijair.v5i2.6907

TABLE III
TEST RESULTS OF 25 POPULATIONS

K10	K11	K12	K20	K21	K22	K30	K31	K32
134	47	216	112	213	90	18	7	131
84	47	214	192	85	210	223	178	250
119	63	77	78	145	72	249	18	135
108	47	187	177	46	225	120	224	65
167	89	7	143	169	107	199	115	89
78	64	116	24	242	112	27	191	80
80	44	141	7	1	185	62	143	33
254	29	106	196	200	50	13	29	185
31	232	46	145	120	216	143	178	244
139	85	227	226	212	165	168	137	228
218	244	41	166	168	143	112	242	244
222	85	147	214	69	97	131	141	54
147	47	77	61	232	246	249	18	80
215	82	142	101	103	29	79	165	164
187	110	86	59	55	190	44	6	210
31	45	46	134	116	89	196	242	63
65	86	246	196	224	92	66	112	72
77	115	135	246	224	26	213	112	6
116	196	65	77	45	212	25	137	50
139	26	47	226	45	47	187	242	108
123	46	215	121	211	90	18	7	123
85	47	244	195	85	212	244	196	249
167	63	77	78	145	72	249	18	135
108	47	197	108	47	239	200	234	65
119	89	7	142	179	179	119	116	89

This calculation process will continue until the last generation. The last generation is a condition that shows that the population has the most optimal value. Table IV shows The results of forming the three matrix keys.

TABLE IV
GENETIC RESULTS FOR 30 GENERATIONS

K10	K11	K12	K20	K21	K22	K30	K31	K32
246	69	62	147	243	82	29	147	232
147	62	144	232	147	29	82	147	246
82	147	147	69	246	82	230	72	147

D.Testing Hill Cipher Encryption

At this stage, Hill Cipher encryption testing will be carried out where the key used is the result of genetics testing. Table V shows the Hill Cipher encryption key.

TABLE V
THE HILL CIPHER ENCRYPTION KEYS

Encryption		
233	176	238
90	238	211
221	75	67

The plain text "TECHNIC" in its basic form is provided as a test material. The Hill Cypher technique requires the usage of multiples of 9 during both the encryption and decryption processes. The length of the text needs to be altered such that it is equivalent to the previous length as closely as possible. Based on the number of words, TECHNIQUE has a length of six characters, but it still needs an additional three characters to reach its full potential. To adhere to the regulations, the absence of plaintext will have the character "X" substituted for it. The answer to that question is "TEKNIKXXX." The numbers 84, 69, 75, 78, 73, 75, 88, 88, and 88 will be obtained once the plaintext is translated into decimal form. Following the process of determining the decimal value, encryption is performed using the equation encryption = K.P mod 256, which results in the following calculations:

$$= \begin{bmatrix} 233 & 176 & 238 \\ 90 & 238 & 211 \\ 221 & 75 & 67 \end{bmatrix} X \begin{bmatrix} 84 \\ 69 \\ 75 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} (233 \times 84) & (176 \times 69) & (238 \times 75) \\ (90 \times 84) & (238 \times 69) & (211 \times 75) \\ (221 \times 84) & (75 \times 69) & (67 \times 75) \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 19572 + 12144 + 17850 \\ 7560 + 16422 + 15825 \\ 18564 + 5175 + 5025 \end{bmatrix} \text{Mod } 256$$

DOI: http://dx.doi.org/10.25139/ijair.v5i2.6907

$$= \begin{bmatrix} 49.566 \\ 39.807 \\ 28.764 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 158 \\ 127 \\ 92 \end{bmatrix} = \begin{bmatrix} ¥ \\ " \\ \} \end{bmatrix}$$

$$= \begin{bmatrix} 233 & 176 & 238 \\ 90 & 238 & 211 \\ 221 & 75 & 67 \end{bmatrix} X \begin{bmatrix} 78 \\ 73 \\ 75 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} (233 \times 78) & (176 \times 73) & (238 \times 75) \\ (90 \times 78) & (238 \times 73) & (211 \times 75) \\ (221 \times 78) & (75 \times 73) & (67 \times 75) \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 18.174 + 12.848 + 17.850 \\ 7.020 + 17.374 + 15.825 \\ 17.238 + 5.475 + 5.025 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 48.872 \\ 40.219 \\ 27.738 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 232 \\ 27 \\ 90 \end{bmatrix} = \begin{bmatrix} È \\ ë \\ | \end{bmatrix}$$

$$= \begin{bmatrix} 233 & 176 & 238 \\ 90 & 238 & 211 \\ 221 & 75 & 67 \end{bmatrix} X \begin{bmatrix} 88 \\ 88 \\ 88 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} (233 \times 88) & (176 \times 88) & (238 \times 88) \\ (90 \times 88) & (238 \times 88) & (211 \times 88) \\ (221 \times 88) & (75 \times 88) & (67 \times 88) \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 20.504 + 15.488 + 20.944 \\ 7.920 + 20.944 + 18.568 \\ 19.448 + 6.600 + 5.896 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 56.936 \\ 47.432 \\ 31.944 \end{bmatrix} Mod\ 256$$

$$= \begin{bmatrix} 104 \\ 72 \\ 200 \end{bmatrix} = \begin{bmatrix} È \\ h \\ 8 \end{bmatrix}$$

From the entire calculation process, the encryption results are obtained from Plainteks: TEKNIKXXX is "**y¨}Eë|Èh8**"

E. Hill Cipher Decryption Test

In testing the decryption using Hill Cipher in Table VI, the Cipher Text obtained is also converted into decimal numbers. The cipher text that is obtained is: "**y¨}Eë|Èh8**" and when converted into the decimal form, it becomes 84, 69, 75, 78, 73, 75, 88, 88 and 88. The key used is the same as the current key to perform encryption but coupled with the XOR process. Here is the key for the decryption process after XOR is performed.

TABLE VI
THE HILL CIPHER DECRYPTION KEY

Decryption		
121	170	204
153	133	161
232	173	190

The decryption process is carried out in the following stages:

$$= \begin{bmatrix} 121 & 170 & 204 \\ 153 & 133 & 161 \\ 232 & 173 & 90 \end{bmatrix} X \begin{bmatrix} 158 \\ 127 \\ 92 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} (121 \times 158) & (170 \times 127) & (204 \times 92) \\ (153 \times 158) & (133 \times 127) & (161 \times 92) \\ (323 \times 158) & (173 \times 127) & (190 \times 92) \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 19.118 + 21.590 + 18.768 \\ 24.174 + 16.891 + 14.812 \\ 36.656 + 21.971 + 17.480 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 59.476 \\ 55.877 \\ 76.107 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 84 \\ 69 \\ 75 \end{bmatrix}$$

$$= \begin{bmatrix} 121 & 170 & 204 \\ 153 & 133 & 161 \\ 232 & 173 & 90 \end{bmatrix} \text{X} \begin{bmatrix} 232 \\ 27 \\ 90 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} (121 \times 232) & (170 \times 27) & (204 \times 90) \\ (153 \times 232) & (133 \times 27) & (161 \times 90) \\ (323 \times 232) & (173 \times 27) & (190 \times 90) \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 28.072 + 4.590 + 18.360 \\ 35.577 + 3.591 + 14.490 \\ 53.824 + 4.671 + 17.100 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 51.022 \\ 53.577 \\ 75.595 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 78 \\ 73 \\ 75 \end{bmatrix}$$

$$= \begin{bmatrix} 121 & 170 & 204 \\ 153 & 133 & 161 \\ 232 & 173 & 90 \end{bmatrix} \text{X} \begin{bmatrix} 104 \\ 72 \\ 200 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} (121 \times 104) & (170 \times 72) & (204 \times 200) \\ (153 \times 104) & (133 \times 72) & (161 \times 200) \\ (323 \times 104) & (173 \times 72) & (190 \times 200) \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 12.584 + 12.240 + 40.800 \\ 15.912 + 9.576 + 32.200 \\ 24.128 + 12.456 + 38.200 \end{bmatrix} \text{Mod } 256$$

$$= \begin{bmatrix} 65.624 \\ 57.688 \\ 74.584 \end{bmatrix} Mod\ 256 = \begin{bmatrix} 88 \\ 88 \\ 88 \end{bmatrix}$$

Based on the results of the calculation process above, the result is that the decryption process is successful. From plain text, "TEKNIKXXX" be encrypted "**y¨}Eë|Èh8**". After that, the conversion results in decimal numbers are described as 84, 69, 75, 78, 73, 75, 88, 88, and 88.

IV. CONCLUSION

In the Hill Cipher algorithm, which uses a three-by-three matrix, searching for keywords that contain determinants takes a special time and cannot be done manually. The search for the encryption key on the Hill Cipher is carried out by a natural selection process where the best parent will be used to better determine the parameters contained in the genetic algorithm. The use of genetic algorithms helps the encryption and decryption process in Hill Cipher, especially in determining the key. The genetic algorithm will generate a series of numbers quickly and accurately. The population generated from the genetic algorithm can produce several key alternatives that can be used in the Hill Cipher algorithm. It is required to test the Hill Cypher method with long text circumstances to determine its success in the encryption and decryption process. This is done to determine the algorithm's correctness and reliability after the genetic algorithm has been used to optimize it.

REFERENCES

[1] M.M. Amin., "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," Jurnal Pseudocode, vol. III, no. 2, pp. 129–136, 2016.
[2] B.S. Hasugian. , "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah" Jurnal Warta, No 53, 2017, DOI: https://doi.org/10.46576/wdw.v0i53.269, ISSN. 1829 – 7463.
[3] F.N. Pabokory., Astuti, I.F. and Kridalaksana, A.H., "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan Fil Dokumen Menggunakan Algoritma Advanced Encryption Standard", Jurnal Informatika Mulawarman, Vol. 10, No. 1, pp. 20–31, 2015.
[4] S. Yunita, P. Hasan and D. Ariyus., "Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon," Sisfotenika, vol. 9, no. 2, pp. 213–224, 2019.
[5] P. Priyono. , "Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks," J. Ris. Komput., vol. 3, Nomor:, no. Algoritma Caesar Cipher, pp. 351–356, 2016.
[6] R. Wardhani, S.R. Nurshiami and N. Larasati. , "Komputasi Enkripsi Dan Dekripsi Menggunakan Algoritma Hill Cipher," J. Ilm. Mat. dan Pendidik. Mat., vol. 14, no. 1, p. 45, 2022, doi: 10.20884/1.jmp.2022.14.1.5727.
[7] W.A. Puspaningrum, A. Djunaidy and R.A. Vinarti. , "Penjadwalan Mata Kuliah Menggunakan Algoritma Genetika di Jurusan Sistem Informasi ITS," vol. 2, no. 1, pp. 127–131, 2013.

[8] A. Laksono, M. Utami and Y. Sugiarti. , "Sistem Penjadwalan Kuliah Menggunakan Metode Algoritma Genetika (Studi Kasus: Fakultas Kedokteran dan Kesehatan Universitas Muhammadiyah Jakarta)," Stud. Inform. J. Sist. Inf., vol. 9, no. 2, pp. 177–188, 2018.
[9] L. Tambunan., "Implementasi Algoritma Genetika dalam Pembuatan Jadwal Kuliah," Jar. Sist. Inf. Robot., vol. 1, no. 01, pp. 1–7, 2017.
[10] A.P.U. Siahaan., "Algoritma Genetika Untuk Pembentukan Kunci Matriks 3 X 3 Pada Kriptografi Hill Cipher", Seminar Nasional Sains dan Teknologi 2016, Fakultas Teknik Universitas Muhammadiyah Jakarta, p-ISSN : 2407 –1846.
[11] B.V. Indriyono, et al, "Comparative Analysis of the Performance Testing Results of the Backtracking Algorithm and Genetics in Solving Sudoku Games", International Journal of Artificial Intelligence & Robotics (IJAIR), Vol.5, No.1, 2023, pp.29-35, 2023.
[12] A. Hidayat and T. Alawiyah., "Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang", Jurnal Matematika Integratif, Volume 9 No 1, April 2013, pp 39 - 51, 2013.
[13] P. Hasan, S. Yunita, D.Ariyus., "Implementasi Hill Cipher Pada Kode Telepon dan Five Modulus Method dalam Mengamankan Pesan", JURNAL SISFOTENIKA, Vol. 10 No. 1, pp. 12-23,2020.
[14] L.J. Pangaribuan., "Kriptografi Hybrida Agloritma Hill Cipher Dan Rivest Shamir Adleman (Rsa) Sebagai Pengembangan Kriptografi Kunci Simetris (STUDI KASUS : Nilai Mahasiswa AMIK MBP)", Jurnal Teknologi Informasi dan Komunikasi, Vol. 7 No.1, pp. 11 – 26, 2018
[15] S.F. Pane, et all, "Implementasi Algoritma Genetika Untuk Optimalisasi Pelayanan Kependudukan", Jurnal Tekno Insentif, Vol. 13, No. 2, pp. 36-43, 2019.
[16] K. Krisnandi and H. Agung., "Implementasi Algoritma Genetika untuk Memprediksi Waktu dan Biaya Pengerjaan Proyek Konstruksi", JURNAL ILMIAH FIFO, Volume IX,No.2, pp. 90-97, 2017.
[17] M.I. Nahwi., "Penyandian Kunci Dengan Optimasi Menggunakan Algoritma Genetika Pada Kunci Enkripsi Kriptografi Hill Cipher", Jurnal & Penelitian Teknik Informatika, Vol. 1, No. 1, pp. 45-50, 2016.
[18] S. Arikunto, Prosedur Penelitian. Jakarta: Rineka cipta, 2019.
[19] I. Saputri, et all,"Pengamanan Pesan Menggunakan Metode Hill Chiper Dalam Keamanan Informasi", Bulletin of Information Technology (BIT), Vol 3, No 4, pp. 341-349, 2022.
[20] A. Serdano, M. Zarlis, Sawaluddin, and D. Hartama, "Pengamanan Pesan Menggunakan Algoritma Hill Cipher Dalam Keamanan Komputer," J. Mahajana Inf., vol. 4, no. 2, pp. 1–5, 2019.
[21] J.I. Sari., Sulindawaty and H.T. Sihotang., "Implementasi Penyembunyian Pesan Pada Citra Digital dengan Menggabungkan Algoritma Hill Cipher dan Metode Least Significant BIT (LSB)", Jurnal Mantik Penusa, Vol. 1, No. 2,2017.
[22] Forouzan, Behrouz, 2006, Cryptography and Network Security, McGraw-Hill.
[23] Kaharuddin, E. Pawan and D. Ariyus., "Kombinasi Arnold Cat Map dan Modifikasi Hill Cipher Menggunakan Kode Bunyi Beep BIOS PHOENIX", Sisfotenika, vol. 9, no. 2, pp. 159–168, 2019.
[24] M.A. Nasuton, E.V. Haryanto and A. Saleh., "Penerapan Metode Hill Cipher Dan Stream Cipher Dalam Mengamankan Database MySQL", Jurnal FTIK, Vol. 1 No. 1, pp. 532-544, 2020.
[25] L.M.A. Khoirul, W. Wahyu and S. Darma., "Optimasi Penjadwalan Mata Pelajaran Menggunakan Metode Tabu Search (Studi Kasus: SMKN 2 Singosari)", International Clinical Psychopharmacology, Vol. 22, No.6, pp. 338-347, 2017.
[26] T. Kenedy, N. Nur and Wijono. "Optimasi Penempatan Load Break Switch (LBS) pada Penyulang Karpan 2 Ambon menggunakan Metode Algoritma Genetika", Electrical, Electronics, Communications, Controls and Informatics System, Vol. 11, No.2, pp. 1-8,2018.

DOI: http://dx.doi.org/10.25139/ijair.v5i2.6907