P-ISSN : 2715-2448 | E-ISSN : 2715-7199
Vol.1 No.2, 10 July 2020
Buana Information Tchnology and Computer Sciences (BIT and CS)

Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security

Agung Susilo Yuda Irawan [1]
Study Program
Technical Information
Faculty of Computer Science,
Universitas Singaperbangsa Karawang
Email:agung@unsika.ac.id

Nono Heryana [2]
Study Program
System Information
Faculty of Computer Science,
Universitas Singaperbangsa Karawang
Email: nono@unsika.ac.id

Arip Solehudin [3]
Study Program
Technical Information
Faculty of Computer Science,
Universitas Singaperbangsa Karawang
Email: arip.solehudin@staff.unsika.ac.id

Abstract—The progress of communication technology has had a positive impact on human life, including in the field of education. The education office is currently implementing computer-based exams starting from the State Higher Education Entrance Joint Selection (SBMPTN) exam to the School Final Examination. But with the implementation of computer-based exams this is of course the less secure the level, therefore the authors make this research with the aim of securing the exam data that will be tested with Hill cipher cryptography and Caesar cipher. Cryptography is a technique of hiding data that is done to secure data, in this case cryptography aims to secure data on exam questions.

Keywords : Kriptografi, Hill Cipher, Caesar Cipher

Abstrak — Kemajuan teknologi komunikasi telah memberikan dampak positif pada kehidupan manusia, termasuk di bidang pendidikan. Kantor pendidikan saat ini sedang melaksanakan ujian berbasis komputer mulai dari ujian Seleksi Bersama Masuk Perguruan Tinggi Negeri (SBMPTN) hingga Ujian Akhir Sekolah. Tetapi dengan implementasi ujian berbasis komputer ini tentu saja semakin tidak aman levelnya, oleh karena itu penulis membuat penelitian ini dengan tujuan mengamankan data ujian yang akan diuji dengan kriptografi Hill cipher dan cipher Caesar. Kriptografi adalah teknik menyembunyikan data yang dilakukan untuk mengamankan data, dalam hal ini kriptografi bertujuan untuk mengamankan data pada pertanyaan ujian.

Kata kunci: Kriptografi, Hill Cipher, Caesar Cipher

I. INTRODUCTION

Currently technology has developed very rapidly, including in the field of education, an example of application technological development that is on the exam. The education office is currently implementing a computer-based exam starting from the Joint Higher Education Entrance Examination (SBMPTN) exams to the Final School Exams. But with the implementation of computer-based exams, of course the less the level of security, then of The authors make this research with the aim of securing the data on the exam questions to be tested with Hill cipher and Caesar cipher cryptography [1].

It can be interpreted that cryptography is hidden tulidan [2]. There are several algorithms or methods on cryptography includes Hill cipher, Caesar cipher, Vernam Cipher, Advanced Encryption Standard (AES), and so forth.

II. METHOD

The method used in this study is the Caesar Cipher and Hill Cipher method for the process cryptography on data security exam questions, to combine the two methods there are several process that must be done. Figure 2 shows the process carried out.

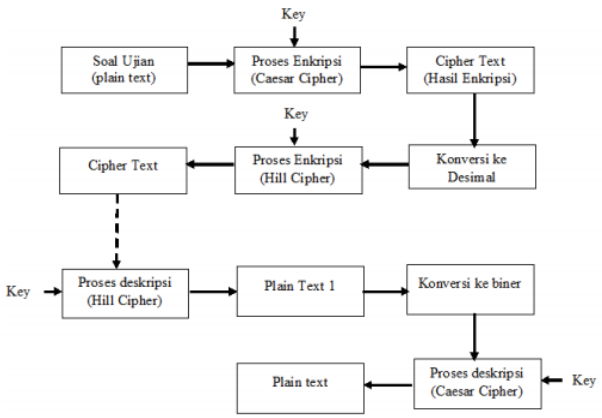

Fig 1 The cryptographic process of Caesar Cipher and Hill Cipher

In Figure 1 can be seen the cryptographic process of Caesar Cipher and Hill Cipher methods. The first process is the problem the test (plain text) is encrypted by the Caesar cipher method and produces Cipher text. Then the cipher text converted to decimal. The result of decimal is re-encrypted using the Hill Cipher method generate Cipher text [3].To process the description or return to the original message with the process carried out it is the opposite of the encryption process, if in the first encryption process with the Caesar Cipher method then on the first description process is the Hill Cipher method [4].

III. RESULTS AND DISCUSSION

The cryptographic process using the Hill Cipher and Caesar Cipher method is done by entering an example Exam

questions to be encrypted and make a key. First the message will be encrypted with using the Caesar Cipher method, then the results are converted to decimal and re-encrypted with the method Hill Cipher with a single process and a key [5].

Examples of exam questions to be encrypted are English exam questions "I am so. I want to eat "with

key (key) = 5. The first stage that will be done is encryption with the Caesar Cipher method. As for the process it is as follows:

Plaintext = I am so . I want to eat

Key = 5

Then change the plaintext and key to binary data, can be seen in Table 1.

TABLE I Conversion from Plaintext to Binary

Plain Text	Biner
I	01001001
a	01100001
m	01101101
s	01110011
o	01101111
.	00101110
I	01001001
w	01110111
a	01100001
n	01101110
t	01110100
t	01110100
o	01101111
e	01100101
a	01100001
t	01110100

Then do the encryption process by shifting the binary number 5 steps to the right, can be seen in Table 2.

TABLE II Encryption Process with Caesar Cipher

Biner	Cipher Text
01001001	01001010
01100001	00001011
01101101	01101011
01110011	10011011
01101111	01111011
00101110	01110001
01001001	01001010
01110111	10111011
01100001	00001011
01101110	01110011
01110100	10100011
01110100	10100011
01101111	01111011
01100101	00101011
01100001	00001011
01110100	10100011

In Table 2 the encryption results obtained by the Caesar Cipher method are still in the form of binary numbers. Then do the conversion to decimal to facilitate the next encryption process.

TABLE III Binary to Decimal Conversion Process

Cipher Text	Decimal
01001010	74
00001011	11
01101011	107
10011011	155
01111011	123
01110001	113
01001010	74
10111011	187
00001011	11
01110011	115
10100011	163
10100011	163
01111011	123
00101011	43
00001011	11
10100011	163

In Table 3 can be seen from the results of the conversion to decimal where the results will be directly encrypted with Hill Cipher method. In the Hill Cipher method, the key used is a matrix in which the matrix is used is 2x2 by using the same key in the encryption process with the method before that is 5 [6] [7].

So that the existing key can be used for the encryption process using the Hill Cipher method, the key will be formed 2x2 matrix by performing a simple calculation process [8].

Key = 5 key k = $\begin{bmatrix} key & key-1 \\ key+1 & key+2 \end{bmatrix}$ k = $\begin{bmatrix} 5 & 5-1 \\ 5+1 & 5+2 \end{bmatrix}$

So from the above calculation results obtained 2x2 matrix key with numbers k = $\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix}$

Next divide the row of decimal numbers in ciphertext2 into a matrix with the number of key matrix columns (key = 2x2).

$\begin{bmatrix} 74 \\ 11 \end{bmatrix}$ $\begin{bmatrix} 107 \\ 155 \end{bmatrix}$ $\begin{bmatrix} 123 \\ 113 \end{bmatrix}$ $\begin{bmatrix} 74 \\ 187 \end{bmatrix}$ $\begin{bmatrix} 11 \\ 115 \end{bmatrix}$ $\begin{bmatrix} 163 \\ 163 \end{bmatrix}$ $\begin{bmatrix} 123 \\ 43 \end{bmatrix}$ $\begin{bmatrix} 11 \\ 163 \end{bmatrix}$

Then do the key matrix multiplication with the matrix that has been made.

$$\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 74 \\ 11 \end{bmatrix} = \begin{bmatrix} 414 \\ 521 \end{bmatrix} \ Mod\ 255 \begin{bmatrix} 159 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 107 \\ 155 \end{bmatrix} = \begin{bmatrix} 1155 \\ 1727 \end{bmatrix} \ Mod\ 255 \begin{bmatrix} 135 \\ 197 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 123 \\ 113 \end{bmatrix} = \begin{bmatrix} 1067 \\ 1529 \end{bmatrix} \ Mod\ 255 \begin{bmatrix} 47 \\ 254 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 4 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 74 \\ 187 \end{bmatrix} = \begin{bmatrix} 1118 \\ 1753 \end{bmatrix} \ Mod\ 255 \begin{bmatrix} 98 \\ 223 \end{bmatrix}$$

$$\begin{bmatrix}5 & 4\\6 & 7\end{bmatrix}\begin{bmatrix}11\\115\end{bmatrix} = \begin{bmatrix}515\\871\end{bmatrix} \; Mod\ 255 \begin{bmatrix}5\\106\end{bmatrix}$$

$$\begin{bmatrix}5 & 4\\6 & 7\end{bmatrix}\begin{bmatrix}163\\163\end{bmatrix} = \begin{bmatrix}1467\\2119\end{bmatrix} \; Mod\ 255 \begin{bmatrix}192\\79\end{bmatrix}$$

$$\begin{bmatrix}5 & 4\\6 & 7\end{bmatrix}\begin{bmatrix}123\\43\end{bmatrix} = \begin{bmatrix}787\\1039\end{bmatrix} \; Mod\ 255 \begin{bmatrix}22\\19\end{bmatrix}$$

$$\begin{bmatrix}5 & 4\\6 & 7\end{bmatrix}\begin{bmatrix}11\\163\end{bmatrix} = \begin{bmatrix}707\\1207\end{bmatrix} \; Mod\ 255 \begin{bmatrix}197\\187\end{bmatrix}$$

In the last process of encryption change the results of this multiplication into the characters that can be seen in table 4.

TABLE IV The Process of Converting Decimal to Character

Decimal	Character
159	Ÿ
11	VT
135	‡
197	Å
47	/
254	þ
98	B
223	ß
5	ENQ
106	J
192	À
79	O
22	SYN
19	DC3
197	Å
187	»

In Table 4 we can see the final ciphertext results from the Caesar Cipher and Hill Cipher method, the ciphertext in the form of ASCII numbers. So, the ciphertext from the example exam questions I am so. I want to eat is Ÿ VT ‡ Å / þ b ß ENQ J À O SYN DC3 Å ».

Furthermore, a description process is carried out to find out whether this method is successful for securing data on the sample exam questions. The first thing that will be done for the description process is the Hill Cipher method by multiplying the inverse key matrix with the ciphertext block matrix.

K = $\begin{bmatrix}5 & 4\\6 & 7\end{bmatrix}$ $detK = (5*7) - (4*6) = 11$

invers modulo:
11-1 mod 255
11x = 1 mod 255
11x = 1+255k
x = (1+255k)/11

Search for k = n with the result that x is an integer.

K = 5; x = (1 + 255 * 5) / 11 = 116 (whole number)

The inverse of 11 mod 255 is equivalent to 116 mod 255 which is 116.

The determinant inverse modulo is used to find the martiks inverse.

K = $\begin{bmatrix}5 & 4\\6 & 7\end{bmatrix}$ then K^{-1} = determinan $\begin{bmatrix}d & -c\\-b & a\end{bmatrix}$

So that

$$K^1 = 116\begin{bmatrix}7 & -4\\-6 & 5\end{bmatrix} = \begin{bmatrix}812 & -464\\-696 & 580\end{bmatrix} mod\ 255 = \begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}$$

Continue multiplying the matrix with ciphertext.

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}159\\11\end{bmatrix} = \begin{bmatrix}797\\11741\end{bmatrix} \; Mod\ 255 \begin{bmatrix}74\\11\end{bmatrix}$$

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}135\\197\end{bmatrix} = \begin{bmatrix}15407\\23105\end{bmatrix} \; Mod\ 255 \begin{bmatrix}107\\197\end{bmatrix}$$

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}47\\254\end{bmatrix} = \begin{bmatrix}13893\\21023\end{bmatrix} \; Mod\ 255 \begin{bmatrix}123\\113\end{bmatrix}$$

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}98\\223\end{bmatrix} = \begin{bmatrix}14864\\22372\end{bmatrix} \; Mod\ 255 \begin{bmatrix}74\\187\end{bmatrix}$$

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}5\\106\end{bmatrix} = \begin{bmatrix}5111\\7765\end{bmatrix} \; Mod\ 255 \begin{bmatrix}11\\115\end{bmatrix}$$

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}192\\79\end{bmatrix} = \begin{bmatrix}12658\\18778\end{bmatrix} \; Mod\ 255 \begin{bmatrix}163\\163\end{bmatrix}$$

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}22\\19\end{bmatrix} = \begin{bmatrix}1908\\2848\end{bmatrix} \; Mod\ 255 \begin{bmatrix}123\\43\end{bmatrix}$$

$$\begin{bmatrix}47 & 46\\69 & 70\end{bmatrix}\begin{bmatrix}197\\187\end{bmatrix} = \begin{bmatrix}17861\\26683\end{bmatrix} \; Mod\ 255 \begin{bmatrix}11\\163\end{bmatrix}$$

After getting the results ,, then do the conversion to binary to proceed to the next process.

TABEL I Proses konversi Desimal ke Biner

Decimal	Biner
74	01001010
11	00001011
107	01101011
155	10011011
123	01111011
113	01110001
74	01001010
187	10111011
11	00001011
115	01110011
163	10100011
163	10100011
123	01111011
43	00101011
11	00001011
163	10100011

These binary numbers are then re-encrypted for the last time using the Caesar cipher method by shifting 5 times to the left, with the results that can be seen in Table 6.

TABLE VI The process of converting Decimal to Binary

Biner	Cipher Text	Plain Text
01001010	01001001	I
00001011	01100001	a
01101011	01101101	m
10011011	01110011	s
01111011	01101111	o
01110001	00101110	.
01001010	01001001	I
10111011	01110111	w
00001011	01100001	a
01110011	01101110	n
10100011	01110100	t
10100011	01110100	t
01111011	01101111	o
00101011	01100101	e
00001011	01100001	a
10100011	01110100	t

In table 5 it can be seen that the results of the description that have been done produce a Plaintext "Iamso.Iwanttoeat" in accordance with the example of the exam questions used for this study, with this the merging of the Hill Cipher and Caesar Cipher methods has been completed.

IV. CONCLUSION

From the results of the research that has been carried out it can be concluded that the Hill Cipher and Caesar Cipher methods can be combined for the process of securing data with a good level of security, this method is also easily understood and for the encryption and description process using only one key so that it is easy to remember.

REFERENCES

[1] R. Kaur, "Rectangular Matrix with Left Inverse For Variation in Hill Cipher: Communication Safe Guard," *J. Gujarat Res. Soc.*, vol. 21, no. 8, pp. 1234–1240, 2019.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv Prepr. arXiv2003.06557*, 2020.

[3] C. Rajvir, S. Satapathy, S. Rajkumar, and L. Ramanathan, "Image Encryption Using Modified Elliptic Curve Cryptography and Hill Cipher," in *Smart Intelligent Computing and Applications*, Springer, 2020, pp. 675–683.

[4] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher," *arXiv Prepr. arXiv2003.11936*, 2020.

[5] I. Irmayani, "Application of Matrix in Hill Cipher Algorithm," in *International Conference on Natural and Social Sciences (ICONSS) Proceeding Series*, 2019, pp. 141–147.

[6] P. E. Coggins III and T. Glatzer, "An Algorithm for a Matrix-Based Enigma Encoder from a Variation of the Hill Cipher as an Application of 2× 2 Matrices," *PRIMUS*, vol. 30, no. 1, pp. 1–18, 2020.

[7] D. Kurniawan and B. Priyatna, "Pengamanan Data Berbasis Mobile Android Dengan Penggabungan Linear Feedback Shift Register (Lfsr) Dan Modifikasi Matriks Kunci Algoritma Kriptografi Playfair Cipher," *J. Telemat. MKOM Vol*, vol. 10, no. 1, 2018.

[8] A. Behera, A. Tripathy, A. R. Tripathy, and S. Rath, "Random Invertible Key Matrix Decomposition for Classical Cryptography," in *Advanced Computing and Intelligent Engineering*, Springer, 2020, pp. 553–563.

[9] S. Kromodimoeljo, Teori dan Aplikasi Kriptografi, Jakarta: SPK IT Consulting, 2010.

[10] M. Khoerudin, "Algoritma Hill Cipher (Sandi Hill),"Materi Perkuliahan Pada Jurusan Teknik Informatika), 22 Maret 2015.

[11] Sholeh, "Algoritma Subtitusi Menggunakan Chaesar Cipher," Caesar Cipher Dan Cipher Key, 3 Oktober 2011.

[12] K. W. M. R. Puspita, "Analisis Kombinasi Metode Caesar Cipher , Vernam Cipher , Dan Hill Cipher Dalam Proses Kriptografi," Seminar Nasional Teknologi Informasi dan Multimedia 2015, pp. 43-48, 2015.

[13] K. Aulia, "Soal Ujian Sekolah (US) Bahasa Inggris Kelas 6 SD/MI Tahun Ajaran 2017/2018," Juragan Les, 2018.

[14] Irawan, A. S. Y., El Ramdhani, A. F., Jordi, M., Mahdi, R. S., & Al Mudzakir, T. (2020). Implementasi Algoritma Advanced Encryption Standard (AES) untuk mengamankan File Video. *SYSTEMATICS*, *2*(1), 28-32.

[15] Hananto, A. L., Solehudin, A., Irawan, A. S. Y., & Priyatna, B. (2019). Analyzing the Kasiski Method Against Vigenere Cipher. *arXiv preprint arXiv:1912.04519*.