BIS INFORMATION TECHNOLOGY AND COMPUTER SCIENCE

Volume 1 2024 | DOI: 10.31603/bistyc.114
5th Borobudur International Symposium on Science and Technology (BIS-STE) 2023

UNIMMA PRESS
UNIVERSITAS MUHAMMADIYAH MAGELANG

Development of an encryption algorithm based on the Caesar Cipher algorithm

K B Utomo[1*], A R Hakim[1] and B Cahyono[1]

[1] Politeknik Negeri Samarinda, Samarinda, Indonesia
[*]Corresponding author email: kbu@polnes.ac.id

Abstract

The problem in securing data is still an important aspect in maintaining data storage, especially data stored in digital form. This causes due to very rapid progress in the field of computers with the concept of an open system that has been widely used, so this can make it easier for someone to do data destruction that requires data stored in digital. This security usually uses encryption. Encryption is the process of communicating information by making that information unreadable without the help of special knowledge. So that encrypted data can be read, the decryption process is needed. The decryption process is used so that the message can be read again by the intended party. One of the algorithms to carry out the encryption and decryption process is the Caesar cipher algorithm, which algorithm is one of the most widely studied. However, the Caesar cipher algorithm has a disadvantage including all letters can be covered, do not recognize lowercase or uppercase letters. It is necessary for the development of the Caesar cipher. The purpose of this research is to develop an encryption algorithm based on the caesar cipher algorithm. A result of this research is a development of a Caesar cipher algorithm that includes more characters, namely A-Z, a-z, 0-9, and comma and space characters. In this study also used a change of 3 characters vertically (below).

Keywords

Encryption algorithm, Caesar cipher algorithm, Data security

Introduction

Data security still is aspect important in guarding data storage, especially stored data in digital form. This matter caused Because very rapid progress in the field knowledge computer with draft open- system already Lots used, so matter this can makes it easier somebody for do destruction of data, especially stored data in digital form without must know to the party's data storage.

Cryptography is studies security (confidentiality) of posts. In the cryptography there is an encryption and decryption process [1]. Encryption in a way explicit can interpreted as a process for change message (information) so no can see without use key opener confidential. Technology this already used for a long time among people military and

Published:
October 20, 2024

Selection and Peer-review under the responsibility of the 5th BIS-STE 2023 Committee

intelligence. Nowadays, technology encryption with a number of modifications already applied for interest general, deep digital activities such as keep important data confidential owned by individual nor company [2]. Decryption is a process of change return disguised form the become information beginning [3]. Cryptography is base for understand security on computers. As for the encryption and description process, Caesar uses the method shift operations. Ways of working shift operation is with method substitute the letters of the alphabet next to each other left or adjacent right the letter [3–5]. Algorithm cryptography (cipher) is something function mathematics used for do encryption and decryption. There are two kinds algorithm cryptography, that is algorithm symmetric (symmetric algorithms) and algorithms asymmetric (asymmetric algorithms) [3][6] as for the encryption process and description cryptography can be found in Figure 1 [7][8].

Encryption is very important thing in cryptography as security of the data sent so that it is kept confidential awake. Message the original called changed plaintext become codes that don't understandable. Message encrypted called ciphertext. There are four objectives fundamental in encryption like confidentiality, data integrity, authentication, and non- repudiation.

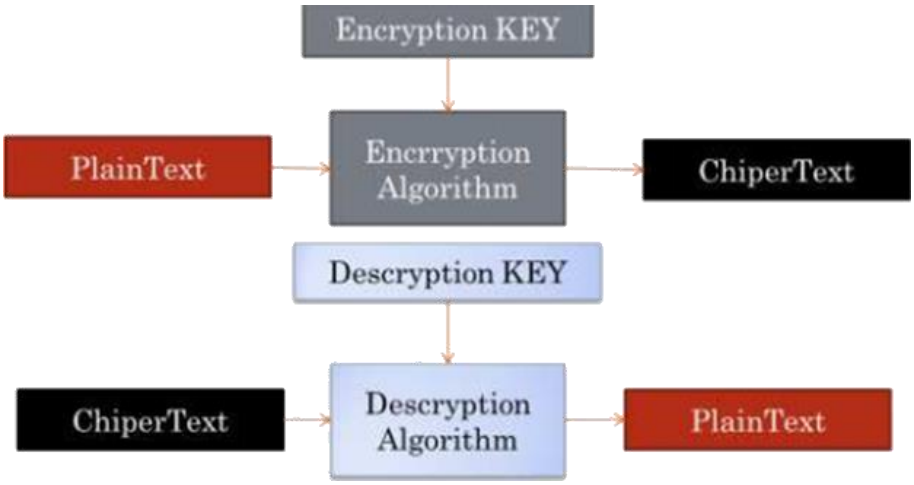

Figure 1. Encryption and decryption process cryptography

Caesar cipher is one of them algorithm oldest and is one of the types of substitution cipher that forms a cipher with method do shift to all characters in plaintext with mark the same shift [7][9]. a number of algorithm cryptography classic that has been lots is known in a way wide own possible weaknesses _ known and solved [7]. Weakness Caesar cipher is No all letter can cover, no know letter small nor letter capital. so that necessary something development of the Caesar cipher.

Method

Algorithm Cryptography Classic

Basically, algorithms cryptography classic can grouped to in two types of ciphers, namely: [10]

1. Substitution Cipher

In a substitution cipher each plaintext unit replaced with one ciphertext unit. One "unit" here means one letters, pairs letters, or grouped more of two letters. In the Caesar Cipher, each letter substituted with letter third next from arrangement the same alphabet. In terms of This the key is amount shift letter that is three. Arrangement alphabet after shifted so far three letter forming A table substitution like shown in Figure 2.

Figure 2. Caesar cipher substitution

2. Transposition Cipher

In a transposition cipher, the letters are inside plaintext still just, just just the order changed. In other words, algorithm This transpose to suite character inside text. Another name for method this is permutation or randomization (scrambling) due to each transpose character inside text The same with mutate the characters.

Algorithm Caesar Cipher

Algorithm Caesar cipher is algorithm substitutions that use draft shift letter with modulo 26. By mathematical can formulated as here S=(T+K) Modulo 26. S= Cipher Text, T= Close Text, K= Key. Algorithm This usually used for the encryption process something nature information special or secret in Roman times. Every letter substituted become letters that shift 3 existing letters in plaintext, in other words shifted by 3 letters after letter the original. For example, letters t=w, h=k, and e=h. In the alphabet letters third after the 't' is the 'w', the letter third after 'h' is 'k', as well letter third after 'e' is 'h' and so on, Steps the encryption [7]:

1. Input the plaintext characters it consists of 26 characters letter
2. Determine magnitude value (Key) which is mark shift character for forming plaintext become ciphertext
3. Arrange row characters in the Caesar cipher based on key (dimensional One)
4. Exchange character to right side of the plaintext become ciphertext with based on the value (key) that has been shifted determined previously.

In the decryption process is the opposite of the encryption process this will convert ciphertext to plaintext with use the same key with shift to the left. Following is rules for do decryption of the algorithm Caesar cipher [7]:

1. Input character ciphertext
2. Determine magnitude value (Key) which is mark shift character For forming Ciphertext becomes Plaintext, value (key) must be the same with value (key) when done encryption
3. Arrange row character ciphertext in the Caesar cipher based on key (dimensional One)

4. Exchange character to the left direction of the ciphertext become plaintext with based on the value (key) that has been shifted determined previously.

Results and Discussion

Based on analysis from series test encryption and decryption as well as pay close attention a number of literatures, then can found a number of sufficient weaknesses / shortcomings fundamental from the Caesar cipher, namely:

1. Amount Limited characters (26 characters) so no possible plaintext consists from diverse characters
2. Decryption process ciphertext become plaintext easily done vecause key is mark shift

Caesar Cipher Version Development

For answer from a number of the shortcomings that exist in the Caesar cipher then need done development with still based on the Caesar cipher algorithm, some development carried out is:

1. Uses two dimensions (8 x 8) for total characters totaling 64 characters
2. Character consists from A – Z, a – z, 0 – 9, commas and spaces
3. Key can more of 1 character, consists from between A - Z characters, a - z, 0 - 9, chars spaces and commas without there is repetition character
4. Shift value done in a way dynamic
5. Shift done vertically

Following are the steps encryption and decryption, Encryption Steps:

1. Enter key (can consists from between A-Z characters, a-z, 0-9, chars' spaces and commas without There is repetition character)
2. Enter the remainder remaining characters with no do repetition characters who have mentioned in character key
3. Input mark shift For exchange mark from plaintext become ciphertext
4. Encryption done with method shift with amount mark shift as entered in step previously done in a way vertical (down). In the case of If mark the shift is 3
   a. If position character is on row 1 then character results encryption is character on the 4th row in the same column, the will applies the same for characters in positions from line 1 to line 5
   b. If position character is on row 6 then character results encryption is character on the 1st row in the same column, the will applies the same for characters on 2 row positions final
5. If one character in plaintext no found, then no will encrypted or still the same with original character.

Decryption Steps:

1. Enter key (can consists from between A-Z characters, a-z, 0-9, chars' spaces and commas without There is repetition character)

2. Enter the remainder remaining characters with no do repetition characters who have mentioned in character key
3. Input mark shift exchange mark from ciphertext become plaintext
4. Decryption done with method shift with amount mark shift as entered in step previously done in a way vertical (to the top). In the case of If mark the shift is 3
   a. If position character is on row 1 then character results decryption is character on the 6th row in the same column, the will applies the same for characters in positions from line 1 to line 3
   b. If position character is on the 4th row, then character results encryption is character on the 1st row in the same column, the will applies the same for characters in row positions 4 to 6
5. If one character in plaintext no found, then no will encrypted or still the same with original character.

Implementation

1. Caesar Cipher (original)

Encryption and decryption process in the algorithm Caesar Cipher begins with determine amount value (key) shift, where in the thesis this is the data used is as following:

Plaintext : ZEBRA

Shift Value (Key) : 3

a. Encryption started from letter first on plaintext that is letter "Z", encryption process presented in Figure 3.

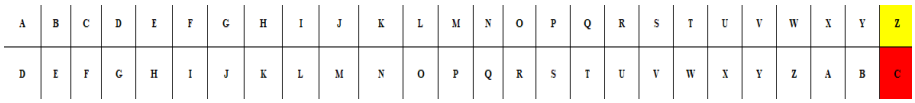

Figure 3. Encryption process the letter "Z" becomes letter "C"

Shift process done to right, and because the letter "Z" is letter final so shift will start from the letter "A" and because mark the shift is 3 then the letter "Z" is encrypted become letter "C."

b. Next step is do encryption the letter "E" becomes the letter "H" as shown in Figure 4.

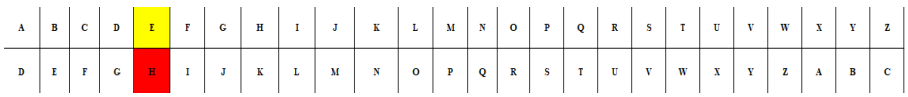

Figure 4. Encryption process the letter "E" becomes letter "H"

c. next process is do encryption the letter "B" becomes the letter "E" as shown in Figure 5.

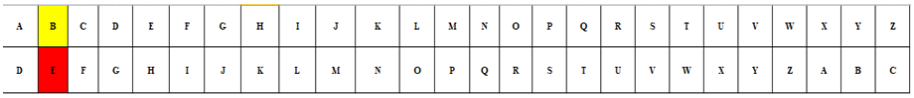

Figure 5. Encryption process the letter "B" becomes letter "E"

d. next process is do encryption the letter "R" becomes the letter "U" as shown in Figure 6.

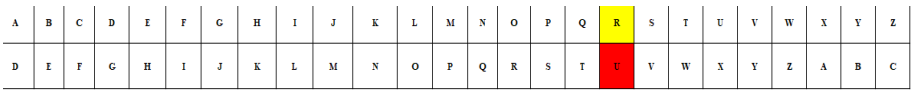

Figure 6. Encryption process the letter "R" becomes letter "U"

e. Final process is do encryption the letter "A" becomes the letter "D" as shown in Figure 7.

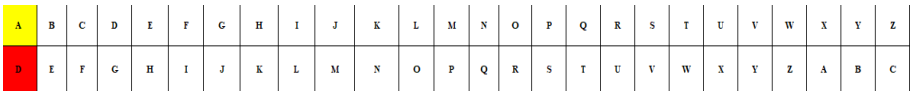

Figure 7. Encryption process the letter "A" becomes letter "D"

With thereby results end of the encryption process from plaintext "ZEBRA" to ciphertext "CHEUD." Steps in the decryption process done almost the same with the encryption process, only just entered character is ciphertext characteristics for changed into plaintext and value shift (key) must be the same with mark shift moment done encryption.

2. Caesar cipher version development

Based on algorithms Caesar cipher, under development algorithm Caesar cipher version developer at this point, the encryption and decryption process in the Caesar Cipher algorithm begins with do expansion key, where the data is used is as following:

Key : "Tenda Merah"

Shift Value : 3

Plaintext : "Zebra"

T	e	n	d	a		M	r
h	A	B	C	D	E	F	G
H	I	J	K	L	N	O	P
Q	R	S	U	V	W	X	Y
Z	b	c	f	g	i	j	k
l	m	o	p	q	s	t	u
v	w	x	y	z	0	1	2
3	4	5	6	7	8	9	,

Figure 8. Caesar Cipher Version Key Expansion Development

First process to be carried out is with input key to in the matrix with No do repetition characters who have mentioned in the characters previous (Figure 8) and next enter character others (A – Z, a – z, 0 – 9, space, comma) with No do repetition characters who have mentioned in character key. Furthermore, the encryption process started

from character first on plaintext that is letter "Z." As presented in Figure 9, for do encryption the "Z" character is performed exchange character with method do exchange vertically to bottom, quantity mark shift determined from initial work done in a way dynamic, and based on the initial scenario that mark the shift is 3 then encrypted "Z" character become character "3".

T	e	n	d	a		M	r
h	A	B	C	D	E	F	G
H	I	J	K	L	N	O	P
Q	R	S	U	V	W	X	Y
Z	b	c	f	g	i	j	k
l	m	o	p	q	s	t	u
v	w	x	y	z	0	1	2
3	4	5	6	7	8	9	,

Figure 9. Encryption process the character "Z" becomes character "3"

a. Next process with do encryption character second that is the character "e" becomes character "R", as shown in Figure 10.

T	e	n	d	a		M	r
h	A	B	C	D	E	F	G
H	I	J	K	L	N	O	P
Q	R	S	U	V	W	X	Y
Z	b	c	f	g	i	j	k
l	m	o	p	q	s	t	u
v	w	x	y	z	0	1	2
3	4	5	6	7	8	9	,

Figure 10. Encryption process the character "e" becomes "R" character

b. Next is the encryption process character second that is the character "b" becomes character "4", as shown in Figure 11.

T	e	n	d	a		M	r
h	A	B	C	D	E	F	G
H	I	J	K	L	N	O	P
Q	R	S	U	V	W	X	Y
Z	b	c	f	g	i	j	k
l	m	o	p	q	s	t	u
v	w	x	y	z	0	1	2
3	4	5	6	7	8	9	,

Figure 11. Encryption process the character "b" becomes character "4"

c. Then the encryption process character second that is the character "r" becomes character "Y", as shown in Figure 12.

T	e	n	d	a		M	r
h	A	B	C	D	E	F	G
H	I	J	K	L	N	O	P
Q	R	S	U	V	W	X	Y
Z	b	c	f	g	i	j	k
l	m	o	p	q	s	t	u
v	w	x	y	z	0	1	2
3	4	5	6	7	8	9	,

Figure 12. Encryption process the character "r" becomes character "Y"

d. Finally, the process encryption character second that is the character "a" becomes character "V", as shown in Figure 13.

T	e	n	d	a		M	r
h	A	B	C	D	E	F	G
H	I	J	K	L	N	O	P
Q	R	S	U	V	W	X	Y
Z	b	c	f	g	i	j	k
l	m	o	p	q	s	t	u
v	w	x	y	z	0	1	2
3	4	5	6	7	8	9	,

Figure 13. Encryption process the character "a" becomes character "V"

From the series of processes above so obtained results encryption from plaintext "Zebra" to ciphertext "3R4YV". Based on results encryption the can obtained inclined ciphertext characters various (no only One type character) and the will more difficult If done decryption by an unauthorized party interested.

Basically, the decryption process no far different with the encryption process. only decryption is the opposite from encryption. And the data will be decrypted is ciphertext. Decryption process using keys and values the same shift with at the moment encryption, however direction the shift to the top.

Conclusion

Characters and encryption results (ciphertext) version original only know One type character (A - Z or a - z) whereas in the Caesar Cipher version of the Algorithm development more various (a – z, A – Z, 0 – 9, commas and spaces) so more lots accommodate lots character. Key use in the Caesar Cipher version original functioned as mark shift while in the Caesar Cipher version development functioned as keywords for maximizing results encryption as well as mark the shift is also determined in a way dynamic. Shift direction characters in the Caesar Cipher version original is horizontal (right / left) and in the Caesar Cipher version development is vertical (bottom / top). Encryption results or the ciphertext Caesar Cipher Algorithm version development more

difficult decrypted remember various ciphertext characters (a – z, A – Z, 0 – 9, comma and space) and using key as well mark the shift done in a way dynamic.

References

[1] A. Pradipta and S. A. Yogyakarta, "Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi," *ijns.org Indonesian Journal on Networking and Security*, vol. 5, p. 3, 2016.

[2] A. Kurnia, A., and M. A. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Batik Ceplok Yogyakarta," vol. 8, no. 1, 2019.

[3] M. Nurtanzis Sutoyo, "Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data," vol. 2, no. 1, 2016.

[4] R. Febrianingsih and A. Hafiz, "Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data."

[5] A. Anto Tri Susilo, "Penerapan Algoritma Asimetris RSA Untuk Keamanan Data Pada Aplikasi Penjualan CV. Sinergi Computer Lubuklinggau Berbasis Web," Jurnal SIMETRIS, vol. 9, no. 2, 2018.

[6] B. Schneier, Applied cryptography : protocols, algorithms, and source code in C. Wiley, 1996.

[7] M. Algoritma Caesar Cipher, H. Dwi Purnomo, and I. Sembiring, "Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks," JIFOTECH (Journal of Information Technology), vol. 2, no. 1, 2022.

[8] F. Maqsood, M. Ahmed, M. Mumtaz Ali, and M. Ali Shah, "Cryptography: A Comparative Analysis for Modern Techniques," 2017. [Online]. Available: www.ijacsa.thesai.org

[9] S. Godara, S. Kundu, and R. Kaler, "An Improved Algorithmic Implementation of Rail Fence Cipher," International Journal of Future Generation Communication and Networking, vol. 11, no. 2, pp. 23–32, Mar. 2018, doi: 10.14257/ijfgcn.2018.11.2.03.

[10] T. Zebua and S. Limun, "Analisa Dan Implementasi Algoritma Triangle Chain Pada Penyandian Record Database," Pelita Informatika Budi Darma, vol. III, no. 2 , 2013.