PROC. INTERNAT. CONF. SCI. ENGIN.
Volume 3, April 2020 | Pages: 741-744

ISSN 2597-5250
E-ISSN 2598-232X

Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message

Septi Yana Wulandari
Postgraduate Program of Mathematics Education, Yogyakarta State University
Jl. Colombo No 1, Karangmalang, Depok, Sleman, Yogyakarta, Indonesia.
Email: septiyanawulandari94.@gmail.com

Abstract. Advances in technology make it easy for humans to communicate with each other. One of them is by sending messages. However, the confidentiality of messages can be hacked by third parties. Therefore, it is necessary to secure the messages sent so that confidentiality can be maintained. One way that can be done to maintain message security is cryptography. Classical cryptography has several types of algorithms including caesar cipher and affine cipher. The purpose of this study is to combine caesar cipher and affine cipher as one technique that can be used to secure messages. This combination is done by changing the plaintext into ciphertext 1 through caesar encryption. Ciphertext 1 is encrypted by affine caesar to produce ciphertext 2. Ciphertext 2 is the message to be sent. Then to change to original message ciphertext 2 is decrypted by affine chiper so that it gets plaintext 1. Then plaintext 1 is decrypted by caesar chiper so that it gets plaintext 2. Plaintext 2 is the message that should be received. The result of this study are a combination of caesar cipher and affine cipher can secure a message sent.

Keywords: Cryptography, Caesar cipher, Affine cipher

INTRODUCTION

Advances in technology, make it easier for humans to communicate with each other. One form of communication that can be done is by long distance messaging. Sending messages can be done via SMS (short message service), e-mail, whatsapp and more. The message sent can be confidential or not confidential. Messages that are not confidential are fine if the message is hacked by a third party. However, confidential messages will be dangerous if hacked by irresponsible parties. Therefore, we need a program to conceal the message.

Discipline aimed at the confidentiality system is called cryptology (Rosen, 2011). One part of cryptology is cryptography. Cryptography is the science and art of maintaining message security (Schneier, 1996). Cryptography is also referred to as scientific studies or techniques to secure digital information, transactions, and distributed computing (Sundarayya P, et al. 2016). So cryptography is a system that can be used to secure information or messages. There are two types of cryptography, namely classical and modern cryptography. For discussion in this paper, more emphasis will be placed on classical cryptography. Previously, in cryptology there were a number of terms that needed to be understood, as shown in table 1 (Rosen, 2011).

Classical cryptography has two basic components of classical cipher: substitution and transposition (Kromodimoeljo, 2010). In substitution cipher letters are replaced by other letters and in transposition cipher the letters are arranged in a different order. Some classical cryptography that can be used to conceal messages is a cesar and affine cipher. The Caesar Cipher is the world's first encoding cipher that was discovered in 1970 by Julius Caesar. Affine cipher is an extension of the caesar cipher. Affine cipher is a cryptographic technique that exchanges monoalphabetic characters. In affine cipher, every character in plaintext will be exchanged with new characters based on the formula used (Babu, 2017). The cipher uses keys in the form of prime numbers in the encryption and decryption process (Sudarayya, 2016).

Tabel 1. A term in cryptology.

Term	Description
Plaintext	A message that is to be altered into a secret form
Ciphertext	A message that has been transformed into a secret form
Encryption	A procedure method for altering a plaintext message into ciphertext by changing the letters of the plaintext using a transformation
Decryption	The reverse process of changing the ciphertext back to the plaintext by the intended receiver

The weakness of the caesar cipher is that the ciphertext results of the transformation are easily solved through the Brute Force method and the percentage of letter frequencies most often appear (Rachmawati and Candra, 2017). Brute Force is a form of attack that dabbles at the possibilities for each key. Therefore, to better maintain the confidentiality of messages, it can combine Caesar ciphers with other types of ciphers. One of them is affine cipher. Affine cipher has advantages that can cover the weakness of caesar cipher. The

advantage is that affine cipher has three different keys in doing encryption, decryption and shift key (Siahaan, 2018). That thing, makes affine cipher more difficult to solve compared to caesar cipher which only has one key.

MATERIALS AND METHODS

Chaesar and Affine Cipher

The cesarean section and affine cipher in concealing messages begin by converting the message into ASCII code. Examples of converting the messages into ASCII code, as shown in table 2.

Tabel 2. Message transformation to code ASCII.

Character	Unicode (Heksadesimal)	ANSI ASCII (Decimal)	Description
SP	20	32	Spacing
!	21	33	exclamation mark (exclamation)
“	22	34	Double quotes
#	23	35	Hash tag (kres)
A	41	65	Latin capital letter A
B	42	66	Latin capital letter B
C	43	67	Latin capital letter C

The combination of cesarean cipher and affine cipher is done by doing encryption and decryption in sequence using both ciphers. So that the plaintext is encrypted with a cesarean cipher will produce a ciphertext 1. Ciphertext 1 is located as a plaintext that is encrypted with an affine cipher so as to produce ciphertext 2. Then for the decryption process, ciphertext 2 is decrypted so that it becomes plaintext. The Plaintext is located as ciphertext 1 which is decrypted so that it becomes a plaintext.

Caesar cipher is part of a cipher called shift transformation. In cesarean cipher to produce encryption that is transforming from plaintext (P) to produce ciphertext (C) can be expressed through the following congruent functions:

$$C \equiv P + k \mod 256, 0 \leq P \leq 255$$

Where k is the number of ASCII code shifts desired. to decrypt it in a cesarean cipher, it is done by transforming from ciphertext (C) to produce a plaintext (P) can be expressed through the following congruent functions:

$$P \equiv C - k \mod 256, 0 \leq P \leq 255$$

The steps to encrypt the cesarean cipher are:

1. Change the message character in the plaintext to ASCII code
2. Determine the value of *k*, then use the transformation $C \equiv P + k \mod 256, 0 \leq P \leq 255$
3. Change the code obtained in step 2 into the message character
4. The result in step 3 is the ciphertext message

The steps to decrypt a cesarean cipher are:

1. Change the message character in the ciphertext to ASCII code
2. Determine the value of *k*, then use the transformation $P \equiv C - k \mod 256, 0 \leq P \leq 255$
3. Change the number obtained in step 2 to the message character
4. The results in step 3 are plaintext messages

Affine cipher is an extension of cesarean cipher. In affine cipher to produce encryption that is transforming from plaintext (P) to produce ciphertext (C) can be expressed through the following congruent functions:

$$C \equiv \big((a \times P) + b\big) \mod 256, 0 \leq P \leq 255$$

Where a and b are integers. b is the number of desired alphabet shifts. a must be relatively prime with 256 or $(a, 256) = 1$ for congruence to be expressed in its inverse [1, 10]. Based on the explanation of the relationship between ciphertext (C) and plaintext (P), then to get the plaintext (P) is the inverse of ciphertext (C). Plaintext (P) can be expressed in the following congruent functions:

$$P \equiv \big(\bar{a}(C - b)\big) \mod 256, 0 \leq C \leq 255$$

Where $\bar{a}$ is the inverse of $a \pmod{26}$. $\bar{a}$ can be searched using congruence $\bar{a} \equiv a^{\emptyset(256)-1} \pmod{256}$. Or you can use the definition (Rosen, 2011) that *“given an integer a with* $(a, m) = 1$, *an integer solution x* of $ax \equiv 1\ (mod\ m)$ *is called an inverse of a modulo m.”*

The steps to encrypt the affine cipher are:

1. Change the message character to ASCII code
2. Determine the values of a and k, then use the transformation $C \equiv \big((a \times P) + k\big) \mod 256, 0 \leq P \leq 255$
3. Change the code obtained in step b into the message character
4. The results in step c are the chiphertext message

The steps to decrypt the affine cipher are:

1. Change the message character to ASCII code
2. Determine the values of $\bar{a}$ and k, then use the transformation $P \equiv \big(\bar{a}(C - k)\big) \mod 256, 0 \leq C \leq 255$
3. Change the code obtained in step b into the message character
4. The results in step c are plaintext messages

Encryption

The plaintext message that will be sent SAYA KULIAH

Encryption is done by a combination of caesar and affine cipher

The key used is $k = 8, a = 9$.
$\bar{a} = \bar{9} \equiv 9^{\emptyset(256)-1} (\text{mod } 256) = 57 \text{ (mod } 256)$ or
$9x \equiv 1 \ (mod \ 256)$
$9 \times 57 \equiv 1 \ (mod \ 256)$
then $x = 57 = \bar{a}$
Encryption 1 : *caesar cipher*
Plaintext SAYA KULIAH

Change into ASCII code, then using $C \equiv P + 8 \bmod 256, 0 \leq P \leq 255$, the message changes to chipertext 1:

	S	A	Y	A		K	U	L	I	A	H
ASCII	83	65	89	65	32	75	85	76	73	65	72
CP 1	91	73	97	73	40	83	93	84	81	73	80

Obtained *ciphertext 1*

[	I	a	I	(	S	]	T	Q	I	P

Encryption 2: *affine* cipher
Plaintext

[	I	a	I	(	S	]	T	Q	I	P

Change into ASCII code

91	73	97	73	40	83	93	84	81	73	80

then using $C \equiv \big((9 \times P) + 8\big) \bmod 256, 0 \leq P \leq 255$ the following results are obtained:
$C \equiv \big((9 \times 91) + 8\big) \bmod 256 = 59$
$C \equiv \big((9 \times 73) + 8\big) \bmod 256 = 153$
$C \equiv \big((9 \times 97) + 8\big) \bmod 256 = 113$
$C \equiv \big((9 \times 73) + 8\big) \bmod 256 = 153$
$C \equiv \big((9 \times 40) + 8\big) \bmod 256 = 112$
$C \equiv \big((9 \times 83) + 8\big) \bmod 256 = 243$
$C \equiv \big((9 \times 93) + 8\big) \bmod 256 = 77$
$C \equiv \big((9 \times 84) + 8\big) \bmod 256 = 252$
$C \equiv \big((9 \times 81) + 8\big) \bmod 256 = 225$
$C \equiv \big((9 \times 73) + 8\big) \bmod 256 = 153$
$C \equiv \big((9 \times 80) + 8\big) \bmod 256 = 216$

59	153	113	153	112	243	77	252	225	153	216

Obtained *ciphertext* 2

;	Ö	à	Ö	p	ó	M	ü	á	Ö	Ø

Decryption

Decryption 1: *Affine cipher*
Ciphertext

;	Ö	à	Ö	P	ó	M	ü	á	Ö	Ø

Change into ASCII code

59	153	113	153	112	243	77	252	225	153	216

then using $P \equiv \big(57(C - 8)\big) \bmod 256, 0 \leq C \leq 255$ the following results are obtained:
$P \equiv \big(57(59 - 8)\big) \bmod 256 = 91$
$P \equiv \big(57(153 - 8)\big) \bmod 256 = 73$
$P \equiv \big(57(113 - 8)\big) \bmod 256 = 97$
$P \equiv \big(57(153 - 8)\big) \bmod 256 = 73$
$P \equiv \big(57(112 - 8)\big) \bmod 256 = 40$
$P \equiv \big(57(243 - 8)\big) \bmod 256 = 83$
$P \equiv \big(57(77 - 8)\big) \bmod 256 = 93$
$P \equiv \big(57(252 - 8)\big) \bmod 256 = 84$
$P \equiv \big(57(225 - 8)\big) \bmod 256 = 81$
$P \equiv \big(57(153 - 8)\big) \bmod 256 = 73$
$P \equiv \big(57(216 - 8)\big) \bmod 256 = 80$

91	73	97	73	40	83	93	84	81	73	80

Obtained plaintext

[	I	a	I	(	S	]	T	Q	I	P

Decryption 2 : *caesar cipher*
Ciphertext

[	I	a	I	(	S	]	T	Q	I	P

Change into numbers

91	73	97	73	40	83	93	84	81	73	80

then using $C \equiv P - 7 \bmod 26, 0 \leq P \leq 25$, the message changed to:

ASCII	83	65	89	65	32	75	85	76	73	65	72

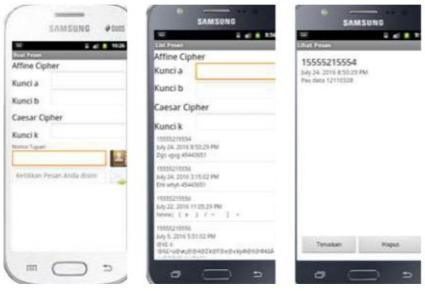
Obtained *ciphertext*

S	A	Y	A		K	U	L	I	A	H

RESULT AND DISCUSSION

Application of Caesar and Affine Cipher

A combination of cesarean section and affine cipher is done so that the encoding is more difficult to solve. That is because, if encoding using a caesar cipher is easy to solve using the brute force method and the most frequent presentation of letter frequencies. One example application of a combination of caesar and affine cipher is that it is used in keeping android-based sms messages (Putra, Mesran, and Sianturi, 2017). The display of Android-based SMS messages can be seen in Figure 1.a, Figure 1.b, and Figure 1.c.



(a) (b) (c)

Figure 1. (a). Display Makes Message, **(b).** Display Receipt Message, **(c).** Display Message view

Caesar ciphers do not have to be combined with affine ciphers or vice versa to secure messages. Caesar cipher can be combined with other algorithms. Affine cipher can also be combined with other algorithms to secure messages. Affine ciphers can be combined with Merkel Hellman's knapsack algorithm to secure messages Fadlan and Hadriansa, 2017). The combination of affine cipher and knapsack merkel hellman can be designed using Microsoft Visual Studio application. In this combination the message to be sent is transformed first into the ASCII code. The use of transformation into the ASCII code will affect the modulo calculation. In the use of transformation into alphabetical numbers, it is enough to use modulo 26 because the number of alphabet is only 26. But the ASCII code is 256, so the modulo used is modulo 256.

Caesar cipher algorithm can be combined with the RSA algorithm to secure document files or text messages (Gunawan, 2018). The use of this combination is considered safe compared to only one algorithm. That's because this combination will combine the algorithm with the calculation of the structure of the alphabet combined with factoring prime numbers. The process of securing files using a combination of cesarean ciphers and RSA algorithms can use applications the way shown in Figure 2.

CONCLUSIONS

Based on the explanation that has been done, it can be concluded that:

1. The combination of cesarean cipher and affine cipher is done because affine cipher has advantages that can cover the shortcomings of cesarean cipher so that the code formed is more difficult to solve. The advantage is that affine cipher has three different keys in doing encryption, decryption and shifting.
2. A combination of cesarean cipher and affine cipher can be used to secure messages. This can be seen from the results of manual calculations that have been carried out
3. The combination of cesarean cipher and affine cipher one of which can be applied to sending Android-based SMS
4. Caesar ciphers and affine ciphers can be combined with other algorithms such as combined with knapsack merkel hellman's algorithm or RSA algorithm.

REFERENCES

Babu S A 2017 Modification Affine Ciphers Algorithm for Cryptographic Password *International Journal of Research in Science & Engineering* **3** 346-351

D. S. Ginting et al. 2017 Modification of Symmetric Cryptography with Combining Affine Chiper and Caesar Chiper which Dynamic Nature in Matrix of Chiper Transposition by Applying Flow Pattern in the Planting Rice *Advances in Science, Technology and Engineering Systems Journal* **2** 6-12

Fadlan M dan Hadriansa 2017 Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algorima Knapsack Merkle Hellman dan Affine Cipher *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)* **4** 268-274

Gunawan I 2018 Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk Pengamanan File Dokumen dan Pesan Teks *Jurnal Nasional Informatika dan Teknologi Jaringan* **2** 124-129

Katz J and Lindell Y 2007 *Introduction to Modern Cryptography* (United States: Chapman & Hall/CRC)

Kromodimoeljo S 2010 *Teori dan Aplikasi Kriptografi* (Jakarta: Penerbit SPK IT Consulting)

Putra H Y, Mesran, dan Sianturi, M 2017 Implementasi Algoritma Affine Cipher dan Caesar Cipher dalam Penyandian Pesan SMS Berbasis Android *Pelita Informatika Budi Darma* **XVI** 126-129

Rachmawati D, dan Candra A 2015 Implementasi Kombinasi Caesar dan Affine cipher untuk keamanan data Teks *Jurnal Edukasi dan Penelitian (JEPIN)* **1** 60-63

Rosen K H 2011 *Elementary Number Theory and its applications 6th ed* (Boston: Pearson)

Schneier, B 1996 *Aplied Cryptography* (New York US: John Wiley & Sons Inc)

Sundarayya P, et al. 2016 Some Technique Algorithms of Extension of Affine Cipher Cryptosystem Using Residue Modulo Prime Number *Open Journal of Applied & Theoretical Mathematics* **2** 88-98

Siahaan, A P U 2018 Enkripsi Teks dengan Algoritma Affine Cipher *Konferensi Nasional Sistem Informasi dan Komputer* http://www.asciitable.com/