

**ISAS ( Information Search and Analysis Skill)**

**“Substitution Methode with**

**Caesar Chiper”**

Group 8

Jasmine Nabila Novel

Muhammad Alif Farhan

Faculty :

Riza Muhammad Nurman S.Kom

Class : 4SC4

Faculty of Engineering University of Indonesia

Depok 16424

# Preface

First, Let us give praise to Allah S.W.T who give guidance to us untill we can complete our ISAS entitled “Digital Watermarking”. As author write this article, author get a lot of support from various parties. Among others are :

1. Our parents, who always help in the form of spirit and material.
2. Mr. Muhammad Suryanegara, ST, M.Sc as director of CCIT Faculty of Engineering, University of Indonesia.
3. Mr. Riza Muhammad Nurman S.Kom, as our faculty who have provided guidance and support and referrals to us so that we can finish ISAS.
4. Our friends who always give the information that they know, exchange ideas and give encouragement to us in writing this article.

Author know that the results of this article is far from perfect and there are still many shortcomings, author hope readers will give comments and suggestions in building this article in order to become better. We hope this article can be useful for those who read or hear, especially for CCIT students of the Faculty of Engineering UI.

Our ISAS titled “Substitution Methode with Caesar Chiper” is One of Technique in Substitusion Encryption.

Depok, March 2018

Author

# TABLE OF CONTENTS

[Preface i](#_Toc508622173)

[TABLE OF CONTENTS ii](#_Toc508622174)

[CHAPTER I 1](#_Toc508622175)

[INTRODUCTION 1](#_Toc508622176)

[I.1 Writing Objective 2](#_Toc508622177)

[I.2 Problem Domain 2](#_Toc508622178)

[I.3 Writing Methodology 2](#_Toc508622179)

[I.4 Writing Framework 2](#_Toc508622180)

[I.5 Problem Domain 3](#_Toc508622181)

[CHAPTER II 4](#_Toc508622182)

[BASIC THEORY 4](#_Toc508622183)

[II.1 Security System 4](#_Toc508622184)

[II.2 Definition of Encryption 4](#_Toc508622185)

[II.3 Definition of Cryptography 4](#_Toc508622186)

[II.4 Definition of Substitution Encryption 5](#_Toc508622187)

[II.5 Definition of Caesar Chiper 5](#_Toc508622188)

[II.6 History of Caesar Chiper 5](#_Toc508622189)

[CHAPTER III 6](#_Toc508622190)

[PROBLEM ANALYSIS 6](#_Toc508622191)

[III.1 Technique and Analysis Caesar Chiper 6](#_Toc508622192)

[III.2 Advantages and Disadvantages using Caesar Chiper 10](#_Toc508622193)

[CHAPTER IV 11](#_Toc508622194)

[CONCLUSSION AND SUGGESTION 11](#_Toc508622195)

[IV.1 Conclussion 11](#_Toc508622196)

[IV.2 Suggestion 11](#_Toc508622197)

# CHAPTER I

# INTRODUCTION

Confidentiality of messages or data owned by a person is important in the delivery of messages so that messages can only be provided by certain people who can access the information. In the era of all sophisticated like this tool to send a message already many including the media such as: facebook and twitter so that we can send messages quickly and vice versa we can receive messages quickly too.

. Of all the particular ease will be very influential when will send a message whose contents only certain people who may know the contents. One that must be really guarded is a message that is confidential because if the message is spread it will be bad. One commonly used way is with encryption. Encryption is a process to disguise or encode a message so that unauthorized people can not know the meaning of the message

To strengthen the security of messages is by using cryptography so people will not be suspicious if the message is encrypted and people will still think if the message does not contain a secret message. Cryptography is the science and art of keeping messages safe when messages are sent from one place to another. As an example of a cryptographic algorithm is: caesare cipher algorithm

Caesar cipher algorithm is the one that includes classical cryptography uses plaintext, ciphertext and the key to perform encryption and decryption process of securing data. The caesar chiper algorithm is a cryptographic technique that is performed by substituting each alphabet of the message to be encrypted through the shift of the order as the key

By utilizing the caesar cipher the confidentiality / security of the message is more awake and will not easily known by others because the existing message or plaintext will be converted into a series of numbers and letters that can not be guessed.

## I.1 Writing Objective

The purpose of this ISAS are :

1. Security System
2. Definition of Encryption
3. Definition of Cryptography
4. Definition of Subsitution Encryption
5. Definition of Caesar Chiper
6. History of Caesar Chiper

## I.2 Problem Domain

Accordance with the title of ISAS " Analysis Caesar Chiper Substitusion Methode " We will discuss about :

1. Technique and Analysis of Caesar Chiper
2. Advantages and Disadvantages of Caesar Chiper

## I.3 Writing Methodology

The method which used in this ISAS is the method of browsing from internet, reading online journal, and make a survey in problem domain.

## I.4 Writing Framework

The paper was written by systematic as follows :

**CHAPTER I : INTRODUCTION**

**1.1 Background**

Discusses the result of research in security data, briefly description about Cryptography , and briefly description about Caesar Chiper.

**1.2 Writing Objective**

The purpose of this article is to understand about Cryptography, Encryption, advantages and disadvantages Caesar Chiper Cryptography, and technique of Caesar Chiper.

## I.5 Problem Domain

First, tell about the advantages and disadvantages of Caesar Chiper Cryptography. It’s Comparison between benefit and deficit. Second tell about technique and analysis of Caesar Chiper used to protect data Security

**1.4 Methodology Writing**

To get data which needed, this paper use the method of observing or direct observation techniques, author reads famous repository online journal.

**1.5 Writing Framework**

This paper Writing Framework consists of four Chapter, the first chapter is introduction which tells the background, writing objective, several problem domain, methodology writing and writing framework of this paper.

**Chapter II Basic of Theory**

In chapter II, paper written several sub chapter. The first sub chapter is to tell about Security System. The second sub chapter is to tell about Definition of Encryption. The third sub chapter is to tell about Definition Cryptography. The fourth sub chapter is to tell about Substition Encryption.. The sixth sub chapter is to tell about Definition of Caesar Chiper. The seventh sub chapter is to tell about History of Caesar Chiper.

**Chapter III Problem Analysis**

Analyzing and solve the problem that contained in problem domain.

**Chapter IV Conclusion and Suggestion**

Conclude and suggest related to this paper.

# CHAPTER II

# BASIC THEORY

## II.1 Security System

In general, security is “the quality or state of being secure to be free from danger”. In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system. The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

## II.2 Definition of Encryption

Encryption is one of the principal means to guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext (original message before encryption) and transforms it into cipher text (scrambled message after encryption) Many encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: Symmetric-key (also called secret-key) and Asymmetric-key (also called public-key) encryption A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together.

## II.3 Definition of Cryptography

Cryptography (cryptography) is derived from Greek, consisting of two syllables namely crypto and graphia. Crypto means to hide, while graphia means writing. Cryptography is the study of mathematical techniques related to information security aspects, such as data confidentiality, data validity, data integrity, and data authentication (Menezes, Oorschot and Vanstone, 1996). In general cryptography is the science and art of keeping the news confidential (Bruce SchneireApplied Cryptography). In addition to the definition of science that studies mathematical techniques related to aspects of information security such as confidentiality, data integrity and authentication.

## II.4 Definition of Substitution Encryption

The substitution password is a type of encryption method in which each unit of light text is replaced by encrypted text with a regular system. Substitution encoding methods have been used from ancient (classical cryptography) to the present (modern cryptography This method is done by replacing each letter of the original text with the other letter as a passphrase that has been defined before by the key algorithm..

## II.5 Definition of Caesar Chiper

Caesar Cipher is one of the oldest and most well known cipher algorithms in the development of cryptography. Caesar cipher is one type of cipher substitution that makes up the cipher by switching characters on plaintext to exactly one character on the chipperext. This technique is called a single alphabet chiper. The cryptographic algorithm of Caesar Cipher is very easy to use. The essence of this cryptographic algorithm is to shift all characters on plaintext with the same shift value.

## II.6 History of Caesar Chiper

Caesar's name was taken from Julius Caesar, who according to Suetonius's book The Life of the Twelve Caesar, used this code with three shifts, to send messages containing secrets or military tactics. By replacing the initial letter position with alphabet or called ROT3 algorithm. Caesar Cipher is one of the oldest and most well known cipher algorithms in the development of cryptography.

# CHAPTER III

# PROBLEM ANALYSIS

## III.1 Technique and Analysis Caesar Chiper

The cryptographic algorithm of Caesar Cipher is very easy to use. The essence of this cryptographic algorithm is to shift all characters in plaintext with the same shift value

The steps taken to form chiperteks with Caesar Cipher are:t.

1. Determines the magnitude of the character shift used in forming the ciphertext to plaintext.
2. Exchange the characters on plaintext into cipherteks based on predetermined shifts.

And for Formula Algorithm Caesar Chiper is :

Formula Encryption :

X= ( Y + K ) mod 26

Formula Decryption :

Y = (X - K ) mod 26

X = PlainText

Y = ChiperText

Mod 26 = Alphabet by Amount 26

K = Key

Here is an example of using Caesar Cipher with a large shift of 3 characters. With the value of the shift, obtained table shift value of Caesar Cipher as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | Y | Y | Z | A | B | C |

Note :

Rows First : Plaintext

Rows Second : Chipertext

Example

SAYA LELAH (PlainText)

VDBD OHODK (ChiperText)

SEPAKBOLA (Plain Text)

VHSCNEROC (Chiper Text)

1. By Use One Key

Example :

Using One Key “FTUI”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| F | T | U | I | A | B | C | D | E | G | H | J | K | L | M | N | O | P | Q | R | S | V | W | X | Y | Z |

Note : Characters which has emerged in not written back again

SAYA LELAH

QFYF JAJFD

1. By Use Shift Chiper

The Caesar Cipher is a type of shift cipher. Shift Ciphers work by using the modulo operator to encrypt and decrypt messages. The Shift Cipher has a key K, which is an integer from 0 to 25.

1. How To Encrypt :

Step by Step :

1. Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number X.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P | Q | R | S | T | U | V | W | X | Y | Z |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

( A=0, B=1, C=2, ...,Y=24, Z=25)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

1. Calculate: Y = (X + K) mod 26
2. Convert the number Y into a letter that matches its order in the alphabet starting from 0.

For Example :

friend to use the Shift Cipher with key K=19 for our message.

encrypt the message "KHAN", as follows:​

K H A N

10 7 0 13

+ 19 19 19 19

( 29 26 19 32) mod 26

3 0 19 6

D A T G

So, after applying the Shift Cipher with key K=19 message text "FTUI" gave cipher text "YONB".

1. How To Decrypt :
2. Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number Y.

(A=0, B=1, C=2, ..., Y=24, Z=25)

1. Calculate: X= (Y - K) mod 26
2. Convert the number X into a letter that matches its order in the alphabet starting from 0

D A T G

3 0 19 6

19 19 19 19

(-16 -19 0 -13) mod 26

10 7 0 13

K H A N

## III.2 Advantages and Disadvantages using Caesar Chiper

Here is Follows Advantages and Disadvantages using Caesar Chiper

Advantages :

1. Very popular in his time julius caesar kingdom for his soldiers

It was done in the days of his kingdom to send secret text messages to his army followers

1. Easy to learn because only shifted the letter as much as 3 digits
2. Only amounted to 26 keys

corresponding to the alphabet numbered 26

1. Easy to Solve

yes, without the need to drag on to solve it

Disadvantages :

1. The security level is very low
2. Keyword-breaking techniques can be done by checking all the existing keys that amounted to 26.
3. It is not recommended to use caesar chiper encryption at this time because it includes old encryption or can be called classical cryptographic algorithm and now switch to modern

# CHAPTER IV

# CONCLUSSION AND SUGGESTION

## IV.1 Conclussion

Substitution encryption is an encryption that replaces plaintext to chipertext which one of them is by caesar chiper method. Caesar chiper is the oldest algorithm in julius caesar era and famous in its time. very easy to learn is by shifting the character as much as 3 digits with a limit of 26 letters in accordance with the number of existing alphabets

## IV.2 Suggestion

Caesar chiper is because the old algorithm method should not be recommended to use it at this time. can switch to modern like md5. but if want to learn it as an early learning encryption it is advisable to learn it

**BIBLIOGRAPHY**

file:///D:/jurnal/Yuli%20Praptomo%20PHS-27-stmikelrahma.pdf

https://www.khanacademy.org/computing/computerscience/cryptography/ciphers/a/ciphers-vs-codes

https://learncryptography.com/classical-encryption/caesar-cipher