Encoding Cryptography Using Matrices

Taufic Leonardo Sutejo 13514022
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13514022@std.stei.itb.ac.id

***Abstract*— Matrix is one of the topics that be discussed in ITB Informatics subjects in second years which is called Geometric Algebra. Long time ago, in the Second World War, people used codes to give important information to their friends because they did not want the enemy knew about their strategies or what they were going to do next, most likely for military purposes. They needed to encrypt and decrypt the code so they knew what the information was. Cryptography is one of the methods to encode and decode the code into information that we, human, can understand.**

***Keywords*—Matrices, Encrypt, Decrypt, Cryptography**

I. Introduction

Nowadays, information is too easy to be accessed. Information can be accessed through the search engines, such as Google, yahoo, Bing, etc. Besides search engines, social media is also one of the most information flow around.

Information that be changed into an image is quite risky. Because of that problem, people thought of solution so that the encoder would not know what the information were and the information could only be known by receiver. The solution was changing the information into a random code. This solution has already existed in thousands years ago. Around 1900 BC, this technique had been used by the Ancient Egypt.

The secret code that is sent by the sender can be alphabets or numbers. The matrices operation takes place in changing the secret information into codes. Before sending the codes to the receiver, sender should give the key to change code or at least both sender and receiver know what the key is.

In this article, writer wanted to explain brief about how the information change into codes, how the encryption and decryption works. This is what they called cryptography.

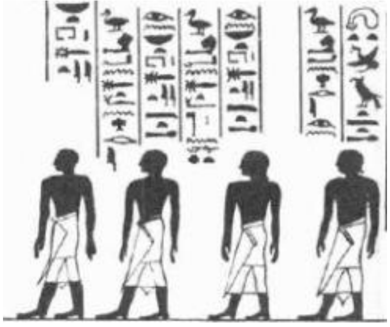


Figure1. Ancient Egypt's drawing
(Source: https://drmgnh.wordpress.com/2013/11/06/a-female-administrator-in-ancient-egypt/, at 10.00 in 15 December 2015)

II. BRIEF HISTORY ABOUT CRYPTOGRAPHY

Cryptography consists of two words, kryptos and graphein. Kryptos comes from Greek, means hidden and Graphein means writing. Cryptography is a study that discussed about encryption.

Like in the part I of this article, around 1900 BC, the first discovery of the use of cryptography was found in the chamber of the tomb of Khnumhotep II, in Egypt. In most early civilizations, discovery of using cryptography was getting a lot.

In around 100 BC, Julius Caesar was known to use cryptography, sending a secret message to his army. The cipher name is Caesar cipher. The cipher substitute each character of the plain text to another character from the cipher text. Each character was shifted by 3 places, for example, letter A was replaced by letter D, letter B was replaced by letter E, letter C was replaced by letter F, and so on until letter Z was replaced by letter C. But this cipher has disadvantage. The substitution cipher can be broken when using the input recursively the same letter in a language.

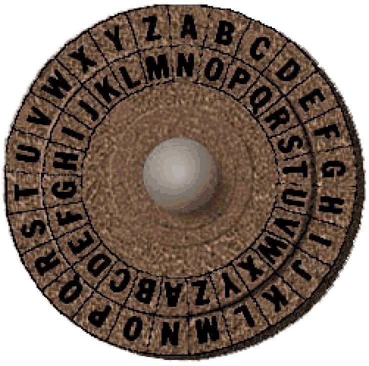
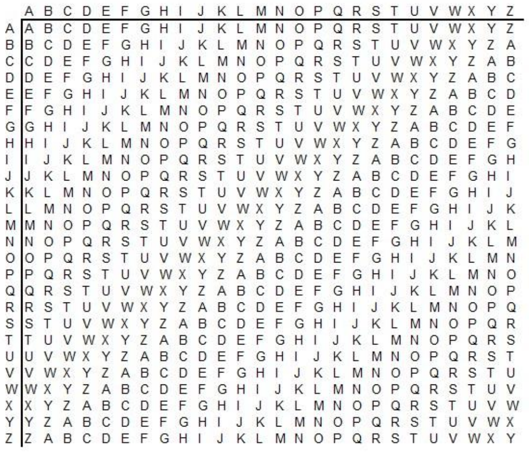

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J

Figure2. Caesar cipher
(Sources: http://www.secretcodebreaker.com/history2.html, at 10.15, 15 December 2015)

In 16th century, the first encryption key has been designed. The designer is Vigenere.



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

Figure3. Vigerene Cipher
(Sources:
https://www.geocaching.com/seek/cache_details.aspx?wp=GC2D14K&title=cipher-this, at 10.30, 15 December 2015)

At the beginning of 19th century, thanks to Faraday, Hebern could design an electro-mechanical contraption which was called the Hebern rotor machine. The rotating disc consists of secret key. The key encoded a substitution table and each key press from the keyboard resulted in the output of cipher text. The disadvantage of this machine is same with Vigerene Cipher.

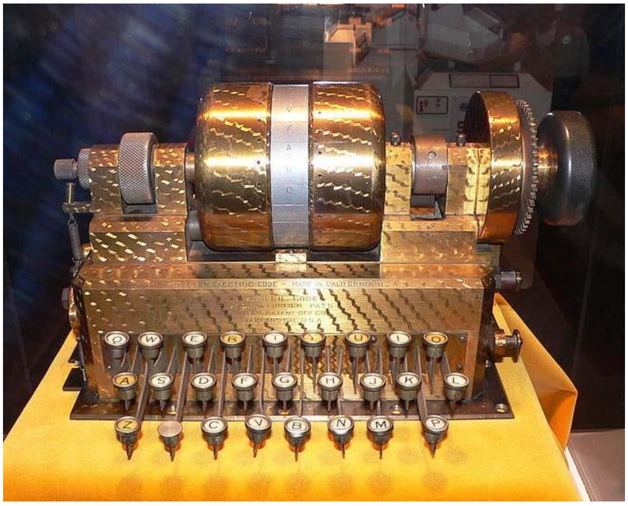


Figure4. Hebern rotor machine
(Sources:
http://www.jproc.ca/crypto/hebern_1.html, at 10.40, 15 December 2015).

At the End of the World War I, the enigma machine was finally invented by German engineer Arthur Scherbius. This machine was the most used at that time. Different between Hebern rotor machine and enigma was the number of rotor. The Enigma machine has 3 or 4 or even more rotor. The Enigma machine was finally broken by Poland and the technology was transferred to British cryptographers to gets the daily key. Until World War II, cryptography was being used as military purposes, hiding important information.

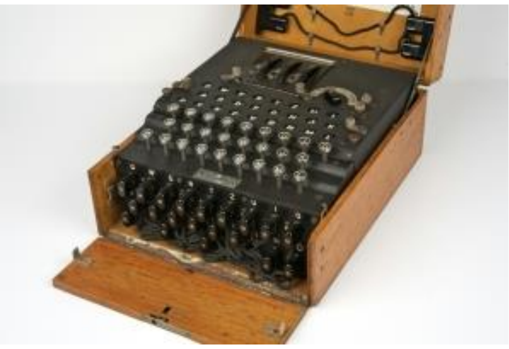


Figure4. Enigma
(Sources:
http://cryptomuseum.com/crypto/enigma/i/index.htm, at 10.45, 15 December 2015)

III. Basic Theory of Matrix

3.1 Matrix

A matrix is a rectangular array that consists of element. The matrix also consists of m represent matrix rows and n represent matrix columns.

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{1n} \\ a_{21} & a_{22} & a_{2n} \\ a_{31} & a_{32} & a_{3n} \\ \dots\dots & \dots\dots\dots & \dots\dots. \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

3.1.1 Matrix consists of several types

- Rectangular matrix
  A matrix is formed by different number of rows and columns. For example,
  $$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$
- Square matrix
  A matrix is formed by same number of rows and columns. For example,
  $$A = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$
- Row matrix
  A matrix is formed in single row. For example,
  $$A = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$
- Column matrix
  A matrix is formed in single row. For example,
  $$A = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$
- Zero matrix
  A matrix is formed with all the elements are zeros. For example,
  $$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$
- Diagonal matrix

A matrix is formed with all the elements are zeros except the diagonal elements. For example

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

- Upper triangular matrix
  A matrix is formed with all the elements below the diagonal are zeros. For example,

$$A = \begin{pmatrix} 1 & 4 & 5 \\ 0 & 2 & 6 \\ 0 & 0 & 3 \end{pmatrix}$$

- Lower triangular matrix
  A matrix is formed with all the elements above the diagonal are zeros. For example,

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & 0 \\ 5 & 6 & 3 \end{pmatrix}$$

- Scalar matrix
  A matrix is formed with all the diagonal elements are equal to a number and beside the diagonal, all the elements are zeros. For example,

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

- Identity matrix
  A square matrix is formed with all the diagonal elements are equal to 1 and beside the diagonal, all the elements are zeros. For example,

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- Transpose matrix
  A matrix is formed with row switch with column and column switch with row from its original matrix. For example,

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, A^T = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$$

- Regular matrix
  A square matrix that has an inverse. For example,

$$A = \begin{pmatrix} 1 & 7 & 9 \\ 4 & 2 & 8 \\ 5 & 6 & 3 \end{pmatrix}$$

- Singular matrix
  A square matrix that has no inverse. For example,

$$A = \begin{pmatrix} 3 & 2 \\ 16 & 8 \end{pmatrix}$$

- Idempotent matrix
  A matrix is called idempotent when $A^2 = A$. For example,

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- Symmetric matrix
  A matrix is called symmetric when $A^T = A$. For example,

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}, A^T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$$

- Anti-symmetric matrix
  A matrix is called anti-symmetric when $A^T = -A$. For example,

$$A = \begin{pmatrix} 1 & 2 & 3 \\ -2 & 4 & 5 \\ -3 & -5 & 6 \end{pmatrix},$$

$$A^T = \begin{pmatrix} -1 & -2 & -3 \\ 2 & -4 & -5 \\ 3 & 5 & -6 \end{pmatrix}$$

- Orthogonal matrix
  A matrix is called orthogonal when $A^T * A = I$. For example,

$$A = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \\ \frac{2}{3} & \frac{2}{3} & \frac{1}{3} \end{pmatrix}$$

3.1.2 Matrix Operation

- Adding matrix
  Two matrices A_{mxn} and B_{pxq} can be added if both have the same rows and columns, row m equal to row p and column n equal to column q.

$$A + B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} 6 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix}$$

$$A + B = \begin{pmatrix} 1+6 & 2+5 & 3+4 \\ 4+3 & 5+2 & 6+1 \end{pmatrix}$$

$$A + B = \begin{pmatrix} 7 & 7 & 7 \\ 7 & 7 & 7 \end{pmatrix}$$

- Scalar matrix multiplication
  The product between real number by a matrix, and each element is multiplied by the real number.

$$2.A = 2\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

$$A = \begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \\ 14 & 16 & 18 \end{pmatrix}$$

- Multiplying_matrices
  Two matrices A_{mxn} and B_{nxq} can be multiply if total column n of matrix A is equal to total row p of matrix B.

$$A.B = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 3 \\ 2 & 1 \end{pmatrix}$$

$$A.B = \begin{pmatrix} 1*2+2*1+1*2 & 1*1+2*3+1*1 \\ 3*2+1*1+3*2 & 3*1+1*3+3*1 \end{pmatrix}$$

$$A.B = \begin{pmatrix} 6 & 8 \\ 13 & 9 \end{pmatrix}$$

  Properties of the multiplying matrices

$$A.B \neq B.A$$

$$(A.B).C = A.(B.C)$$

- Inverse Matrix

  Multiplication between a matrix and its inverse is equal to identity matrix.

  $$A.A^{-1} = I$$

  Properties of the inverse matrix

  $$(A.B)^{-1} = B^{-1}.A^{-1}$$
  $$(A^{-1})^{-1} = A$$
  $$(k.A)^{-1} = k^{-1}A^{-1}$$
  $$(A^{T})^{-1} = (A^{-1})^{T}$$

  Calculate the inverse matrix

  There are two way to calculate inverse matrix.

1. Multiplying one per determinant of a matrix with the cofactor of a transpose matrix.

   $$A^{-1} = \frac{1}{|A|} Cofactor\ of\ A^{T}$$

2. Use Gauss-Jordan elimination to transform [A|I] into [I|A^{-1}]

3.2. Cryptography

Sometimes information is too valuable so sender does not want the information is known by others except the receiver.

Cryptography is a way to make the information becomes codes. Cryptography consists of decide what to be sent, encoding process and decoding process.

This is the encoding process steps:

1. Write the message in a row.
2. Decide the conversion rule such as changing every alphabet into number. A to 1, B to 2, so on.
3. Write the conversion.
4. Write the conversion into a matrix.
5. Decide the key matrix. There are 2 rules. First, the key matrix should be integers in inverse and no inverse. Second, make sure the key matrix can be multiply by the message matrix.
6. Calculate Code = key_matrix * message_matrix.
7. Write the code into a row.

Decoding process is exactly the same, just change the key_matrix into inverse key_matrix.

IV. ENCODING AND DECODING MESSAGE INTO MATRIX

According to the part III cryptography, the step that the writer should do to change message into codes is.

1. Message: I LOVE CRYPTOGRAPHY
2. Deciding conversion rule:

   A – 1, B – 2, C – 3, D – 4, E – 5, F – 6, G – 7, H – 8, I – 9, J – 10, K – 11, L – 12, M – 13, N – 14, O – 15, P – 16, Q – 17, R – 18, S – 19, T – 20, U – 21, V – 22, W – 23, X – 24, Y – 25, Z – 26.
3. Convert message corresponding to the conversion rule.

   9 12 15 22 5 3 18 25 16 20 15 7 18 1 16 8 25
4. Convert message row into matrix.

$$MessageMatrix = A = \begin{pmatrix} 9 & 12 & 15 & 22 & 5 & 3 \\ 18 & 25 & 16 & 20 & 15 & 7 \\ 18 & 1 & 16 & 8 & 25 & 0 \end{pmatrix}$$

5. Decide the key.

$$KeyMatrix = K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix}$$

6. Calculate the code.

$$Code = C = K.A$$

$$C = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix} \begin{pmatrix} 9 & 12 & 15 & 22 & 5 & 3 \\ 18 & 25 & 16 & 20 & 15 & 7 \\ 18 & 1 & 16 & 8 & 25 & 0 \end{pmatrix}$$

$$C = \begin{pmatrix} 99 & 65 & 95 & 86 & 110 & 17 \\ 252 & 157 & 238 & 208 & 285 & 41 \\ 315 & 196 & 301 & 266 & 355 & 51 \end{pmatrix}$$

7. The message that will be sent:

   99 65 95 86 110 17 252 157 238 208 285 41 315 196 301 266 355 51

To read the message that has been encrypting, the receiver should decode the message code. This is the step to decode the message code.

1. Message code: 99 65 95 86 110 17 252 157 238 208 285 41 315 196 301 266 355 51
2. Change into a matrix

$$C = \begin{pmatrix} 99 & 65 & 95 & 86 & 110 & 17 \\ 252 & 157 & 238 & 208 & 285 & 41 \\ 315 & 196 & 301 & 266 & 355 & 51 \end{pmatrix}$$

3. Inverse the KeyMatrix

$$KeyMatrix = K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix}$$

$$K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 2 & -2 & 1 \\ 4 & 1 & -2 \\ -3 & 0 & 1 \end{pmatrix}$$

   Inverse matrix using Gauss-Jordan elimination.

4. Calculate Message = KeyMatrix * C

$$Message = M = K^{-1}.C$$

$$M = \begin{pmatrix} 2 & -2 & 1 \\ 4 & 1 & -2 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 99 & 65 & 95 & 86 & 110 & 17 \\ 252 & 157 & 238 & 208 & 285 & 41 \\ 315 & 196 & 301 & 266 & 355 & 51 \end{pmatrix}$$

$$M = \begin{pmatrix} 9 & 12 & 15 & 22 & 5 & 3 \\ 18 & 25 & 16 & 20 & 15 & 7 \\ 18 & 1 & 16 & 8 & 25 & 0 \end{pmatrix}$$

5. Convert the matrix into message row

   9 12 15 22 5 3 18 25 16 20 15 7 18 1 16 8 25 0
6. Convert the message row corresponding to the conversion

   I LOVE CRYPTOGRAPHY.

V. CONCLUSION

In Conclusion, using cryptography the sender can change a message into a code according to the conversion rule. The conversion rule is decided by the sender. Sender can give extra function. But the function that the sender give must be inversed too. After decide the conversion rule, decide the matrix key that return determinant equal to 1 and the key can be multiply by its message matrix. Calculate the code using the rule Code = Key_matrix * message_matrix. The code now is ready to be sent. Cryptography helps human in keeping information privately. (Message: 95 17 80 74 76 91 83 45 237 39 207 178 199 227 206 109 304 52 263 247 288 262 140. Key_matrix still same.)

REFERENCES

[1]http://staff.uny.ac.id/sites/default/files/Aplikasi%20matriks%20inverse%20dalam%20kriptografi.pdf, at 12.00, 15 December 2015

[2]http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf, at 12.15, 15 December 2015

[3]http://www.studentpulse.com/articles/41/a-brief-history-of-cryptography, at 12.37, 15 December 2015

[4]http://www.vitutor.com/alg/matrix/, at 14.00, 15 December 2015

[5]http://aix1.uottawa.ca/~jkhoury/cryptography.htm, at 14.25, 15 December 2015

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 16 December 2015

Taufic Leonardo Sutejo/ 13514022