Penggunaan Transformasi Matriks dalam Enkripsi dan Dekripsi

Varian Caesar - 13514041
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13514041@std.stei.itb.ac.id

***Abstrak*—Enkripsi dan Dekripsi adalah 2 metode utama dan penting dalam kriptografi. Kriptografi adalah pengkajian tentang penyandian isi sandi yang merupakan pesan rahasia. Enkripsi adalah proses mengubah data yang asli menjadi kode sandi, dari *plain text* ke *chipper text*. Sebaliknya, Dekripsi yaitu proses mengubah kode sandi menjadi data asli kembali, yaitu dari *chipper text* ke *plain text*. Dalam proses penyandian, digunakan banyak cara dan algoritma untuk menyamarkan data ke *chipper text*. Salah satunya adalah penyandian dengan transformasi matriks. Pada makalah ini akan dijelaskan cara penyandian teks dengan memanfaatkan transformasi matriks dengan bilangan modulo 26.**

***Kata Kunci*—Transformasi Matriks, Kriptografi, sandi, enkripsi, dekripsi, *plain text, chipper text*.**

I. Pendahuluan

Aplikasi matriks sangatlah luas. Salah satu aplikasi matriks yang sangat berguna adalah dalam dunia kriptografi (ilmu pembacaan sandi) yaitu pada saat enkripsi dan dekripsi. Penggunaan matriks dalam membantu penyandian sangat praktis dan mudah tanpa perhitungan yang cukup rumit. Di dalam bahasan makalah ini, penyandian yang digunakan yaitu algoritma *Hill Ciphers* yang ditemukan oleh Lester S.Hill pada tahun 1929.

Inti dari algoritma *Hill Cipher* adalah, pertama kita harus merepresentasikan setiap alfabet dengan angka yang habis dibagi 26 atau mod 26 karena dalam kasus yang dibahas adalah enkripsi pada pesan teks, jika ingin menambahkan symbol dan tanda baca maka dapat disesuaikan bilangan modulonya. Setelah selesai merepresentasikan angka pada setiap alphabet, kita harus menyiapkan matriks yang berisi kunci atau *key* penyandian. Karakter *plain text* akan dibaca per dua karakter sekaligus sebagai matriks 2 x 1 dan ditransformasi dengan matriks *key* menjadi *chipper text* pada proses enkripsi. Pada proses Dekripsi, matriks *key* di invers lalu *chipper text* akan dibaca per 2 karakter dan ditransformasi dengan matriks *key* yang sudah diinvers tadi untuk mendapatkan *plain text* semula.

II. Dasar Teori

Dasar Teori yang digunakan adalah matriks khususnya transformasi matriks.

A. *Matriks*

Matriks adalah sebuah struktur dimana elemen – elemennya disusun menurut baris dan kolom membentuk persegi panjang. Elemen matriks yang memanjang ke bawah disebut baris, sedangkan yang memanjang ke samping disebut kolom.

$$M = \begin{bmatrix} 1 & 2 & 5 & 1 \\ 9 & -1 & 2 & 0 \\ 4 & 6 & 7 & -3 \end{bmatrix}$$

Pada contoh matriks diatas, Matriks M memiliki jumlah baris sebanyak 3 dan kolom sebanyak 4. Maka kita menyebut ukuran matriks M sebagai matriks 3x4.

B. *Eliminasi Gauss*

Eliminasi Gauss adalah suatu metode untuk mengoperasikan nilai-nilai di dalam matriks sehingga menjadi matriks yang lebih sederhana lagi. Dengan melakukan operasi baris elementer sehingga matriks tersebut menjadi matriks eselon. Metode ini dapat digunakan sebagai salah satu metode penyelesaian persamaan linear dengan menggunakan matriks. Caranya dengan mengubah persamaan linear tersebut ke dalam matriks teraugmentasi dan mengoperasikannya.
Perhatikan contoh berikut untuk lebih jelasnya :

$$\begin{matrix} 1 & 2 & 1 & 6 \\ 1 & 3 & 2 & 9 \\ 2 & 1 & 2 & 12 \end{matrix}$$

Operasikan Matriks nya:

$$\begin{matrix} 1 & 2 & 1 & 6 \\ 0 & 1 & 1 & 3 \\ 2 & 1 & 2 & 1 \end{matrix} \qquad R2 – R1$$

$$\begin{matrix} 1 & 2 & 1 & 6 \\ 0 & 1 & 1 & 3 \\ 0 & -3 & 0 & 0 \end{matrix} \qquad R3 - 2R1$$

$$\begin{matrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 3 & 9 \end{matrix} \qquad R3 + 3R2$$

$$\begin{matrix} 1 & 2 & 1 & 6 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 3 \end{matrix} \qquad R3 / 3$$

Maka diperoleh hasil berupa matriks eselon.

C. *Eliminasi Gauss Jordan*

Eliminasi Gauss-Jordan adalah pengembangan dari eliminasi Gauss yang hasilnya lebih sederhana lagi. Caranya adalah dengan meneruskan operasi baris dari eliminasi Gauss sehingga menghasilkan matriks yang Eselon-tereduksi. Ini juga dapat digunakan sebagai salah satu metode penyelesaian persamaan linear dengan menggunakan matriks. Untuk lebih jelasnya perhatikan contoh berikut :

Dari soal yang sama dengan metode gauss kita peroleh matriks akhir yaitu :

$$\begin{matrix} 1 & 2 & 1 & 6 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 3 \end{matrix}$$

Selanjutnya kita akan mengoperasikan kembali matriks diatas agar menjadi matriks eselon tereduksi :

$$\begin{matrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 3 \end{matrix} \qquad \begin{matrix} \\ \\ R1 - 2R2 \end{matrix}$$

$$\begin{matrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 \end{matrix} \qquad \begin{matrix} \\ R1 + R3 \\ R2 - R3 \end{matrix}$$

D. *Matriks Invers*

Invers dari matriks M adalah matriks M^{-1} dengan ukuran n x n (matriks segi empat). Berikut adalah cara menghitung matriks invers :

1.Matriks 2 x 2

Misalkan A adalah matriks 2x2 :

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Inversnya adalah A^{-1} yaitu diperoleh dari :

$$A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

2.Matriks n x n

Untuk inverse matriks n x n, kita perlu mengenal matriks identitas atau sering dilambangkan dengan I. Matriks identitas yaitu matriks yang mempunyai elemen bernilai 1 pada diagonalnya dan sisanya bernilai 0.

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Misal kita ingin melakukan invers terhadap matriks A yang ber-ordo 3x3 :

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

Kita gabungkan matriks identitas 3x3 dengan matriks A :

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 5 & 6 & 0 & 0 & 0 & 1 \end{array}\right]$$

Selanjutnya kita akan melakukan operasi gauss jordan untuk membuatnya menjadi matriks eselon tereduksi. (pengerjaan tidak ditampilkan)

Hasilnya menjadi :

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -24 & 18 & 5 \\ 0 & 1 & 0 & 20 & -15 & -4 \\ 0 & 0 & 1 & -5 & 4 & 1 \end{array}\right]$$

Bila diperhatikan, posisi matriks identitas bertukar tempat dengan matriks A yang sudah menjadi A^{-1}.

Sehingga hasilnya adalah :

$$A^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$$

E. *Transformasi Matriks*

Tiap – tiap transformasi lanjar dari R^n ke R^m adalah transformasi matriks. Misalkan $\mathbf{e_1}$, $\mathbf{e_2}$, … $\mathbf{e_n}$ adalah basis standar untuk R^n.

Misal A adalah matriks m x n yang berisi T($\mathbf{e_1}$), T($\mathbf{e_2}$), T($\mathbf{e_3}$), … T($\mathbf{e_n}$) sebagai kolom dari matriks A. Secara Umum :

$$T(\mathbf{e_1}) = \begin{bmatrix} a11 \\ a21 \\ \vdots \\ . \\ am1 \end{bmatrix} \quad T(\mathbf{e_2}) = \begin{bmatrix} a12 \\ a22 \\ \vdots \\ . \\ am2 \end{bmatrix}$$

$$T(\mathbf{e_3}) = \begin{bmatrix} a13 \\ a23 \\ \vdots \\ . \\ am3 \end{bmatrix}$$

$$A = \begin{bmatrix} a11 & a12 & \cdots & a1n \\ a21 & a22 & \cdots & a2n \\ . & . & \cdots & . \\ . & . & \cdots & . \\ am1 & am2 & \cdots & amn \end{bmatrix}$$

Contoh : Carilah matriks transformasi dari T : R^3 -> R^3 yang didefinisikan oleh :

$$T\begin{pmatrix} x1 \\ x2 \\ x3 \end{pmatrix} = \begin{bmatrix} x1 + 2\,x2 + x3 \\ x1 + 5\,x2 \\ x3 \end{bmatrix}$$

Jawab :

Basis standar di R^3 adalah (1,0,0), (0,1,0) dan (0,0,1).

$$T\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{bmatrix} 1 + 2.0 + 0 \\ 1 + 5.0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

$$T\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{bmatrix} 0 + 2.1 + 0 \\ 0 + 5.1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 5 \\ 0 \end{bmatrix}$$

$$T\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{bmatrix} 0 + 2.0 + 1 \\ 0 + 5.0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

Matriks transformasi A yaitu :

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Kita dapat melakukan pemeriksaan terhadap matriks tranformasi yang kita daptkan dengan cara mengalikannya dengan vektor **X** yang komponenya adalah (x1,x2,x3).

T(**X**) = A . **X**

$$= \begin{bmatrix} 1 & 2 & 1 \\ 1 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x1 \\ x2 \\ x3 \end{bmatrix}$$

$$= \begin{bmatrix} x1 + 2\,x2 + x3 \\ x1 + 5\,x2 \\ x3 \end{bmatrix}$$

Yang benar merupakan fungsi transformasi pada soal.

III. Penerapan Transformasi Matriks dalam Enkripsi dan Dekripsi

A. Tabel Alfabet dan Kode yang Digunakan

Alfabet	Kode Sandi
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	0

Gambar 3.1 Tabel Alfabet dan kode sandinya

Kode sandi yang dibuat tidak harus mengikuti tabel diatas tetapi bisa diubah.

B. Kriptografi

Kriptografi adalah pengkajian tentang penyandian dan penguraian *(decoding)* isi sandi yang berupa pesan rahasia. Kode rahasia itu sudah dikenal sejak adanya komunikasi. Karena ilmu pengetahuan dan teknologi yang semakin maju, timbulah cara yang lebih praktis dan canggih untuk memelihara informasi penting yang dipancarkan melalui saluran komunikasi umum.

Di dalam kriptografi, kode – kode disebut sandi (*chipper*). Pesan yang tidak dikode disebut teks biasa (*plain text*). Sedangkan pesan yang dikode disebut teks sandi (*chipper text).* Proses pengubahan dari bentuk teks biasa ke bentuk teks sandi disebut penyandian (*enchipering).* Permasalahan yang dihadapi pada kriptografi adalah masalah penyandian dan penguraian sandi. Seperti contoh adalah pesan email " GOOD BYE DAYS" akan disandikan ke bentuk teks sandi atau suatu teks sandi ingin diubah kembali ke bentuk *plaint text* agar bisa dibaca.

C. Kriptografi dengan Menggunakan Matriks (Enkripsi)

Untuk masalah seperti contoh diatas, teks : "GOOD BYE DAYS" akan diubah ke teks sandi dan juga teks sandi yang akan di dekripsi ke teks biasa kembali langkah pertama yang harus kita lakukan adalah menentukan matriks penyandian (dalam hal ini matriks transformasi)
Misal akan digunakan matriks transformasi A selama pembahasan di makalah ini dengan isi matriks A sebagai berikut :

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

Langkah berikutnya, masing-masing alfabet kita beri nilai numerik yang merpresentasikannya, dalam pembahasan ini sudah disediakan tabel alfabet dan juga kode numerik nya di upa bab sebelumnya.

G	O	O	D	B	Y	E	D	A	Y	S	
7	15	15	4	2	25	5	4	1	25	19	

Langkah selanjutnya, kita akan mengelompokkan alfabet tersebut dalam kelompok-kelompok yang berisi 2 buah alfabet di dalamnya,jika jumlah alfabet adalah ganjil maka dapat ditambahkan elemen *dummy* pada alfabet terakhir untuk melengkapi pasangan huruf. Dari contoh diatas, kita peroleh pasangan alfabet :

GO OD BY ED AY SS

Secara traversal, kita konversikan setiap pasangan huruf teks biasa diatas kedalam bentuk vektor kolom **P**.

Untuk pasangan GO, **P1** = $\begin{bmatrix} 7 \\ 15 \end{bmatrix}$

Untuk pasangan OD, **P2** = $\begin{bmatrix} 15 \\ 4 \end{bmatrix}$

Untuk pasangan BY, **P3** = $\begin{bmatrix} 2 \\ 25 \end{bmatrix}$

Untuk pasangan ED, **P4** = $\begin{bmatrix} 5 \\ 4 \end{bmatrix}$

Untuk pasangan AY, **P5** = $\begin{bmatrix} 1 \\ 25 \end{bmatrix}$

Untuk pasangan SS, **P6** = $\begin{bmatrix} 19 \\ 19 \end{bmatrix}$

Langkah berikutnya adalah kita akan mentransformasikan vektor kolom **P** dengan menggunakan matriks A yang kita jadikan *key*.

Untuk pasangan GO, $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 7 \\ 15 \end{bmatrix} = \begin{bmatrix} 37 \\ 45 \end{bmatrix}$ mod 26
= $\begin{bmatrix} 11 \\ 19 \end{bmatrix}$, jadi pasangan GO menghasilkan sandi KS.

Untuk pasangan OD, $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 15 \\ 4 \end{bmatrix} = \begin{bmatrix} 23 \\ 12 \end{bmatrix}$ mod 26
= $\begin{bmatrix} 23 \\ 12 \end{bmatrix}$, jadi pasangan OD menghasilkan sandi WL.

Untuk pasangan BY, $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 2 \\ 25 \end{bmatrix} = \begin{bmatrix} 52 \\ 75 \end{bmatrix}$ mod 26
= $\begin{bmatrix} 0 \\ 23 \end{bmatrix}$, jadi pasangan BY menghasilkan sandi ZW.

Untuk pasangan ED, $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 5 \\ 4 \end{bmatrix} = \begin{bmatrix} 13 \\ 12 \end{bmatrix}$ mod 26
= $\begin{bmatrix} 13 \\ 12 \end{bmatrix}$, jadi pasangan ED menghasilkan sandi ML.

Untuk pasangan AY, $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 1 \\ 25 \end{bmatrix} = \begin{bmatrix} 51 \\ 75 \end{bmatrix}$ mod 26
= $\begin{bmatrix} 25 \\ 23 \end{bmatrix}$, jadi pasangan AY menghasilkan sandi YW.

Untuk pasangan SS, $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 19 \\ 19 \end{bmatrix} = \begin{bmatrix} 57 \\ 57 \end{bmatrix}$ mod 26
= $\begin{bmatrix} 5 \\ 5 \end{bmatrix}$, jadi pasangan SS menghasilkan sandi EE.

Akhirnya, diperoleh teks sandi : *KSWLZWMLYWEE*.

D. Kriptografi dengan Menggunakan Matriks (Dekripsi)

Dari proses enkripsi diatas, apabila kondisinya dibalik sekarang kita memiliki teks sandi *KSWLZWMLYWEE* dan matriks kuncinya adalah tetap matriks A. Kita dapat men-dekripsi ulang teks sandi tersebut dengan cara mengelompokkan nya menjadi kelompok alfabet beranggotakan 2 huruf, hanya saja matriks A harus diubah menjadi matriks invers nya. Karena dalam pengerjaan kriptografi banyak menggunakan modulo, maka untuk mendapatkan invers dari matriks *key* kita akan menggunakan metode invers matriks modulo.

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

Pertama kita akan mencari determinan matriks A :

$|A| = (1 * 3) – (2 * 0) = 3$

Invers modulo :

3^{-1} mod 26 ≡ 3x = 1 + 26k, diperoleh

$x = \frac{1+26k}{3}$

untuk k = 1, diperoleh x = 9. Artinya invers dari 3 mod 26 ekuivalen dengan 9 mod 26.
Sehingga :

$A^{-1} = 9 \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix}$ mod 26

$A^{-1} = \begin{bmatrix} 27 & -18 \\ 0 & 9 \end{bmatrix}$ mod 26

$A^{-1} = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}$

Setelah mendapat matriks invers, proses yang sama dengan enkripsi kita ulangi. Maka akan didapatkan *plain text* semula. Sebagai contoh, kita akan mendekripsi ulang "GOOD BYE DAYS" pada contoh sebelumnya.
Hasil enkripsi : *KSWLZWMLYWEE*

KS	WL	ZW	ML	YW	EE
11 19	23 12	0 23	13 12	25 23	5 5

Untuk pasangan KS, $\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 11 \\ 19 \end{bmatrix} = \begin{bmatrix} 163 \\ 171 \end{bmatrix}$ mod 26
$= \begin{bmatrix} 7 \\ 15 \end{bmatrix}$, jadi KS menghasilkan *plain text* GO

Untuk pasangan WL, $\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 23 \\ 12 \end{bmatrix} = \begin{bmatrix} 119 \\ 108 \end{bmatrix}$ mod 26
$= \begin{bmatrix} 15 \\ 4 \end{bmatrix}$, jadi WL menghasilkan *plain text* OD

Untuk pasangan ZW, $\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 0 \\ 23 \end{bmatrix} = \begin{bmatrix} 184 \\ 207 \end{bmatrix}$ mod 26
$= \begin{bmatrix} 2 \\ 25 \end{bmatrix}$, jadi ZW menghasilkan *plain text* BY

Untuk pasangan ML, $\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 13 \\ 12 \end{bmatrix} = \begin{bmatrix} 109 \\ 108 \end{bmatrix}$ mod 26
$= \begin{bmatrix} 5 \\ 4 \end{bmatrix}$, jadi pasangan ML menghasilkan *plain text* ED

Untuk pasangan YW, $\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 25 \\ 23 \end{bmatrix} = \begin{bmatrix} 209 \\ 207 \end{bmatrix}$ mod 26
$= \begin{bmatrix} 1 \\ 25 \end{bmatrix}$, jadi YW menghasilkan *plain text* AY

Untuk pasangan EE, $\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 45 \\ 45 \end{bmatrix}$ mod 26
$= \begin{bmatrix} 19 \\ 19 \end{bmatrix}$, jadi EE menghasilkan *plain text* SS

Jadi *plain text* yang kita dapatkan dari proses dekripsi diatas adalah "GOOD BYE DAYS". Karena hurruf S terakhir adalah *dummy* maka kita buang untuk menghasilkan *plain text* yang benar.

IV. KESIMPULAN

Matriks mempunyai banyak fungsi baik dalam matematika maupun cabang ilmu pengetahuan yang lain untuk memudahkan perhitungan. Dalam Kriptografi khususnya dalam *Hill Cipher* , matriks berguna dalam proses dekripsi maupun enkripsi pesan rahasia. Dengan kombinasi transformasi matriks, invers dan operasi pada matriks, dapat dibuat berbagai kombinasi *key*. Tidak hanya pesan teks, pesan multimedia seperti gambar pun dapat di-*encode* dengan bantuan matriks. Inti dari *Hill Cipher* adalah, memecah alfabet menjadi kelompok kecil dengan 2 anggota lalu menkonversinya ke vektor kolom dan ditransformasi dengan matriks *key* yang dipersiapkan. Dalam proses dekripsi, prosesnya agak berbeda sedikit karena matriks *key* harus di-invers terlebih dahulu sebelum dilakukan transformasi ke *plain text* .

VI. UCAPAN TERIMA KASIH

Penulis mengucap syukur dan berterima-kasih kepada Tuhan Yang Maha Esa karena atas berkat dan karunia-Nya penulis dapat menyelesaikan makalah ini tanpa menemui masalah yang berarti.

Penulis juga mengucapkan terima kasih kepada bapak Dr.Ir. Rinaldi Munir, MT. dan bapak Drs. Judhi Santoso, M.Sc sebagai dosen pengajar dan pembimbing mata kuliah IF 2123 Aljabar Geometri, Program Studi Teknik Informatika, Institut Teknologi Bandung yang telah memberikan pengetahuan yang sangat bermanfaat bagi penulis dalam menyelesaikan makalah ini.

REFERENSI

[1] Munir, Rinaldi, *Matematika Diskrit*. Bandung: Percetakan ITB,2006.

[2] Lester S. Hill, Cryptography in an Algebraic Alphabet, *The American Mathematical Monthly* Vol.36, June–July 1929, pp. 306–312.

[3] Vince, John, *Geometric Algebra For Computer Graphics*. Springer

[4] http://practicalcryptography.com/ciphers/hill-cipher/ diakses tanggal 11 Desember 2015, Pukul 23.01.

[5] http://crypto.interactive-maths.com/hill-cipher.html diakses tanggal 11 Desember 2015, Pukul 23.34.

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, 11 Desember 2015

ttd

Varian Caesar
13514041