Transformasi Linier dalam Metode Enkripsi Hill-*Cipher*

Muhammad Reza Ramadhan - 13514107
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
rezaramadhan.m@students.itb.ac.id

***Abstract*—Metode Enkripsi klasik yang tidak mudah dipecahkan adalah Hill-cipher, ini disebabkan adanya penggunaan matriks tertentu yang menyebabkan suatu karakter tidak selalu berubah menjadi karakter yang sama. Pada makalah ini akan dibahas mengenai teori dasar yang digunakan dalam Hill-cipher, pengertian dari enkripsi, proses perubahan *plaintext* menjadi *ciphertext* secara detail pada Hill-cipher, serta pembahasan mengenai kelebihan dan kekurangan Hill-chiper.**

***Kata Kunci*—Enkripsi, Hill-cipher, matriks, tranformasi linear, vektor.**

I. PENDAHULUAN

Keamanan informasi adalah suatu hal yang telah menjadi sebuah hal penting pada beberapa tahun belakangan ini. Keberjalanan informasi penting dan rahasia melalui layanan internet sudah menjadi hal biasa yang sering terjadi dalam kehidupan sehari-hari. Untuk menjaga agar informasi rahasia tersebut tidak mudah dicapai oleh sembarang manusia, terdapat sebuah teknik untuk mengubah informasi tersebut menjadi data tertentu yang tidak bisa dipahami oleh sembarang manusia.

Teknik untuk mengubah informasi yang ada menjadi informasi yang tidak mudah dipahami oleh orang lain biasa disebut dengan enkripsi data. Terdapat banyak metode dalam enkripsi data tersebut, salah satunya adalah sebuah metode yang disebut Hill-*cipher*. Hill-*cipher* adalah metode yang menggunakan dasar-dasar matriks dan transformasi linear. Metode ini memiliki beberapa kelebihan dan kekurangan dibandingkan dengan metode lain, salah satu kelebihannya adalah bahwa setiap huruf yang dienkripsi tidak berubah menjadi huruf lain yang sama seperti pada metode Caesar-*cipher*.

II. DASAR TEORI

A. Matriks

Secara sederhana, matriks dapat didefinisikan sebagai kumpulan bilangan yang disusun dalam kolom dan baris tertentu[3]. Dalam penyajian matriks, elemen dengan kolom ke-q dan baris ke-p biasa disebut dengan $a_{p,q}$. Selain itu, matriks dengan jumlah kolom m dan jumlah baris n biasa disebut matriks m x n. Berikut adalah contoh penyajian matriks dengan jumlah kolom m dan baris n:

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}$$

Dalam keilmuan Teknik Informatika, matriks biasa direpresentasikan sebagai array dua dimensi, yaitu dimana array baris memiliki array kolom didalamnya.

Pada matriks persegi, yaitu matriks yang memiliki banyaknya kolom dan baris yang sama, terdapat sebuah bilangan yang disebut determinan. Determinan adalah sebuah bilangan yang mempunyai banyak informasi mengenai matriks tersebut. Salah satu informasi yang terdapat pada determinan suatu matriks adalah apakah suatu matriks memiliki invers atau tidak.

Determinan suatu matriks dapat dicari dengan menggunakan teknik kofaktor, yaitu jika terdapat matriks

$$M = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}$$

Maka determinannya adalah

$$\det(\mathrm{M}) = a_{1,m}\det(m_{1,m}) + a_{2,m}\det(m_{2,m}) + \cdots + a_{n,m}\det(m_{n,m})$$

Dengan $m_{p,q}$ adalah matriks minor baris ke-p dan kolom ke-q, yaitu bagian dari matriks M yang telah dihilangkan baris ke-p dan kolom ke-q. Terlihat bahwa definisi fungsi detereminan matriks tersebut rekursif. Basis dari fungsi itu adalah bahwa determinan dari matriks 1x1 adalah elemen ke-1,1.

Pada matriks berlaku operasi perkalian, penjumlahan, dan pengurangan. Pada perkalian matriks, jika terdapat matriks A, X dan I, dengan I adalah matriks identitas yang isinya adalah angka 1 pada diagonal utama dan 0 pada elemen lainnya, sedemikian sehingga

$$AX = I$$

maka X dapat disebut sebagai invers dari matriks A atau biasa dituliskan A^{-1}.

Untuk mencari inverse dari suatu matriks, perlu dipastikan terlebih dahulu bahwa determinan dari matriks tersebut tidak sama dengan nol, karena jika suatu matriks memiliki determinan 0 maka matriks tersebut tidak memiliki invers.

Untuk mencari invers dari suatu matriks, cara yang dapat

dilakukan adalah:

$$A^{-1} = \frac{1}{\det(A)} adj(A)$$

dengan adj(A) adalah adjoin dari matriks A yang dinyatakan dengan

$$adj(A) = C^T$$

yaitu traspos dari matriks kofaktor dari A. Kofaktor dari matriks A dapat dinyatakan:

$$C = \begin{pmatrix} \det(m_{1,1}) & \det(m_{1,2}) & \cdots & \det(m_{1,m}) \\ \det(m_{2,1}) & \det(m_{2,2}) & \cdots & \det(m_{2,m}) \\ \vdots & \vdots & \ddots & \vdots \\ \det(m_{n,1}) & \det(m_{n,1}) & \cdots & \det(m_{n,m}) \end{pmatrix}$$

B. Transformasi Linear

Secara sederhana, transformasi linear dapat dinyatakan sebagai sebuah fungsi yang dapat merubah sebuah vektor ***v*** menjadi sebuah vektor baru ***w***. Kedua vektor ***v*** dan ***w*** tersebut dapat berupa vektor dalam ruang vektor yang sama ataupun beberapa vektor dalam ruang vektor yang berbeda.

Transformasi lanjar sendiri biasa dinyatakan dalam notasi ***T(v)***, dimana T adalah sebuah fungsi yang dapat merubah vektor ***v*** menjadi vektor baru.

Sebuah transformasi dapat dinyatakan sebagai transformasi lanjar apabila dalam transformasi tersebut berlaku dua syarat, yaitu

1. $T(\boldsymbol{v} + \boldsymbol{w}) = T(\boldsymbol{v}) + T(\boldsymbol{w})$
2. $T(c\boldsymbol{v}) = cT(\boldsymbol{v})$

Dengan dua syarat sederhana diatas, kita dapat menentukan bahwa salah satu teknik transformasi yang adalah dengan mengalikan sebuah matriks pada vektor yang ada. Apabila sebuah matriks A dikalikan dengan vektor ***v***, maka hasilnya adalah sebuah vektor baru. Penggunaan matriks sebagai salah satu alternatif transformasi linier dapat dibuktikan dengan:

1. $A(\boldsymbol{v} + \boldsymbol{w}) = A\boldsymbol{v} + A\boldsymbol{w}$
2. $A(cv) = cA(\boldsymbol{v})$

C. Enkripsi

Enkripsi data sudah dikenal oleh umat manusia sejak tahun 1900 SM, yang digunakan oleh bangsa mesir dalam penggunaan hieroglif yang berbeda dari hieroglif biasa untuk menyembunyikan makna yang sebenarnya dari suatu tulisan rahasia.

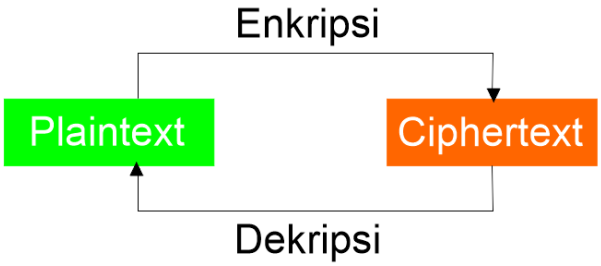
Enkripsi berasal dari bahasa Yunani kryptos yang berarti tersembunyi atau rahasia (Rouse, techtarget.com). Secara sederhana enkripsi adalah proses merubah data sedemikian rupa sehingga data tersebut tidak mudah dibaca oleh sembarang orang. Tidak sedikit jenis enkripsi yang ada di dunia ini, mulai dari enkripsi paling sederhana yaitu mengubah suatu alfabet menjadi simbol aneh seperti sandi morse, menggeser setiap alfabet sekian kali sehingga menjadi alfabet baru, mesin Enigma yang digunakan oleh tentara Nazi pada Perang Dunia kedua, hingga algoritma RSA yang banyak digunakan oleh bank-bank di seluruh dunia untuk mengenkripsi data nasabahnya.

Selain enkripsi, terdapat pula yang disebut dekripsi yaitu proses pengembalian data yang telah dienkripsi menjadi data biasa yang dapat dibaca oleh semua orang. Proses dekripsi ini menggunakan algoritma yang merupakan kebalikan dari algoritma enkripsi. Contohnya adalah pada algoritma penggeseran alfabet, maka untuk mendekripsi hal tersebut maka diperlukan penggeseran kebalikan dari penggeseran yang dilakukan diawal.

Data awal yang belum dienkripsi biasa disebut plaintext, sedangkan data akhir yang telah dienkripsi biasa disebut ciphertext. Algoritma-algoritma yang digunakan untuk merubah plaintext ini menjadi ciphertext sendiri lah yang membuat dunia enkripsi menjadi sangat beragam.

Pada dunia ilmu komputasi terdapat sebuah cabang ilmu bernama kriptografi, yaitu ilmu yang mempelajari cara menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna (Munir, 2006:V-21).

Berikut adalah ilustrasi mengenai proses perubahan informasi pada alur enkripsi-dekripsi:



Gambar 2.1: Ilustrasi Enkripsi-Dekripsi

Salah satu contoh aplikasi enkripsi pada kehidupan sehari-hari adalah enkripsi pada program televisi yang disebar oleh penyedia televisi kabel. Sebelum data program televisi tersebut disebar, program televisi tersebut dienkripsi dengan cara tertentu. Setelah data terenkripsi tersebut diterima oleh pelanggan, *decoder* milik masing-masing pelanggan yang telah dibeli sebelumnya akan mendekripsi sinyal terenkripsi tadi sehingga program televisi tersebut bisa disaksikan kembali oleh pelanggan.

III. HILL-CIPHER

Hill-*cipher* diciptakan oleh Lester S. Hill pada tahun 1929 sebagai salah satu metode enkripsi yang berdasarkan pada teori-teori pada aljabar linear. Untuk merubah *plaintext* menjadi *ciphertext* dan sebaliknya, Hill menggunakan teori transformasi linear untuk merubah suatu vektor menjadi vektor lain, untuk mendekripsi kembali vektor tersebut, ia menggunakan invers dari transformasi tersebut.

Hill-*cipher* menggunakan *key* enkripsi berupa sebuah matriks persegi. Ia memanfaatkan salah satu teknik transformasi linear yaitu menggunakan matriks tertentu untuk merubah sebuah *plaintext* menjadi *ciphertext.* Secara singkat, syarat untuk matriks yang bisa digunakan dalam Hill Cipher ini adalah:

1. Merupakan matriks persegi
2. Determinan dari matriks tersebut tidak sama dengan

0. Hal ini bertujuan agar matriks memiliki invers yang akan digunakan pada dekripsi pesan.

A. *Enkripsi pada Hill Cipher*

Setelah menentukan sebuah matriks persegi *nxn* untuk menjadi kunci pada teknik enkripsi ini, hal pertama yang dilakukan pada metode Hill-Cipher ini adalah merubah input yang ada menjadi bilagan sesuai kode tertentu, cara paling sederhana adalah dengan menggunakan 1 sebagai A, 2 sebagai B, dan selanjutnya hingga 26 berarti Z.

Langkah berikutnya adalah memecahkan input menjadi beberapa buah vektor dengan n elemen. Jika input yang diterima memiliki jumlah yang tidak habis dibagi n, maka sisa dari input tersebut ditambah dengan elemen *dummy*.

Setelah itu, dilakukan transformasi linear standar antara setiap vektor yang ada dengan matriks kunci. Setelah itu, setiap hasil transformasi dilakukan operasi modulus pada setiap elemen vektornya. Hal ini bertujuan untuk mengubah bilangan yang lebih besar dari kode yang tersedia – misalnya didapat 47 dari 26 kode huruf yang ada – agar bisa menjadi alfabet yang tersedia kembali.

Contoh dari penerapan hill Cipher ini pada kalimat AKU ADALAH REZA dengan key = $\begin{pmatrix}5 & 7\\ 8 & 11\end{pmatrix}$ adalah:

1. Merubah semua karakter menjadi angka yang sesuai, yaitu dengan metode A = 1, B = 2, dan seterusnya, maka AKU = 1 11 21, ADALAH = 1 4 1 12 1 8, REZA = 18 5 26 1. Sehingga kode akhirnya adalah 1 11 21 1 4 1 12 1 8 18 5 26 1. Selain itu, karakter spasi tidak dianggap ada pada contoh ini.
2. Memecah kode tersebut menjadi vektor dengan dua elemen:
$$v1 = \begin{pmatrix}1\\12\end{pmatrix}\ v2 = \begin{pmatrix}21\\1\end{pmatrix}\ v3 = \begin{pmatrix}4\\1\end{pmatrix}$$
$$v4 = \begin{pmatrix}12\\1\end{pmatrix}\ v5 = \begin{pmatrix}8\\18\end{pmatrix}\ v6 = \begin{pmatrix}5\\26\end{pmatrix}$$
$$v7 = \begin{pmatrix}1\\0\end{pmatrix}$$
Pada vektor terakhir, karena hanya tersisa satu huruf maka elemen kedua diisi dengan *dummy*. Nilai *dummy* bisa berubah menjadi berapapun selama tidak sama dengan salah satu kode di pengubahan huruf menjadi angka. Pada contoh ini, penulis menggunakan 0 sebagai *dummy*.
3. Mentransformasi setiap vektor tersebut menjadi vektor baru dengan transformasi geometri yaitu $\boldsymbol{w} = A\boldsymbol{v}$, sehingga vektor barunya menjadi:
$$w1 = \begin{pmatrix}89\\140\end{pmatrix}\ w2 = \begin{pmatrix}112\\179\end{pmatrix}\ w3 = \begin{pmatrix}21\\43\end{pmatrix}$$
$$w4 = \begin{pmatrix}67\\107\end{pmatrix}\ w5 = \begin{pmatrix}65\\262\end{pmatrix}\ w6 = \begin{pmatrix}207\\326\end{pmatrix}$$
$$w7 = \begin{pmatrix}5\\0\end{pmatrix}$$
4. Memberikan operasi mod 26 pada setiap elemen vektor tersebut sehingga menjadi
$$w1 = \begin{pmatrix}11\\10\end{pmatrix}\ w2 = \begin{pmatrix}8\\23\end{pmatrix}\ w3 = \begin{pmatrix}21\\17\end{pmatrix}$$
$$w4 = \begin{pmatrix}15\\3\end{pmatrix}\ w5 = \begin{pmatrix}13\\2\end{pmatrix}\ w6 = \begin{pmatrix}25\\14\end{pmatrix}$$
$$w7 = \begin{pmatrix}5\\0\end{pmatrix}$$
5. Mengubah kembali menjadi huruf yang bersesuaian.

Pada contoh ini, AKU ADALAH REZA setelah dilakukan enkripsi metode Hill Cipher berubah menjadi KJHWUQOCMBYNE.

B. *Dekripsi pada Hill Cipher*

Proses dekripsi pada Hill Cipher ini sangat sederhana. Yang membedakannya dengan proses enkripsi hanyalah key yang digunakan adalah inverse dari matriks yang digunakan sebagai key pada tahap enkripsi.

Pada contoh enkripsi digunakan key = $\begin{pmatrix}5 & 7\\ 8 & 11\end{pmatrix}$ sehingga key yang digunakan pada proses dekripsi ini adalah $\begin{pmatrix}-11 & 7\\ 8 & -5\end{pmatrix}$ Contoh untuk dekripsi KJHWUQOCMBYNE adalah sebagai berikut:

1. Merubah setiap huruf menjadi angka yang bersesuaian, sehingga KJHWUQOCMBYNE berubah menjadi 11 10 8 23 21 17 15 3 13 2 25 14 5 0.
2. Mengubah bentuk tersebut menjadi beberapa vektor dengan jumlah elemen dua:
$$v1 = \begin{pmatrix}11\\10\end{pmatrix}\ v2 = \begin{pmatrix}8\\23\end{pmatrix}\ v3 = \begin{pmatrix}21\\17\end{pmatrix}$$
$$v4 = \begin{pmatrix}15\\3\end{pmatrix}\ v5 = \begin{pmatrix}13\\2\end{pmatrix}\ v6 = \begin{pmatrix}25\\14\end{pmatrix}$$
$$v7 = \begin{pmatrix}5\\0\end{pmatrix}$$
3. Mengubah menjadi vektor baru $\boldsymbol{w}$ dengan $\boldsymbol{w} = A\boldsymbol{v}$
$$w1 = \begin{pmatrix}-51\\38\end{pmatrix}\ w2 = \begin{pmatrix}73\\-51\end{pmatrix}\ w3 = \begin{pmatrix}-112\\83\end{pmatrix}$$
$$w4 = \begin{pmatrix}-144\\105\end{pmatrix}\ w5 = \begin{pmatrix}-129\\94\end{pmatrix}\ w6 = \begin{pmatrix}-177\\130\end{pmatrix}$$
$$w7 = \begin{pmatrix}-55\\0\end{pmatrix}$$
4. Memberikan operasi modulo pada setiap elemen vektor.
$$w1 = \begin{pmatrix}1\\12\end{pmatrix}\ w2 = \begin{pmatrix}21\\1\end{pmatrix}\ w3 = \begin{pmatrix}4\\1\end{pmatrix}$$
$$w4 = \begin{pmatrix}12\\1\end{pmatrix}\ w5 = \begin{pmatrix}8\\18\end{pmatrix}\ w6 = \begin{pmatrix}5\\26\end{pmatrix}$$
$$w7 = \begin{pmatrix}1\\0\end{pmatrix}$$
5. Mengubah menjadi *plaintext* yang sebenarnya, yaitu 1 11 21 1 4 1 12 1 8 18 5 26 1 bersesuaian dengan AKUADALAHREZA.

III. ANALISIS KELEBIHAN DAN KELEMAHAN

A. *Kelebihan*

Salah satu kelebihan dari algoritma ini adalah bahwa beberapa karakter yang sama tidak selalu diubah menjadi karakter baru yang sama. Contohnya adalah pada perubahan AKUADALAHREZA menjadi KJHWUQOCMBYNE terlihat bahwa karakter pertama dan keempat pada *plaintext* sama yaitu A, sedangkan pada *ciphertext* yang dibuat berbeda, yaitu karakter pertama K dan karakter keempat W. Hal ini membuat orang lain yang

berusaha memecahkan kode ini mengalami kesulitan jika ia tidak tahu metode apa yang digunakan untuk melakukan enkripsi.

Selain itu, terdapat banyak sekali kemungkinan kunci yang diambil. Sebagai contoh saja, jika kita menggunakan matriks 3x3 dengan setiap elemen kunci paling kecil adalah 1 dan paling besar adalah 26, maka terdapat 26^9 kemungkinan yang ada, atau sekitar $5{,}4x10^{12}$ kemungkinan. Jika kita mengurangi nilai tersebut dengan asumsi dari semua kemungkinan tersebut terdapat 10% matriks yang tidak memiliki invers sehingga tidak bisa dipakai, maka total kemungkinan yang ada masih sangat besar, yaitu $4{,}8x10^{12}$.

Kelebihan lainnya adalah key yang diambil bisa merupakan matriks persegi ukuran berapapun, dengan demikian pemecah kode akan sulit menentukan "pemotongan" dari data terenkripsi tersebut.

Metode Hill-chipher ini juga bisa dikombinasikan dengan menggunakan matriks key dengan ukuran yang berbeda. Sebagai contoh misalnya enkripsi pertama dilakukan dengan matriks berukuran 15x15, setelah itu, ciphertext hasil enkripsi bisa dienkripsikan lagi dengan matriks berukuran 28x28. Proses ini akan memakan waktu yang lebih lama, namun akan mempersulit seorang pemecah kode karena proses ini dapat diulang berkali-kali dengan matriks yang berbeda.

Tetapi jika pengombinasian key matriks diatas dilakukan dengan matriks berukuran sama maka tidak akan berpengaruh sama sekali terhadap kesulitan pemecah kode dalam mencari matriks key, karena pemecah kode hanya perlu mencari sebuah matriks yang merupakan hasil perkalian dari dua matriks yang dikombinasikan tersebut. Hal ini dapat terlihat dengan:

$$\boldsymbol{w} = A\boldsymbol{v} \ldots (\mathbf{1})$$
$$\boldsymbol{y} = B\boldsymbol{w} \ldots (\mathbf{2})$$

substitusi persamaan (1) ke persamaan (2)

$$\boldsymbol{y} = BA\boldsymbol{v}$$

jika BA adalah matriks dengan ukuran yang sama, maka kita bisa mengganti BA adalah sebuah matriks baru C maka

$$\boldsymbol{y} = C\boldsymbol{v}$$

Terlihat bahwa proses kombinasi dua matriks dengan ukuran yang sama tidak ada bedanya dengan menggunakan satu buah matriks saja.

B. Kekurangan

Karena hill cipher menggunakan matriks tertentu, pemecah kode dapat mencari setiap elemen dari matriks *key* tersebut dengan menggunakan metode persamaan linear biasa. Syarat utama agar matriks key tersebut bisa dicari adalah jika pemecah kode memiliki pasangan *ciphertext* dan *plaintext* sebanyak n^2. Mencari setiap elemen matriks dengan persamaan linear memang merupakan hal yang melelahkan jika dilakukan secara manual, namun jika hal ini dilakukan menggunakan komputer dengan menggunakan program tertentu, proses pencarian bisa dilakukan dalam waktu yang singkat. Kelemahan utama dari teknik ini adalah bahwa pemecah kode harus mengetahui terlebih dahulu berapa ukuran dari matriks key.

Teknik *bruteforce*, yaitu mencoba semua kemungkinan dari matriks *key* bisa dilakukan dengan teknik ini, namun seperti yang pernah dibahas sebelumnya diketahui bahwa terlalu banyak kemungkinan *key* yang bisa digunakan serta fakta bahwa ukuran dari matriks yang dijadikan key juga bisa menjadi berapapun menyebabkan jika teknik bruteforce ini dilakukan, maka akan diperlukan waktu yang lama untuk menemukan matriks key yang cocok.

Metode Hill Cipher ini memang bisa menghasilkan output enkripsi yang berbeda untuk beberapa huruf yang sama. Tapi, diketahui bahwa dengan menggunakan input vektor yang sama, akan dihasilkan juga output vektor yang sama juga. Sebagai contoh, setiap vektor yang merepresentasikan AK akan berubah menjadi KJ pada enkripsi dengan key = $\begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix}$.

Hal ini akan menjadi berbahaya jika kita berusaha mengenkripsi sebuah gambar yang memiliki kontras warna yang jelas antara satu bagian gambar dengan gambar yang lainnya. Sebagai contoh, jika kita menggunakan metode Hill-Cipher untuk mengenkripsi logo Nike berikut

Gambar 3.1: Logo Nike sebelum dienkripsi.
Sumber: [6]

Maka karena terdapat banyak sekali komponen vektor yang mirip pada setiap warna putih dan hitam di gambar tersebut maka metode Hill Cipher tidak akan banyak berguna karena setiap vektor yang merepresentasikan warna putih akan diganti menjadi vektor baru yang akan merepresentasikan warna tertentu, begitupun untuk vektor yang merepresentasikan warna hitam. Untuk ilustrasi, hasil enkripsi Gambar 3.1 diatas akan menjadi

Gambar 3.2: Logo Nike setelah dienkripsi.
Sumber: [6]

Terlihat bahwa logo Nike tidak benar-benar tersembunyi pada hasil enkripsi tersebut.

IV. KESIMPULAN

Enkripsi Hill-cipher adalah sebuah metode enkripsi yang pertama kali ditemukan 86 tahun yang lalu. Metode ini memang tidak bisa dibandingkan dengan metode enkripsi modern seperti *Block Cipher* atau *Stream Cipher*, namun terlihat bahwa Hill *Cipher* ini jauh lebih baik jika dibandingkan dengan metode enkripsi sangat klasik seperti Caesar *Cipher*.

Hill Cipher ini memang masih rentan terhadap beberapa metode serangan kriptografi seperti known-plaintext attack, dimana pemecah kode mencari beberapa kata umum yang mungkin telah diubah menjadi pesan terenkripsi tertentu.

DAFTAR PUSTAKA

[1] Strang, Gilbert. *Introduction to Linear Algebra*. Wellesley – Cambridge Press. 2009. Wellesley, USA.

[2] Ramadhan, Muhammad Reza. 2015. *Aplikasi Enkripsi Sederhana untuk Penyimpanan Database Password*. Matematika Diskrit – Sem. I Tahun 2015/2016. Bandung: Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

[3] Definition of Matrix http://chortle.ccsu.edu/vectorlessons/vmch13/vmch13_2.html diakses pada 13 Desember 2015

[4] Practical Cryptography – Hill Cipher http://practicalcryptography.com/ciphers/hill-cipher/ diakses pada 10 Desember 2015

[5] Hill Cipher – Crypto Corner http://crypto.interactive-maths.com/hill-cipher.html diakses pada 11 Desember 2015

[6] Doyle, Ryan. *Hill's Cipher: Linear Algebra in Cryptography*. https://rctechnical.files.wordpress.com/2014/09/r_doyle_hill-cipher.pdf diakses pada 10 Desember 2015

PERNYATAAN

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

Bandung, 13 Desember 2015

Muhammad Reza Ramadhan
13514107