Aplikasi Aljabar Lanjar untuk Penyelesaian Persoalan Kriptografi dengan Hill *Cipher*

Nursyahrina - 13513060
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13513060@std.stei.itb.ac.id

***Abstract*—Aljabar lanjar adalah salah satu bahasan dalam mata kuliah Aljabar Geometri. Aljabar lanjar atau yang biasa disebut pula dengan Aljabar linier membahas diantaranya konsep sistem persamaan lanjar, matriks, trnasformasi lanjar, aturan bebas lanjar, dan lain-lain. Konsep-konsep aljabar lanjar ini dapat digunakan untuk menyelesaikan berbagai persoalan diantaranya persoalan kriptografi, analisis jaringan, rangkaian listrik, strategi game, interpolasi, grafik komputer, dan masih banyak aplikasi lainnya yang sangat bermanfaat dalam kehidupan sehari-hari. Pada makalah ini akan dibahas aplikasi aljabar lanjar untuk pernyelesaian persoalan kriptografi dengan Hill-cipher**

***Keywords*—aljabar lanjar, hill-cipher, kriptografi, matriks, mod, transformasi**

I. PENDAHULUAN

Sebuah pesan adalah data atau informasi yang dapat dimengerti dan memiliki makna. Pesan ini dapat berupa teks, gambar, suara (*audio*), *video*, dll. Dalam penggunaan secara luas, ada pesan yang harus dikirimkan, *hardcopy* melalui pos, kurir, maupun *softcopy*-nya melalui internet, atau saluran komunikasi lainnya. Untuk penggunaan berulang-ulang dan dalam waktu lama, penyimpanan dari pesan juga harus diperhatikan. Dalam pengiriman dan penyimpanan data ini, sering muncul masalah keamanan data. Data atau informasi pada pesan yang apa adanya (tidak dilindungi atau disandikan) akan mudah bocor ke pihak lain. Bagi organisasi, pemerintahan, atau perusahaan, masalah security data adalah hal yang sangat krusial, karena menyangkut rahasia organisasi, bisnis, bahkan negara. Oleh karena itu diperlukan metode untuk mengamankan data atau informasi pada pesan tersebut. Caranya adalah dengan menerapkan konsep kriptografi, mengubah pesan menjadi kode yang sudah tidak bermakna dan sulit untuk dipecahkan.

II. PENGENALAN KRIPTOGRAFI

A. Terminologi Kriptografi

Kriptografi adalah studi tentang *encoding* dan *decoding* pesan rahasia. Dalam terminologi kriptografi, pesan yang belum disandikan disebut dengan *plaintext*. Pesan yang sudah disandikan dan tidak bermakna lagi disebut *ciphertext* atau dikenal juga dengan sebutan kriptogram. Sandi untuk kriptografi disebut *ciphers*. Proses mengubah *plaintext* menjadi *ciphertext* , *encryption* / *enciphering*, sementara proses untuk mengembalikan *ciphertext* menjadi bentuk *plaintext*-nya disebut *decryption* / *deciphering*. *Plaintext* yang sudah diubah kebentuk *ciphertext* harus dapat dikembalikan ke bentuk semula. [1]

B. *Ciphers*

Cipher yang paling sederhana adalah *cipher* substitusi, dimana masing-masing huruf alfabet digantikan dengan huruf lainnya. Misal, A diganti dengan D, B diganti dengan E, C diganti dengan F dan seterusnya. Namun ada kelemahan yang sangat jelas dalam *chiper* subtitusi ini. Penggantian huruf akan selalu sama, maksudnya A akan tetap digantikan dengan D, jadi akan mudah melihat hubungan substitusi diantara huruf-huruf yang ada dan pesan yang ada akan mudah dipecahkan dengan metode statistik. Salah satu cara untuk mengatasi masalah seperti ini adalah dengan menggunakan sistem poligrafik. Sistem Poligrafik adalah adalah sistem dimana *plaintext* dibagi menjadi *n*-set huruf, yang masing-masingnya akan digantikan dengan n-set huruf *cipher*. Ada sebuah sistem poligrafik berbasis transformasi matriks yang disebut *Hill ciphers.* [1]

III. DASAR TEORI

Untuk memahami aplikasi aljabar lanjar untuk penyelesaian masalah kriptografi dengan *Hill ciphers*, perlu terlebih dahulu untuk memahami konsep dasar dari bahasan-bahasan aljabar lanjar yang digunakan dalam proses *encryption* dan *decryption*, diantaranya matriks, eliminasi gauss, aturan bebas lanjar dan transformasi lanjar.

A. Matriks

a. Bentuk Umum Matriks

Matriks adalah kumpulan angka yang disusun dalam

bentuk array berdimensi yang memiliki baris dan kolom. Ukuran matriks ditentukan oleh jumlah baris dan kolom matriks tersebut. Bentuk umum sebuah matriks adalah

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Matriks diatas matriks $A_{m \times n}$ dengan m adalah ukuran baris dan n adalah ukuran kolom dari matriks. Elemen matriks A pada baris ke i dan kolom ke j disebut A[ij]. Berikut beberapa contoh matriks :

$$\begin{bmatrix} 1 & 2 \\ 3 & 0 \\ -1 & 4 \end{bmatrix}, \quad [2 \quad 1 \quad 0 \quad -3], \quad \begin{bmatrix} e & \pi & -\sqrt{2} \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \quad [4]$$

Gambar 1 Contoh-Contoh Matriks
Sumber : Anton, Rorres.2010."*Elementary Linear Algebra Application Version 10th ed*".

b. Operasi pada Matriks

Sebuah matriks dikatakan sama jika memiliki ukuran yang sama dan jenis entri (elemen) yang sama.

1. Penjumlahan dan Pengurangan

   Matriks yang bisa dijumlahkan dan dikurangi adalah yang sama. Penjumlahan dan pengurangan matriks dilakukan dengan menjumlahkan atau mengurangi masing-masing elemen matriks sesuai indeks [ij] nya. Jika dua matriks A dan B didefinisikan sebagai berikut :

$$A = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 4 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 4 & 2 \\ 7 & 4 & 5 \end{bmatrix}$$

   Maka,

$$A + B = \begin{bmatrix} 3 & 6 & 6 \\ 8 & 8 & 10 \end{bmatrix}$$

   dan

$$A - B = \begin{bmatrix} -3 & -2 & 1 \\ -6 & 0 & 0 \end{bmatrix}$$

2. Perkalian Skalar

   Sebuah Matriks A dan bilangan skalar c jika dikalikan, maka hasilnya adalah perkalian c dengan masing-masing elemen matriks A. Misal, sebuah matriks A sebagai berikut :

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

   Maka,

$$cA = \begin{bmatrix} 0 & 6 & 9 \\ 3 & 12 & 15 \end{bmatrix}$$

3. Perkalian Matriks

   Sebuah matriks A dengan ukuran mxr dan matriks B dengan ukuran rxn jika dikalikan maka hasilnya AB adalah matriks dengan ukuran mxn. Misal, dua buah matriks sebagai berikut,

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

   Maka,

$$AB = \begin{bmatrix} (0x1) + (2x2) + (3x1) & (0x2) + (2x3) + (3x3) \\ (1x1) + (4x2) + (5x1) & (1x2) + (4x3) + (5x3) \end{bmatrix}$$

$$AB = \begin{bmatrix} 7 & 15 \\ 14 & 29 \end{bmatrix}$$

4. Determinan Matriks

   Untuk matriks persegi sederhana 2x2 dengan bentuk

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

   mempunyai nilai determinan sebagai berikut :

$$\det(A) = ad - bc$$

   Misal, sebuah matriks A sebagai berikut,

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

   maka,

$$\det(A) = (3x4) - (5x1) = 7$$

5. Invers Matriks

   Untuk matriks persegi sederhana 2x2 dengan bentuk

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

   Invers A yang dinyatakan dengan notasi A^{-1} adalah

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

   Misal matriks A seperti yang dinyatakan pada contoh determinan matriks diatas, Inversnya adalah

$$A^{-1} = \frac{1}{3x4 - 1x5} \begin{bmatrix} 4 & -5 \\ -1 & 3 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 4/7 & -5/7 \\ -1/7 & 3/7 \end{bmatrix}$$

B. Eliminasi Gauss

Metode eliminasi ini dapat digunakan untuk menyelesaikan Sistem Persamaan Lanjar (SPL). Sebelum melakukan proses eliminasi, terlebih dahulu SPL dibuat dalam bentuk matriks augmented dan diubah menjadi matriks eselon atau matriks eselon tereduksi dengan Operasi Baris Elementer (OBE).

Matriks eselon memiliki sifat-sifat sebagai berikut :

1. jika sebuah baris titdak seluruhnya nol, maka bilangan tak nol pertama adalah satu yang disebut satu utama,
2. jika ada baris yang seluruhnya nol, maka didapatkan pada bagian bawah,
3. pada dua baris berurutan, maka nilai satu utama pada baris yang lebih bawah, posisinya lebih ke kanan dari pada satu utama baris yang lebih tinggi.

Matriks eselon tereduksi memiliki sifat-sifat matriks eselon, namun sebuah kolom pada matriks eselon tereduksi yang memiliki satu utama, memiliki nol di tempat yang lain. Hal ini berarti kolom tersebut hanya terdiri dari satu utama dan sisanya adalah nol. Matriks augmented diubah menjadi kedua jenis matriks ini menggunakan Operasi Baris Elementer (OBE) sebagai berikut :

1. mengalikan sebuah baris dengan konstanta tidak nol,
2. mempertukarkan dua buah baris,
3. menjumlahkan sebuah baris dengan k kali baris yang lain.

Setelah terbentuk matriks eselon, dilakukan substitusi mundur terhadap SPL yang telah disederhanakan, maka didapatkan solusi untuk sistem persamaan tersebut. Proses ini disebut Eliminasi Gauss. Jika OBE dilanjutkan sehingga membentuk matriks eselon tereduksi, maka akan langsung didapatkan solusi sistem persamaan, tanpa harus melakukan substitusi. Proses ini disebut Eliminasi Gauss-Jordan.

C. Aritmatika Modular

Jika dalam kriptografi, simbol atau karakter yang digunakan untuk pesan rahasia adalah huruf alfabet, maka ada pembatasan dalam penggunaan karakter, yaitu sebanyak jumlah huruf alfabet, yaitu 26 buah. Karena itu, ketika berhadapan dengan perhitungan yang melebihi angka 26 (angka 0 merepresentasikan huruf 'Z' seperti pada Table 1, sehingga angka 26 sisa 0 dari pembagian dengan 26 berarti huruf Z), maka penentuan huruf yang digunakan akan bergulir lagi ke huruf A, diukur berdasarkan sisa pembagiannya dengan 26. Konsep ini dalam matematika disebut aritmatika modular. Berikut definisi dan konsep dari aritmatika modular,

- Jika m adalah bilangan bulat positif, dan a dan b bilangan bulat sembarang, maka a disebut ekivalen dengan b modulo m,
  $$a = b \pmod m$$
  jika $a - b$ adalah bilangan bulat kelipatan m.

- Untuk modulus m manapun, dapat dibuktikan, bahwa a ekivalen modulo m, dengan salah satu bilangan berikut 0,1,2,3,...,$m - 1$ yang kemudian disebut sisa a modulo m.
  $$Z_m = \{0,1,2,3,...,m-1\}$$

- Setiap bilangan bukan a bukan nol mempunyai *reciprocal* atau invers perkalian dinotasikan dengan a^{-1} dengan aturan sebagai berikut,
  $$aa^{-1} = a^{-1}a = 1$$

- Jika a adalah bilangan pada set Z_m, maka sebuah bilangan a^{-1} pada set Z_m disebut invers perkalian atau *reciprocal* dari a modulo m jika $aa^{-1} = a^{-1}a = 1 \pmod m$.
- Jika a dan m tidak memiliki faktor prima yang sama, maka a mempunyai invers perkalian dengan modulo m

Misal ditanya berapa invers perkalian dari 3 mod 26. Berdasarkan definisi sebelumnya, pada persoalan ini a = 3. 3 dan 26 tidak memiliki faktor prima yang sama, maka 3 mempunyai invers perkalian dengan modulo m.

$$3x = 1 \ (mod\ 26)$$
$$3 \cdot 9 = 27 = 1 \ (mod\ 26)$$
$$3^{-1} = 9 \ (mod\ 26)$$

Invers perkalian dari 3 mod 26 adalah 9. [1]

Berikut adalah Table invers perkalian lengkap untuk mod 26 yang kemudian akan digunakan dalam kriptografi dengan *Hill ciphers*.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Table 1 Invers Perkalian (*Reciprocal*) mod 26
*Sumber : Anton, Rorres.2010."*Elementary Linear Algebra Application Version 10th ed*".*

IV. *HILL CIPHERS*

Hill ciphers pertama kali diperkenalkan oleh Lester S. Hill melalui dua paper yang berjudul "Cryptography in an Algebraic Alphabet" yang diterbitkan di American Mathematical Monthly edisi ke-36 (Juni-Juli 1929), dan "Concerning Certain Linear Transformation Apparaztus of Cryptography" di American Mathematical Monthly edisi 38 (Maret 1931) [1]

Untuk pembahasan selanjutnya, diasumsikan bahwa semua karakter huruf sebagai *plaintext* dan *ciphertext* dipasangkan dengan nilai angka yang menyatakan posisi masing-masing huruf di alfabet.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
J	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*
10	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*
S	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	
19	*20*	*21*	*22*	*23*	*24*	*25*	*0*	

Table 2 Pasangan Huruf Alfabet dan Angka untuk *Cipher* Sederhana
*Sumber : Anton, Rorres.2010."*Elementary Linear Algebra Application Version 10th ed*".*

A. Enciphering

Langkah-langkah untuk melakukan en*cipher*ing dengan *Hill ciphers* sederhana adalah sebagai berikut :

1. Pilihlah matriks *ciphers* sederhana berukuran 2x2 dengan elemen-elemen berupa integer.
   $$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

2. Kelompokkan *plaintext* menjadi pasangan dua huruf. Untuk *plaintext* dengan jumlah huruf ganjil, tambahkan elemen "dummy" setelah karakter *plaintext* terakhir. Kemudian ubah masing-masing huruf dengan nilai angkanya sesuai Table 1.
3. Buat pasangan *plaintext* misal p1 dan p2 menjadi vektor kolom sebagai berikut,

$$\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

dan hitung perkalian produk A**p**. **p** adalah *plaintext* vector dan A**p** *ciphertext* vector.
4. Ubah masing-masing *ciphertext* vector menjadi huruf alfabetnya sesuai Table 1[1]

Case 1

Sebuah pesan berisi kalimat "I AM HIDING" akan di enkripsi menggunakan Hill *Cipher*.

Solution

1. Memilih matriks *cipher*, misal matriks A sebagai berikut,

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

2. Mengelompokkan *plaintext* menjadi pasangan dua huruf, karena jumlah huruf ganjil, ditambahkan satu huruf dummy 'G'

I A M H I D I N G G
9 1 13 8 9 4 9 14 7 7

3. Mengubah pasangan huruf menjadi *ciphertext* vector dengan mengalikan *plaintext* vector dengan matriks

- $\begin{bmatrix} 2 & 4 \\ 6 & 0 \end{bmatrix}\begin{bmatrix} 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 22 \\ 54 \end{bmatrix}$ atau $\begin{bmatrix} 22 \\ 2 \end{bmatrix}$
- $\begin{bmatrix} 2 & 4 \\ 6 & 0 \end{bmatrix}\begin{bmatrix} 13 \\ 8 \end{bmatrix} = \begin{bmatrix} 58 \\ 78 \end{bmatrix}$ atau $\begin{bmatrix} 6 \\ 0 \end{bmatrix}$
- $\begin{bmatrix} 2 & 4 \\ 6 & 0 \end{bmatrix}\begin{bmatrix} 9 \\ 4 \end{bmatrix} = \begin{bmatrix} 34 \\ 54 \end{bmatrix}$ atau $\begin{bmatrix} 8 \\ 2 \end{bmatrix}$
- $\begin{bmatrix} 2 & 4 \\ 6 & 0 \end{bmatrix}\begin{bmatrix} 9 \\ 14 \end{bmatrix} = \begin{bmatrix} 74 \\ 54 \end{bmatrix}$ atau $\begin{bmatrix} 22 \\ 2 \end{bmatrix}$
- $\begin{bmatrix} 2 & 4 \\ 6 & 0 \end{bmatrix}\begin{bmatrix} 7 \\ 7 \end{bmatrix} = \begin{bmatrix} 42 \\ 42 \end{bmatrix}$ atau $\begin{bmatrix} 16 \\ 16 \end{bmatrix}$

4. Mengubah *ciphertext* vector menjadi bentuk teksnya

22 2 6 0 8 2 22 2 16 16
V B F Z H B V B P P

5. Pesan rahasi diatas setelah dienkripsi menjadi "VBFZHBVBPP"

B. Deciphering

Semua *cipher* yang benar-benar dapat digunakan harus disertai dengan prosedur De*cipher*ing untuk mengembalikan *ciphertext* menjadi *plaintext* asalnya, menggunakan invers (mod 26) dari matriks enkripsinya.

Matriks A dikatakan invertible modulo *m* jika ada matriks B dengan elemen-elemen yang termasuk pada set Z_m dimana

$$AB = BA = I \ (mod\ m)$$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Diperkirakan matriks A invertible modulo 26 dan menggunakan Hill 2-*cipher*. Jika

$$\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

merupakan vektor *plaintext* , maka

$$\boldsymbol{c} = A\boldsymbol{p}\ (mod\ 26)$$

adalah vektor *ciphertext*-nya dan

$$\boldsymbol{p} = A^{-1}\boldsymbol{c}\ (mod\ 26)$$

Maka masing-masing vektor *plaintext*-nya dapat ditentukan dengan mengalikan invers modulo 26 dari matriks A dengan vektor *ciphertext*

Oleh karena itu penting untuk mengetahui matriks yang invertible modulo 26 dan bagaimana menetukan inversnya.

- Matriks A invertible modulo 26 jika dan hanya jika det(A) memiliki invers perkalian atau reciprocal modulo 26. Dengan kata lain det(A) tidak memiliki faktor prima 2 atau 13 (tidak dapat dibagi 2 atau 13).
- Sebuah matriks A ukuran 2x2 memiliki elemen-elemen dalam set Z_{26} dan invertible modulo 26, maka invers modulo dari matriks A adalah

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

dimana $\det(A)^{-1}$ adalah invers perkalian det(A) modulo 26[1]

Case 2

Sebuah pesan kriptograf "NKXCSFOFLQWUWIPB" akan dikembalikan kebentuk *plaintext*nya dengan menggunakan Hill 2-*cipher* dan matriks A sebagai berikut,

$$A = \begin{bmatrix} 1 & 3 \\ 0 & 7 \end{bmatrix}$$

Solution

1. Menetukan invers modulo matriks A. Matriks A invertible karena det(A) = 7 mempunyai invers perkalian mod 26 yaitu 15 (Lihat Table 1).

$$\det(A)^{-1} = 15$$

$$A^{-1} = \det(A)^{-1}\begin{bmatrix} 7 & -3 \\ 0 & 1 \end{bmatrix}\ mod\ 26$$

$$A^{-1} = 15\begin{bmatrix} 7 & -3 \\ 0 & 1 \end{bmatrix}\ mod\ 26$$

$$A^{-1} = \begin{bmatrix} 105 & -45 \\ 0 & 15 \end{bmatrix} \text{ atau } \begin{bmatrix} 1 & 7 \\ 0 & 15 \end{bmatrix}\ mod\ 26$$

2. Mengubah vektor *ciphertext* menjadi vektor *plaintext*.

N K X C S F O F L Q W U W I P B
1411 24 3 19 6 15 6 12 17 23 21 23 9 162

- $\begin{bmatrix} 1 & 7 \\ 0 & 15 \end{bmatrix}\begin{bmatrix} 14 \\ 11 \end{bmatrix} = \begin{bmatrix} 91 \\ 165 \end{bmatrix}$ atau $\begin{bmatrix} 13 \\ 9 \end{bmatrix}$
- $\begin{bmatrix} 1 & 7 \\ 0 & 15 \end{bmatrix}\begin{bmatrix} 24 \\ 3 \end{bmatrix} = \begin{bmatrix} 45 \\ 45 \end{bmatrix}$ atau $\begin{bmatrix} 19 \\ 19 \end{bmatrix}$
- $\begin{bmatrix} 1 & 7 \\ 0 & 15 \end{bmatrix}\begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} 61 \\ 90 \end{bmatrix}$ atau $\begin{bmatrix} 9 \\ 12 \end{bmatrix}$
- $\begin{bmatrix} 1 & 7 \\ 0 & 15 \end{bmatrix}\begin{bmatrix} 15 \\ 6 \end{bmatrix} = \begin{bmatrix} 57 \\ 90 \end{bmatrix}$ atau $\begin{bmatrix} 5 \\ 12 \end{bmatrix}$
- $\begin{bmatrix} 1 & 7 \\ 0 & 15 \end{bmatrix}\begin{bmatrix} 12 \\ 17 \end{bmatrix} = \begin{bmatrix} 131 \\ 255 \end{bmatrix}$ atau $\begin{bmatrix} 1 \\ 21 \end{bmatrix}$

- $\begin{bmatrix}1 & 7\\0 & 15\end{bmatrix}\begin{bmatrix}23\\21\end{bmatrix} = \begin{bmatrix}170\\315\end{bmatrix}$ atau $\begin{bmatrix}14\\3\end{bmatrix}$
- $\begin{bmatrix}1 & 7\\0 & 15\end{bmatrix}\begin{bmatrix}23\\9\end{bmatrix} = \begin{bmatrix}86\\135\end{bmatrix}$ atau $\begin{bmatrix}8\\5\end{bmatrix}$
- $\begin{bmatrix}1 & 7\\0 & 15\end{bmatrix}\begin{bmatrix}16\\2\end{bmatrix} = \begin{bmatrix}30\\30\end{bmatrix}$ atau $\begin{bmatrix}4\\4\end{bmatrix}$

3. Mengubah vektor *plaintext* menjadi *plaintext*nya.
   13 9 1919 9 12 5 12 1 21 14 3 8 5 4 4
   M I S S I L E L A U N C H E D D
4. Pesan rahasia yang ingin disampaikan adalah "MISSILE LAUNCHED"

C. Memecahkan Kode *Hill ciphers*

Kode Hill-*cipher* memungkinkan untuk dipecahkan. Jika kita mengetahui sedikit potongan dari *plaintext* asalnya, misal beberapa huruf awal, maka dapat ditentukan matriks A Hill-*cipher* yang digunakan. Kemudian dari matriks tersebut dapat ditentukan keseluruhan pesan rahasia *plaintext*-nya.

Hal mendasar pada aljabar lanjar bahwa transformasi lanjar ditentukan berdasarkan nilai pada basis. Hal ini menunjukkan jika kita memiliki Hill *n-cipher* dan jika $\mathbf{p}_1$, $\mathbf{p}_2$, $\mathbf{p}_3$, ... adalah vektor *plaintext* bebas lanjar dengan bagian vektor *ciphertext*-nya A$\mathbf{p}_1$, A$\mathbf{p}_2$, A$\mathbf{p}_3$, ... diketahui, maka informasi ini cukup untuk menentukan matiks A dan invers-nya A^{-1}(mod *m*)

- Diketahui $\mathbf{p}_1$, $\mathbf{p}_2$, $\mathbf{p}_3$, ... adalah vektor *plaintext* bebas lanjar dan vektor *ciphertext*-nya $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$, ... Jika
$$P = \begin{bmatrix}\mathbf{p}_1^T\\\mathbf{p}_2^T\\\cdots\\\mathbf{p}_n^T\end{bmatrix}$$
- adalah matriks nxn dengan barisan vektor *plaintext*, dan
$$C = \begin{bmatrix}\mathbf{c}_1^T\\\mathbf{c}_2^T\\\cdots\\\mathbf{c}_n^T\end{bmatrix}$$

adalah matriks nxn dengan barisan vektor *ciphertext*, maka serangkaian operasi baris elementer akan menjadikan matriks C menjadi matriks I untuk transformasi matriks P menjadi $(A^{-1})^T$.[1]

Case 3

Sebuah pesan rahasia yang telah dienkripsi menjadi "AHEEOQXTFAYSIUGWRKIX". Diketahui 4 huruf pertamanya berarti "DEAR". Pecahkan kodenya!

Solution

1. Tentukan matriks vektor *plaintext* dan *ciphertext* dari potongan pesan yang telah diketahui.
$$\mathbf{p}_1 = \begin{bmatrix}4\\5\end{bmatrix} \leftrightarrow \mathbf{c}_1 = \begin{bmatrix}1\\8\end{bmatrix}$$
$$\mathbf{p}_2 = \begin{bmatrix}1\\18\end{bmatrix} \leftrightarrow \mathbf{c}_2 = \begin{bmatrix}5\\5\end{bmatrix}$$
2. Kombinasikan vektor p dan c membentuk matriks [C|P]
$$C = \begin{bmatrix}\mathbf{c}_1^T\\\mathbf{c}_2^T\end{bmatrix} = \begin{bmatrix}1 & 8\\5 & 5\end{bmatrix}$$
$$P = \begin{bmatrix}\mathbf{p}_1^T\\\mathbf{p}_2^T\end{bmatrix} = \begin{bmatrix}4 & 5\\1 & 18\end{bmatrix}$$
$$\left(\begin{array}{cc|cc}1 & 8 & 4 & 5\\5 & 5 & 1 & 18\end{array}\right)$$
3. Transformasikan matriks P menjadi matriks$(A^{-1})^T$ dengan mengubah matriks C menjadi matriks I (matriks eselon tereduksi) dengan operasi baris elementer.
$$\left(\begin{array}{cc|cc}1 & 8 & 4 & 5\\5 & 5 & 1 & 18\end{array}\right)$$
$$\left(\begin{array}{cc|cc}1 & 8 & 4 & 5\\0 & -35 & -19 & -7\end{array}\right)$$ Baris ke-2 ditambah -5Xbaris ke-1
$$\left(\begin{array}{cc|cc}1 & 8 & 4 & 5\\0 & 17 & 7 & 19\end{array}\right)$$ Baris ke-2 diubah menjadi sisa mod 26
$$\left(\begin{array}{cc|cc}1 & 8 & 4 & 5\\0 & 391 & 161 & 437\end{array}\right)$$ Baris ke-2 dikali 17^{-1}mod 26 (x23)
$$\left(\begin{array}{cc|cc}1 & 8 & 4 & 5\\0 & 1 & 5 & 21\end{array}\right)$$ Baris ke-2 diubah menjadi sisa mod 26
$$\left(\begin{array}{cc|cc}1 & 0 & -36 & -163\\0 & 1 & 5 & 21\end{array}\right)$$ Baris ke-1 ditambah -8Xbaris ke-2
$$\left(\begin{array}{cc|cc}1 & 0 & 16 & 19\\0 & 1 & 5 & 21\end{array}\right)$$ Baris ke-1 diubah menjadi sisa mod 26

Maka terbentuk kombinasi matriks $[I|(A^{-1})^T]$
$$(A^{-1})^T = \begin{bmatrix}16 & 19\\5 & 21\end{bmatrix}$$
$$A^{-1} = \begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}$$
4. Tentukan angka *ciphertext* untuk semua karakter pada kode pesan rahasia.
   AH E E O Q X T F A Y S I U G W
   1 8 5 5 15 17 24 20 6 1 25 19 9 21 7 23
   R K I X
   18 11 9 24
5. Setelah didapatkan invers modulo matriks A dan vektor *ciphertext*nya, kemudian lakukan proses dekripsi.
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}1\\8\end{bmatrix} = \begin{bmatrix}56\\187\end{bmatrix} \text{ atau } \begin{bmatrix}4\\5\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}5\\5\end{bmatrix} = \begin{bmatrix}105\\200\end{bmatrix} \text{ atau } \begin{bmatrix}1\\18\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}15\\17\end{bmatrix} = \begin{bmatrix}325\\642\end{bmatrix} \text{ atau } \begin{bmatrix}13\\18\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}24\\20\end{bmatrix} = \begin{bmatrix}484\\876\end{bmatrix} \text{ atau } \begin{bmatrix}16\\18\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}6\\1\end{bmatrix} = \begin{bmatrix}101\\135\end{bmatrix} \text{ atau } \begin{bmatrix}23\\5\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}25\\19\end{bmatrix} = \begin{bmatrix}495\\874\end{bmatrix} \text{ atau } \begin{bmatrix}1\\16\end{bmatrix}$$

$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}9\\21\end{bmatrix}=\begin{bmatrix}249\\612\end{bmatrix} \text{ atau } \begin{bmatrix}15\\14\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}7\\23\end{bmatrix}=\begin{bmatrix}227\\616\end{bmatrix} \text{ atau } \begin{bmatrix}19\\18\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}18\\11\end{bmatrix}=\begin{bmatrix}343\\573\end{bmatrix} \text{ atau } \begin{bmatrix}5\\1\end{bmatrix}$$
$$\begin{bmatrix}16 & 5\\19 & 21\end{bmatrix}\begin{bmatrix}9\\24\end{bmatrix}=\begin{bmatrix}264\\675\end{bmatrix} \text{ atau } \begin{bmatrix}4\\25\end{bmatrix}$$

6. Pesan rahasia yang dienkripsi adalah “DEAR MR PR WEAPONS READY”

V. SIMPULAN

Penyelasaian persoalan kriptografi dengan menggunakan *Hill-ciphers* adalah salah satu aplikasi dari konsep aljabar lanjar. Dalam melakukan enkripsi dan dekripsi pesan rahasia menggunakan konsep matriks dan operasi-operasi pada matriks. Selain itu juga digunakan operasi baris elementer yang biasa diterapkan pada eliminasi gauss jordan. Konsep aturan bebas lanjar dan transformasi lanjar juga dijadikan dasar pada penyelesain persoalan kriptografi dengan *Hill-ciphers*.

REFERENCES

[1] Anton, Rorres.2010.”*Elementary Linear Algebra Application Version 10th ed*”.

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 Desember 2015

NURSYAHRINA (13513060)