Aplikasi Operasi Baris Elementer Matriks dalam Kriptografi

Ikhwanul Muslimin/13514020
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13514020@std.stei.itb.ac.id

***Abstrak*—Kriptografi atau seni persandian memerlukan algoritma yang unik untuk alasan keamanan. Agar lebih aman, algoritma perlu dibuat sendiri dan diatur agar kuncinya dapat diubah-ubah sesuai keinginan. Operasi baris elementer (OBE) pada matriks sistem persamaan lanjar dapat digunakan sebagai kunci kriptografi. Algoritmanya cukup mudah, yaitu hanya dengan menyelesaikan matriks menjadi matriks eselon. Hasil penyelesaian itu berupa angka yang merepresentasikan karakter sesuai dengan kunci yang telah disepakati.**

***Keywords*—kriptografi, matriks, operasi baris lanjar, eselon, kunci.**

I. PENDAHULUAN

Dalam kehidupan sekarang, privasi dan kerahasiaan menjadi sebuah hal yang krusial. Antara satu pihak dan pihak lain sekarang sangat sering berkomunikasi melalui media. Komunikasi ini bisa berupa saling kirim pesan, gambar, video, dan sebagainya.

Komunikasi yang disalurkan melalui perantara bisa jadi bocor di pihak ketiga yang tidak diinginkan. Bocornya informasi ini akan berbahaya jika pihak ketiga tersebut menggunakannya untuk tindak kejahatan, pencurian data, penyadapan, dan lain-lain.

Tidak hanya data yang dikirim melalui media, data yang dikirim langsung juga terkadang harus dirahasiakan dari pihak luar. Data yang seperti ini pun dapat dicuri, misalnya melalui kamera tersembunyi, atau sengaja dicuri secara fisik. Oleh karena itu, diperlukan cara untuk menyembunyikan pesan tersebut.

Saat ini, terdapat berbagai cara untuk menyembunyikan isi pesan tersebut. Salah satu cara untuk mengatasi hal ini adalah membuat sebuah mesin kriptografi yang berfungsi untuk mengonversi satu teks sumber menjadi berkas yang telah dienkripsi (*encoding*) atau sebaliknya, mengonversi berkas enkripsi menjadi teks yang dapat dibaca (*decoding*). Kode-kode kunci harus hanya diketahui oleh pihak pengirim pesan dan penerima pesan. Sehingga, ketika suatu informasi bocor, informasi tersebut tetap tidak dapat diketahui, selama algoritma dan kunci-kunci kriptografi tidak diketahui.

Kriptografi yang baik dan cenderung lebih aman adalah kriptografi yang menggunakan algoritma buatan sendiri, sehingga kunci-kunci hanya diketahui oleh pemakai saja, sedangkan orang lain kecil kemungkinannya untuk memahami isi pesan tersebut.

Oleh karena itu, dalam makalah ini, penulis ingin mengajukan satu cara baru dalam enkripsi berkas. Cara tersebut adalah dengan menggunakan sistem persamaan lanjar yang membentuk matriks, yang kemudian diselesaikan dengan operasi baris lanjar. Hasil dari penyelesaian sistem persamaan lanjar ini merupakan kata yang dimaksud dalam sebuah teks.

II. DASAR TEORI

A. Teori Operasi Baris Elementer pada Matriks

Operasi baris elementer (OBE) merupakan operasi aritmatika (penjumlahan dan perkalian) yang dikenakan pada setiap unsur dalam suatu baris pada sebuah matriks[1]. Operasi baris elementer meliputi:

1. Pertukaran baris
2. Perkalian suatu baris dengan konstanta tak nol
3. Penjumlahan hasil perkalian suatu baris dengan konstanta tak nol (seperti butir 2) dengan baris lain[1].

Contoh operasi baris elementer

(a) $A = \begin{pmatrix} -3 & -2 & -1 \\ 1 & 2 & 3 \\ 0 & 2 & 4 \end{pmatrix}$

$b_1 \leftrightarrow b_2 \sim \begin{pmatrix} 1 & 2 & 3 \\ -3 & -2 & -1 \\ 0 & 2 & 4 \end{pmatrix}$

Baris pertama (b_1) ditukar dengan baris kedua (b_2)

(b) $B = \begin{pmatrix} 1 & -1 & 0 & -1 \\ 0 & 2 & 1 & 7 \\ 2 & -1 & 1 & 3 \end{pmatrix}$

Perkalian (-2) dengan b_1 lalu tambahkan pada b_3

$-2b_1 + b_3 \sim \begin{pmatrix} 1 & -1 & 0 & -1 \\ 0 & 2 & 1 & 7 \\ 0 & 1 & 1 & 5 \end{pmatrix}$

Terminologi pada matriks
Misalkan diberikan matriks berikut.

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

- Bilangan 1 (pada baris pertama kolom pertama) dinamakan satu utama.
- Bilangan 2 pada baris kedua dinamakan unsur pertama tak nol pada baris kedua.
- Baris pertama dan kedua dinamakan baris tak nol, karena pada kedua baris tersebut memuat unsur tak nol.
- Baris ketiga dinamakan baris nol, karena setiap unsur pada baris ketiga adalah nol.

Tujuan dilakukannya operasi baris elementer pada suatu matriks adalah menghasilkan matriks yang memenuhi beberapa sifat berikut[1].

1. Pada baris tak nol unsur tak nol pertama adalah 1 (membuat satu utama).
2. Pada baris yang berurutan, baris yang lebih rendah memuat 1 utama yang lebih ke kanan.
3. Jika ada baris nol (baris yang semua unsurnya nol), maka ia diletakkan pada baris paling bawah.
4. Pada kolom yang memuat satu utama, maka unsur yang lainnya adalah nol.

Jika butir 1, 2, dan 3 dipenuhi, maka matriks hasil OBE dinamakan berbentuk *esilon baris* (prosesnya dinamakan *eliminasi Gauss*). Sementara itu, jika semua poin dipenuhi maktriks dinamakan berbentuk *esilon baris tereduksi* (prosesnya dinamakan *eliminasi Gauss Jordan*)[1].

Penggunaan OBE untuk mencari solusi persamaan lanjar

Misalkan diketahui sistem persamaan lanjar (SPL), maka SPL tersebut dapat dicari solusinya dengan OBE sampai terbentuk matriks esilon baris atau esilon baris tereduksi[1].

Sebagai contoh, berikut ini adalah sebuah SPL.

$$a+c = 4$$
$$a-b = -1$$
$$2b+c = 7$$

SPL tersebut direpresentasikan sebagai matriks *augmented* sebagai berikut.

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 4 \\ 1 & -1 & 0 & -1 \\ 0 & 2 & 1 & 7 \end{array}\right)$$

Setelah dilakukan OBE, terbentuk sebuah matriks esilon tereduksi sebagai berikut.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

Sehingga, diperoleh hasil $a = 1$, $b = 2$, dan $c = 3$.

B. Teori Kriptografi

Kriptografi adalah studi tentang teknik matematika untuk seluruh aspek keamanan informasi[2]. Keamanan informasi meliputi aspek-aspek berikut ini[3].

- kerahasiaan atau privasi, yaitu menjaga supaya pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak,
- intergritas data, yaitu memberikan jaminan bahwa untuk tiap bagian pesan tidak akan mengalami perubahan dari saat data dibuat/dikirim oleh pengirim sampai dengan saat data tersebut dibuka oleh penerima data,
- autentikasi, yaitu berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan,
- nirpenangkalan (*nonrepudiation*), yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang tertentu sehingga apabila ada seseorang yang mencoba mengakui memiliki dokumen tersebut, dapat dibuktikan kebenarannya dari pengakuan orang lain.

Setiap aspek-aspek keamanan pesan di atas dapat dialamatkan dengan standar metode dalam kriptografi. Disamping mengubah simbol-simbol pesan, kakas dari kriptografi dapat dimanfaatkan untuk berbagi kode akses antara orang satu dengan orang lain yang dituju sehingga tidak ada orang lain yang dapat mengakses sebuah informasi kecuali mereka berdua[2].

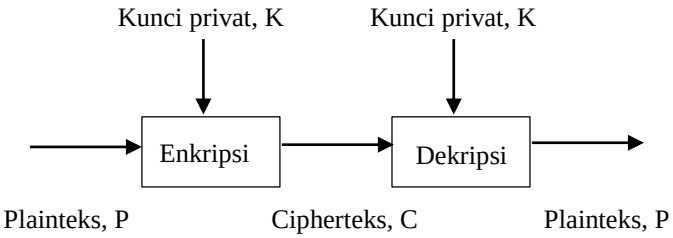
Terminologi dalam kriptografi[2]

- Enkripsi = proses mengonversi sebuah pesan untuk menyembunyikan informasi yang dikandungnya; proses ini dapat mengandung *encoding* dan *enciphering*.
- *Plaintext* = pesan yang akan ditransmisikan.
- *Chippertext* = pesan yang sudah dikonversi menjadi kode.
- *Alfabet* = sekumpulan simbol, juga mengarah sebagai karakter.
- *Karakter* = sebuah elemen dari alfabet.
- *Bit* = karakter 0 atau 1 dalam alfabet biner.
- *String* = serangkaian karakter terbatas dari sebuah alfabet.
- *Encode* = proses mengonversi pesan dari *plaintext* menjadi *chippertext*.
- *Decode* = kebalikan dari *encode*.

Jenis-jenis algoritma kriptografi

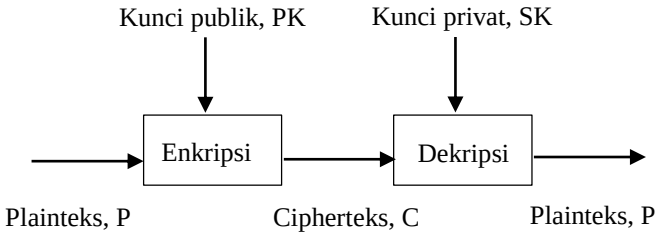
Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dibedakan menjadi dua macam[3], yaitu kriptografi simetri (*symetric cryptography*) dan kriptografi asimetri (*asymetric cryptography*). (elib unikom)

Pada sistem kriptografi simetri, kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem simetri terletak pada kerahasiaan kunci[3].



Gambar 1. Kriptografi simetri

Pada sistem kriptografi asimetris, kunci untuk proses enkripsi tidak sama dengan kunci untuk proses dekripsi. Istilah lain untuk kriptografi asimetri adalah kriptografi kunci publok, sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, sementara kunci dekripsi hanya diketahui oleh penerima pesan[3].



Gambar 2. Kriptografi asimetri

Beberapa contoh algoritma kriptografi yang umum adalah RSA, ElGamal, DSA, Pailer, Rabin, Difffe-Hellman, dan lain-lain[4].

III. ANALISIS

Dari teori dasar, dapat dikatakan bahwa pada intinya, kriptografi dapat menggunakan kode kunci apapun dalam proses enkripsi dan dekripsiya, asal diketahui oleh kedua pihak yang berkomunikasi, dan terjaga kerahasiaannya. Pada makalah ini, penulis akan mengimplementasikan teori operasi baris lanjar pada matriks sistem persamaan lanjar untuk kriptografi.

Algoritma ini memiliki beberapa kesepakatan, antara lain sebagai berikut.

(a) Karakter yang didukung adalah huruf dari a sampai z, huruf kecil dan huruf kapital disamakan.
(b) Angka dari 0 sampai 9.
(c) Tanda baca titik (.), koma (,), tanda tanya (?).

Karena proses OBE hanya mendukung hasil berupa bilangan, maka sebelumnya karakter-karakter tersebut diubah dulu menjadi bentuk angka. Perjanjiannya adalah sebagaimana yang diberikan tabel berikut.

a/A	1	k/K	11	u/U	21	5	35
b/B	2	l/L	12	v/V	22	6	36
c/C	3	m/M	13	w/W	23	7	37
d/D	4	n/N	14	x/X	24	8	38
e/E	5	o/O	15	y/Y	25	9	39
f/F	6	p/P	16	z/Z	26	0	30
g/G	7	q/Q	17	1	31	.	40
h/H	8	r/R	18	2	32	,	41
i/I	9	s/S	19	3	33	?	42
j/J	10	t/T	20	4	34		

Tabel 1. Tabel perjanjian konversi

Sebagai contoh, kata ADA akan dibuat menjadi 1 4 1 terlebih dahulu.

Format penulisan

(a) Ditulis secara lanjar, setiap huruf dipisah dengan koma.
Sebagai contoh 1 0 0 1, 0 1 0 4, 0 0 1 1 untuk kata ADA.
(b) Tidak unik
Karena matriks untuk kata suatu kata tidak unik, maka chipperteks juga tidak unik. Kata ADA juga dapat dibuat chipperteks sebagai 2 1 3 9, 1 1 6 11, 0 3 2 14.
(c) Spasi dituliskan dengan titik (.)
Misalnya kata ADA AKU, maka dalam chipperteksnya adalah 1 0 0 1, 0 1 0 4, 0 0 1 1. 1 0 0 1, 0 1 0 11, 0 0 1 21.

1. Proses Enkripsi

Seperti yang telah dibahas di atas, misalkan kita ingin mengenkripsi suatu kata, maka kita terjemahkan terlebih dahulu kata tersebut. Setelah itu, kita bentuk matriks yang bersesuaian dengan kata tersebut.

Sebagai contoh, misalnya kita ingin melakukan enkripsi terhadap kata SIAPA.

Langkah 1
kata tersebut diterjemahkan menjadi 19 9 1 16 1
Langkah 2
Buat masing-masing baris matriks. Karena SIAPA berisi lima karakter, maka akan ada 5 baris dan 6 kolom.
Baris pertama, sebagai contoh, kita ingin mengambil konstanta 2, 3, 1, 1, 0, maka baris pertama adalah:
2 3 1 1 0 X, dengan X = 2(19) + 3(9) + 1 (1) + 1 (16) + 0(1) = 82.
Baris kedua, 2 1 1 0 0 48
Baris ketiga, 1 0 0 0 0 19
Baris keempat, 0 1 2 3 4 63
Baris kelima, 0 0 0 0 0 1 1

Langkah 3
Selanjutnya adalah tinggal menyusun sesuai format yang telah disepakati. Sehingga, chipperteks yang dihasilkan adalah 2 3 1 1 0 82, 2 1 1 0 0 48, 1 0 0 0 0 19, 0 1 2 3 4 63, 0 0 0 0 1 1.

2. Proses Dekripsi

Aplikasi OBE akan nyata dilakukan di proses dekripsi. Pada proses dekripsi, diberikan sebuah chipperteks yang hendak dibaca isinya. Secara kasar, proses dekripsi adalah mencari solusi matriks yang diberikan.
Misalnya kita ingin mencari plainteks dari kode 2 3 1 1 0 82, 2 1 1 0 0 48, 1 0 0 0 0 19, 0 1 2 3 4 63, 0 0 0 0 1 1 yang tak lain adalah kata SIAPA. Berikut ini langkah-langkahnya.

Langkah 1
Bentuk chipperteks lanjar menjadi bentuk matriks baris-kolom.

$$M = \begin{pmatrix} 2 & 3 & 1 & 1 & 0 & 82 \\ 2 & 1 & 1 & 0 & 0 & 48 \\ 1 & 0 & 0 & 0 & 0 & 19 \\ 0 & 1 & 2 & 3 & 4 & 63 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Langkah 2
Buat matriks eselon dari matriks di atas.

$$M = \begin{pmatrix} 2 & 3 & 1 & 1 & 0 & 82 \\ 2 & 1 & 1 & 0 & 0 & 48 \\ 1 & 0 & 0 & 0 & 0 & 19 \\ 0 & 1 & 2 & 3 & 4 & 63 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$b_3 \leftrightarrow b_1\ M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 19 \\ 2 & 1 & 1 & 0 & 0 & 48 \\ 2 & 3 & 1 & 1 & 0 & 82 \\ 0 & 1 & 2 & 3 & 4 & 63 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$b_2 - 2b_1\ M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 19 \\ 0 & 1 & 1 & 0 & 0 & 10 \\ 2 & 3 & 1 & 1 & 0 & 82 \\ 0 & 1 & 2 & 3 & 4 & 63 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$b_3 - 2b_1\ M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 19 \\ 0 & 1 & 1 & 0 & 0 & 10 \\ 0 & 3 & 1 & 1 & 0 & 44 \\ 0 & 1 & 2 & 3 & 4 & 63 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$b_3 - 3b_2\ M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 19 \\ 0 & 1 & 1 & 0 & 0 & 10 \\ 0 & 0 & -2 & 1 & 0 & 14 \\ 0 & 1 & 2 & 3 & 4 & 63 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

dan seterusnya.

Sampai akhirnya diperoleh matriks esilon berikut.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 19 \\ 0 & 1 & 1 & 0 & 0 & 10 \\ 0 & 0 & 1 & -1/2 & 0 & -7 \\ 0 & 0 & 0 & 1 & 8/7 & 120/7 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Langkah 3
Buat matriks esilon tereduksi dari matriks esilon di atas.
Cara yang digunakan sama dengan langkah-langkah pada langkah 2, sehingga pada akhirnya diperoleh matriks esilon sebagai berikut.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 19 \\ 0 & 1 & 0 & 0 & 0 & 9 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 16 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Sehingga, secara berturut-turut diperoleh terjemah dari chipperteks tersebut adalah 19 9 1 16 1.

Langkah 4
Terjemahkan plainteks yang berbentuk angka menjadi karakter-karakter yang sesuai. Dalam hal ini, kode 19 9 1 16 1 adalah kata SIAPA.

3. Kelebihan dan Kelemahan

Metode kriptografi dengan memanfaatkan operasi baris lanjar memiliki kelebihan dan kelemahan. Berikut ini beberapa kelebihannya.

(a) Tergolong baru, jadi relatif aman.
(b) Algoritma sederhana, hanya sebatas menyelesaikan matriks sistem persamaan lanjar
(c) Tabel perjanjian konversi karakter ke angka dapat diubah-ubah sesuai keperluan, sehingga antara satu kode dan kode lain bisa berbeda arti tergantung kesepakatan. Ini dapat digunakan untuk menghindari bocornya kode kunci.
(d) Proses enkripsi dan dekripsi dapat dilakukan oleh komputer, karena sistem operasi baris lanjar ini berpola.

Sedangkan kelemahan dari metode ini adalah sebagai beirkut.

(a) Membutuhkan memori cukup besar, karena satu karaker memerlukan digit sejumlah panjang kata. Semakin panjang kata, semakin banyak digit yang diperlukan.
(b) Berupa kriptografi simetris, kunci enkripsi dan dekripsi sama, yang dalam hal ini adalah tabel konversi. Sehingga ketika kunci tersebut diketahui, maka jika tidak segera mengubah tabel konversi, akan bocor.

IV. SIMPULAN DAN SARAN

A. *Simpulan*

Operasi baris lanjar dapat digunakan sebagai metode baru perumusan kriptografi. Untuk proses enkripsi, kata yang akan disandikan terlebih dahulu dikonversi ke bentuk digit yang telah disepakati. Digit-digit ini kemudian dibentuk matriks sistem persamaan lanjar. Untuk proses dekripsi, penyelesaiannya adalah dengan memanfaatkan operasi baris lanjar sampai membentuk matrik esilon. Penggunaan metode OBE dalam kriptografi memiliki kelebihan, di antaranya masih tegolong baru sehingga lebih aman, dan tabel konversi yang merupakan kunci kode bersifat fleksibel. Sedangkan kekurangannya adalah tergolong kriptografi simetris, dan memerlukan memori yang besar.

B. *Saran*

Beberapa saran untuk pengembangan metode ini di masa depan adalah perlu diperbanyak lagi karakter-karakter yang didukung. Selain itu, perlu diperhatikan juga alokasi memori agar tidak terlalu besar.

V. UCAPAN TERIMA KASIH

Penulis panjatkan puji syukur ke hadirat Allah subhanahu wata'ala yang telah memberikan kemudahan dalam menyusun makalah ini. Penulis juga berterima kasih kepada Bapak Rinaldi Munir yang telah membimbing saya dalam mata kuliah Aljabar Geometri, terutama mengenai teori sistem persamaan lanjar dan operasi baris elementer yang menjadi dasar makalah ini.

REFERENSI

[1] Adiwijaya, *Aplikasi Matriks dan Ruang Vektor*, Yogyakarta:Graha Ilmu, 2014, Bab 1 dan Bab 3.

[2] Anonim, *Math3024 Elementary Cryptography and* Protocols, Sydney : The University of Sydney.

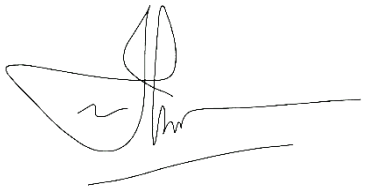
[3] Ronisaptop, *BAB II Tinjauan Pustaka*, http://elib.unikom.ac.id/files/disk1/437/jbptunikompp-gdl-ronisaptop-21805-7-11.unik-i.pdf diakses tanggal 14 Desember 2015.

[4] Nigel Smart, *Cryptography: An Introduction (3rd Edition)*, University of Bristol, Chapter 11 dan Chapter 15.

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, 15 Desember 2015



Ikhwanul Muslimin/13514020