Penerapan Hill Chiper pada Keamanan Pesan Teks

Tomy Satria Alasi
Facebook/tomy.satria.alasi
Ilmutomy.blogspot.com
Ilmutomy.wordpress.com

Algoritma Hill Chiper adalah suatu fungsi matematis yang digunakan untukmelakukan enkripsidan dekripsiAda dua macam algoritma kriptografi, yaitu algoritmasimetris(symmetric algorithms) dan algoritmaasimetris(asymmetric algorithms). Hill cipher yang merupakan poly alphabetic cipher dapat dikategorikan sebagai block cipher, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula.

2.3.5.1.1 Sejarah Hill Chiper

Sejak kekaisaran Romawi, kriptosistem yang lebih rumit dikembangkan oleh orang seperti oleh ahli Matematika Italia Leon Battista Alberti (lahir pada tahun 1404), Matematikawan Jerman Johannes Trithernius (lahir pada tahun 1492), seorang kriptographer dan diplomat Perancis Blaise de Vigenére (1523−1596), Lester S. Hill, yang menemukan Hill Cipher (Hill Cipher) pada tahun 1929. Hill Cipher merupakan jenis lain dari polygraphic cipher. Sandi ini mengenkripsi suatu string huruf menjadi bentuk string yang lain dengan panjang yang sama. Teknik Hill Cipher dikembangkan oleh

Lester S. Hill pada Hunter College dan dipublikasikan pada Americian Mathematical Monthly, Volume 36, Issue 6 (Juni−Juli, 1929) halaman 306 − 312.

Hill Cipher menggunakan matriks untuk mentransformasi string berupa blok huruf. Hill Cipher berdasarkan pada aljabar linier dan seperti sandi Vigenére, Hill Cipher merupakan block cipher. Sandi ini dapat dipecahkan dengan known-plaintext attacks tetapi tahan melawan ciphertext-only attack. Cara kerja sandi ini berdasarkan atas perkalian matriks dengan menggunakan sebuah kunci K. Penjelasan mengenai Hill Cipher ini dapat diuraikan sebagai berikut: Misalkan m adalah bilangan bulat positif dan P = C = (Z26)m dan misalkan K = {m x m meripakan matriks yang nilai elemenya terdiri dari Z26| maka untuk suatu kunci K, dapat didefenisikan sebagai ek (x) Mod 26 dan dk (y) = k-1 y Mod 26 dimana semua operasi dilakukan dalam matrix Z¬26.

2.3.5.1.2 Operasi Hill Chiper

Setiap huruf diwakili oleh modulo nomor 26. (Seringkali sederhana skema A = 0 , B = 1 , ... , Z = 25 yang digunakan , tapi ini bukan fitur penting dari cipher .) Untuk mengenkripsi pesan , setiap blok huruf n (dianggap sebagai vektor n - komponen) dikalikan dengan n dibalik × n matriks , lagi modulus 26. untuk mendekripsi pesan , setiap blok dikalikan dengan kebalikan dari matriks yang digunakan untuk enkripsi. Matriks yang digunakan untuk enkripsi adalah kunci cipher , dan harus dipilih secara acak dari himpunan dibalik n × n matriks (modulo 26) . Penjelasan cara kerja dari Hill Cipher dapat disederhanakan dengan cara seperti berikut: Misalkan K merupakan sebuah matriks kunci *m* × *m* yang merupakan representasi dari suatu persamaan linier. *Ciphertext* (C) dan *plaintext* p merupakan matriks *m* × 1. Maka didapat persamaan untuk menghasilkan *ciphertext* sebagai berikut:

C = K . P (mod 26)

Diman :

C = K . P

C = Ciphertext

K = Kunci

P = Plaintext

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11}\ K_{12}\ K_{13} \\ K_{21}\ K_{22}\ K_{23} \\ K_{31}\ K_{32}\ K_{33} \end{bmatrix} = \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \text{ mod } 26$$

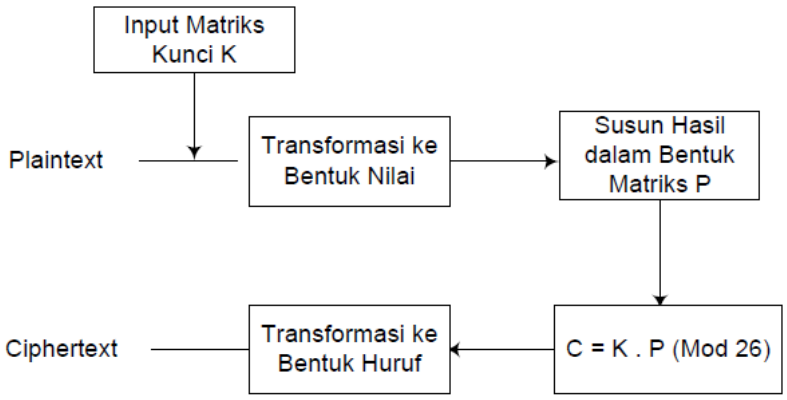
Dekripsi memerlukan kunci K yang bersifat *invertible*. Contohnya K . k^{-1} (mod 26) = I dimana I merupakan matriks identitas. Karena C = K . P Mod 26 maka K = C . P^{-1} Mod 26 Tidak semua *plaintext* bersifat *invertible* (dapat dibalik kembali). Sandi Caesar, Hill Cipher, dan sandi Playfair semua bekerja dengan sebuah alphabet tunggal saat disubstitusi.

2.3.5.1 Enkripsian Hill Cipher

Langkah-langkah untuk proses enkripsi *plaintext* dengan Hill Cipher adalah sebagai berikut:

1. Pilih suatu matriks kunci K yang berupa matriks bujur sangkar yang dipakai sebagai kunci.
2. Transformasikan tiap huruf dalam teks ke bilangan bulat yang sesuai (A = 0; B = 1; … Z = 25) .
3. Kelompokkan barisan angka yang didapat ke dalam beberapa blok vektor P yang panjangnya sama dengan ukuran matriks K.
4. Hitung C = K . P (mod 26) untuk tiap vektor P.

Kembalikan tiap angka dalam vektor sandi C ke huruf yang sesuai untuk mendapatkan teks sandi .



Bagian ini akan menjelaskan enkripsi dengan Hill Cipher dengan memberikan contoh. Hill Cipher menggunakan matriks untuk mentransformasikan *string plaintext* menjadi *ciphertext*. Untuk mentransformasikan *plaintext* maka pertama sekali semua huruf alphabet dinyatakan dalam nilai seperti pada tabel 2.1 berikut:

Tabel 2.1 Nilai Transformasi Plainteks

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

Tabel 21. Nilai Transformasi Plainteks
Sumber :

Misalkan terdapat pesan berikut yang akan dienkripsi dengan Hill Cipher: Tomy Satria Alasi, Selanjutnya adalah membagi pesan tersebut menjadi bentuk pasangan yang terdiri atas tiga huruf (*digraph*), Misalkan : ‘ TOMY SATRIA ALASI’ maka menjadi : “TOM{19,14,12}, YSA{24,18,0}, TRI{19,17,08}, AAL{0,0,11}, ASI{0,18,08}”. Jika pesan tidak terdiri atas jumlah huruf dalam nilai genap, maka harus ditambahkan sebuah karakter null pada akhir pesan. Setelah itu tiap pasangan dikonversi ke bentuk nilai berdasarkan ekivalen dari huruf pada tabel di atas.

T	O	M	Y	S	A	T	R
19	14	12	24	18	0	19	18
I	A	A	L	A	S	I	
8	0	0	11	0	18	8	

Tiap pasangan string di atas akan di-*encipher* dengan menggunakan matriks kunci, kunci bebas di bawah modulus 26 dengan Kunci 3x3, *Encipher* pada pasangan pertama dan dinyatakan sebagai vektor kolom “TOM” adalah {19,14,12} kemudian dikalikan dengan matriks kunci.

Kunci 3x3			Abjad	Nilai	Perkalian Matriks			Tambah	Nilai mod	*Encipher*
17	17	5	T	19	323	238	60	621	23	X
21	18	21	O	14	399	252	252	903	19	T
2	2	19	M	12	38	28	228	294	8	I

Table 2.2 Operasi *Enchiper*

Sehingga nilai vektor kolom “TOM” {19, 14, 12 } maka setelah di *Encipher* menghasilkan “XTI” {23, 19, 8 }. Maka setelah dilakukan berulang dari “TOM YSA TRI AAL ASI” menghasilkan “XTI MWG CVQ DXB IYG “ dengan nilai {23, 19, 8}, {12,

22, 6}, {2, 15, 16}, {3, 23, 1}, {8, 24 ,6 }. Sehingga pesan yang terkirim dari “Tomy Satria Alasi” adalah “Xtim Wgcvrd Xbiyg”.

.

Biografi Penulis

Tomy Satria Alasi. SD N Kandang Mbelang Kutacane, SMP-SMA di Pondok Pesantren Darul Iman, Sedang menyelesaikan S1 Tehnik Informatika di STMIK Budidarma Medan , Indonesia tahun 2011 sampai 20015. Berawal dari ketidak tahuan dan ingin memahami ilmu komputer, suka programing, gaming, networking, vidio editing. Berbagai artikel menarik lain tersedia secara gratis di situs blog *http://ilmutomy.blogspot.com*