PENERAPAN MATRIKS PERSEGI PANJANG SEBAGAI KUNCI PUBLIK DAN KUNCI PRIVAT PADA MODIFIKASI CIPHER HILL

Maxrizal[a], **Baiq Desy Aniska Prayanti**[b]
[a] Jurusan Sistem Informasi STMIK Atma Luhur Pangkalpinang
Jl. Jendral Sudirman, Selindung, Pangkalpinang, Kep. Bangka Belitung,
maxrizal@atmaluhur.ac.id
[b] Universitas Bangka Belitung
Kampus Terpadu Balunijuk, Merawang, Bangka, Kep. Bangka Belitung

ABSTRAK

Matriks nonsingular memiliki peranan penting dalam kehidupan. Sedangkan, penerapan matriks persegi panjang masih belum banyak ditemukan. Salah satu penerapan matriks nonsingular dalam kriftografi adalah Cipher Hill. Cipher Hill menggunakan kunci bersifat simetris. Selain itu, pada kriftografi dikenal juga kunci asimetris yang diklaim lebih aman dari pada kunci simetris. Pada makalah ini diperkenalkan modifikasi Cipher Hill menggunakan kunci asimetris. Kunci-kunci asimetris dibentuk dari matriks-matriks persegi panjang.

Kata Kunci : matriks persegi panjang, kunci publik, kunci privat, modifikasi cipher hill.

ABSTRACT

Nonsingular matrices have an important role in life. However, the application of rectangular matrices is still not widely found. One application of nonsingular matrices in cryptography is Cipher Hill. Cipher Hill uses symmetric keys. Other that, cryptography also recognizes asymmetric keys. This key is safer than the symmetric key. In this paper, we introduce Cipher Hill modifications using asymmetric keys. Asymmetrical keys are formed using rectangular matrices.

Kata Kunci : rectangular matrix, public key, private key, cipher hill modification.

Pendahuluan

Konsep matriks merupakan topik penting pada materi aljabar linear elementer. Berdasarkan ukuran atau ordonya matriks dibedakan menjadi matriks persegi $\left(M_{n\times n}\right)$ dan matriks persegi panjang $\left(M_{m\times n}\right)$, dengan $m\neq n$. Matriks persegi dibedakan menjadi matriks singular dan matriks nonsingular. Dalam kajian aljabar, penerapan matriks nonsingular sangat penting dalam kehidupan sehari-hari. Hal ini disebabkan karena matriks nonsingular memiliki balikan *(invers)* terhadap operasi perkalian matriks. Sebaliknya, penerapan matriks singular dan matriks persegi panjang $\left(M_{m\times n}\right)$ masih belum banyak ditemukan.

Salah satu penerapan konsep matriks yang digunakan dalam bidang kriptografi adalah Cipher Hill yang

diperkenalkan oleh Lester. S. Hill pada tahun 1929. Cipher Hill menggunakan matriks nonsingular sebagai kunci dan mengelompokkan pesan (*plaintext)* menjadi beberapa blok dengan ukuran sama. Sebelum dikirim ke penerima, pengirim akan mengenkripsi blok *plaintext* P menjadi pesan yang sudah disandikan *(ciphertext)* C sehingga diperoleh $C = KP \bmod M$, dengan K adalah matriks nonsingular. Selanjutnya, *ciphertext* C diterima oleh penerima dan dideskripsikan kembali menjadi *plaintext* $P = K^{-1}C \bmod M$. Perhatikan bahwa kunci K harus dimiliki oleh pengirim dan penerima. Sifat kunci seperti ini dinamakan kunci simetri. Kelemahan sistem kunci ini adalah kunci harus dikirim melalui jalur yang aman agar pihak yang tidak berhak tidak dapat mengetahuinya.

Pada kriptografi juga dikenal kunci asimetri. Kunci yang ada pada penerima berbeda dengan kunci yang dimiliki pengirim. Penerima membangkitkan kunci privat dan kunci publik, sedangkan pengirim hanya memiliki kunci publik. Kunci asimetri diklaim lebih aman dari pada kunci simetri.

Untuk itu, pada makalah ini akan diperkenalkan modifikasi Cipher Hill menggunakan kunci yang asimetris. Pada makalah ini, kita akan memperkenalkan penerapan matriks persegi panjang sebagai kunci privat dan kunci publik. Kita akan mengubah konsep Cipher Hill yang simetris menjadi Cipher Hill yang asimetris.

Metode Penelitian

Penelitian ini merupakan penelitian studi literatur. Beberapa definisi tentang sifat matriks dan Cipher Hill diperoleh dari Howard Anton *et al* (2005). Selanjutnya, sifat Cipher Hill dan modifikasinya juga disadur dari Acharya *et al* (2009), Adinarayana *et al* (2012) dan Parmar *et al* (2015).

Hasil dan Pembahasan

1. Motivasi modifikasi pada Cipher Hill

Dalam kajian ini, kita akan menjelaskan motivasi dari modifikasi Cipher Hill menggunakan matriks persegi panjang. Diberikan matriks Y berukuran $m \times n$ dan matriks P berukuran $n \times r$, dengan $m \neq n$. Selanjutnya dibentuk

$$C = YP ,$$

yang berukuran $m \times r$. Perhatikan bahwa matriks Y matiks persegi panjang yang tidak memiliki invers, sehingga tidak berlaku $P = Y^{-1}C$. Selanjutnya, diberikan matriks X berukuran $n \times m$. Kita kalikan kedua ruas dengan matriks X dari kiri sehingga diperoleh

$$XC = XYP \ .$$

Perhatikan bahwa matriks XY berukuran $n \times n$ dan pilihlah XY yang nonsingular, sehingga diperoleh

$$P = \left(XY\right)^{-1} XC$$

Perhatikan bahwa, jika kita diberikan *plaintext* P , kunci X dan Y , dan *ciphertext* C maka kita dapatkan enkripsi $C = YP$ dan deskripsi $P = \left(XY\right)^{-1} XC$.

2. Algoritma Modifikasi Cipher Hill

Ada 2 jenis algoritma pada algoritma kunci asimetri yaitu algoritma pembangkit kunci dan algoritma enkripsi dan deskripsi. Sebelum mengirim pesan, pihak penerima harus membangkitkan kunci publik dan kunci privat. Kunci publik akan dikirim penerima kepada pengirim untuk mengenkripsi pesan. Berikut algoritma pembangkit kunci yang dilakukan oleh penerima pesan.

1. Memilih matriks $X_{n \times m}$ dan $Y_{m \times n}$, dengan $n \neq m$.
2. Menghitung $K_{n \times n} = XY$.
3. Menganalisa K . Jika K tidak *invertible* (dapat dibalik) atas mod M maka ulangi langkah 1 dan 2. Jika K *invertible* atas mod M, maka X adalah kunci privat dan Y adalah kunci publik.

Selanjutnya, penerima akan mengirim kunci publik Y kepada pengirim pesan dan menyimpan kunci privat X untuk dirinya sendiri. Berikut ini algoritma enkripsi dan deskripsi

1. Enkripsi :
   Menghitung $C_{m \times r} = Y_{m \times n} P_{n \times r}$.
2. Deskripsi **:**
   Menghitung
   $P_{n \times r} = \left(K^{-1}\right)_{n \times n} X_{n \times m} C_{m \times r}$.

Setelah pesan dienkripsi oleh pengirim, *ciphertext* C akan dikirim ke penerima dan penerima melakukan proses deskripsi untuk mendapatkan *plaintext* P.

3. Analisis Keamanan

Pada modifikasi Cipher Hill berlaku enkripsi $C = YP$. Walaupun Y kunci publik yang tidak dirahasiakan tetapi P tidak dapat ditemukan dengan mudah karena Y merupakan matriks persegi panjang. Hal ini karena Y^{-1} tidak ada. Berbeda halnya dengan Cipher Hill. Pada Cipher Hill, kunci bersifat sangat rahasia.

Selanjutnya, kita juga memperoleh ukuran matriks *ciphertext* dan *plaintext* berbeda, sehingga akan sulit dicari korespondensi satu-satu antara elemen *ciphertext* dan *plaintext*. Berikut tabel perbandingannnya.

Tabel 1. Perbandingan Cipher Hill dan Modifikasi Cipher Hill

Cipher Hill	Modifikasi Hill Cipher
Kunci simetri	Kunci asimetri
Kunci berupa matriks berukuran $n\times n$	Kunci publik berukuran $m\times n$ dan kunci privat berukuran $n\times m$
*Plaintex*t dan *ciphertext* berukuran sama	*Plaintex*t dan *ciphertext* berukuran tidak sama

3. Contoh Kasus

Max akan berkirim pesan ke Niska. Mereka sepakat menggunakan modulo 26 dan Hill-2-Cipher, artinya pesan dipecah menjadi blok-blok yang berisi 2 huruf.

Tabel 2. Tabel Konversi

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
1	2	3	4	5	6	7	8	9	1 0
K	L	M	N	O	P	Q	R	S	T
1	1	1	1	1	1	1	1	1	2
1	2	3	4	5	6	7	8	9	0
U	V	W	X	Y	Z				
2	2	2	2	2	0				
1	2	3	4	5					

Selanjutnya, Niska membangkitkan kunci publik dan kunci privat. Niska memilih calon kunci publik $X=\begin{bmatrix}3 & 8 & 7\\ 10 & 15 & 20\end{bmatrix}$ dan calon kunci privat $Y=\begin{bmatrix}3 & 8\\ 5 & 22\\ 11 & 23\end{bmatrix}$. Selanjutnya, Niska menghitung

$$K=XY=\begin{bmatrix}22 & 23\\ 13 & 12\end{bmatrix}\bmod 26\ .$$

Niska memperoleh $\det(K)=17$. Berdasarkan Tabel Resiprok Modulo 17^{-1} ada yaitu $17^{-1}=23$.

Tabel 3. Tabel resiprok modulo 26

a	**1**	**3**	**5**	**7**	**9**	**11**	**15**	**17**	**19**
a^{-1}	2	3	4	5	6	7	8	9	10
a	21	23	25						
a^{-1}	5	17	25						

Dengan demikian, K *invertible* atas modulo 26. Jadi, Niska telah mendapatkan kunci privat $X=\begin{bmatrix}3 & 8 & 7\\ 10 & 15 & 20\end{bmatrix}$ dan kunci publik $Y=\begin{bmatrix}3 & 8\\ 5 & 22\\ 11 & 23\end{bmatrix}$.

Selanjutnya, Niska mengirim kunci publik $Y=\begin{bmatrix}3 & 8\\ 5 & 22\\ 11 & 23\end{bmatrix}$ ke Max dan dia menyimpan kunci privat $X=\begin{bmatrix}3 & 8 & 7\\ 10 & 15 & 20\end{bmatrix}$. Max akan mengirim kata "BEHIND" dan telah memperoleh kunci publik $Y=\begin{bmatrix}3 & 8\\ 5 & 22\\ 11 & 23\end{bmatrix}$ dari Niska. Selanjutnya, Max mengkonversi $P=\begin{bmatrix}2 & 8 & 14\\ 5 & 9 & 4\end{bmatrix}$ dan menghitung

$$C=YP=\begin{bmatrix}20 & 18 & 22\\ 16 & 4 & 2\\ 7 & 9 & 12\end{bmatrix}\bmod 26\ .$$

Max mengkonversi dan mengirim "TPGRDIVBL" ke Niska.

Niska yang telah menerima "TPGRDIVBL" dari Max akan mengkonversi $C=\begin{bmatrix}20 & 18 & 22\\ 16 & 4 & 2\\ 7 & 9 & 12\end{bmatrix}$. Niska mempunyai kunci privat $X=\begin{bmatrix}3 & 8 & 7\\ 10 & 15 & 20\end{bmatrix}$ dan mengetahui kunci publik $Y=\begin{bmatrix}3 & 8\\ 5 & 22\\ 11 & 23\end{bmatrix}$. Selanjutnya, Niska menghitung

$$K=XY=\begin{bmatrix}22 & 23\\ 13 & 12\end{bmatrix}\bmod 26\ .$$

Dia mendapatkan $K^{-1}=\begin{bmatrix}16 & 17\\ 13 & 12\end{bmatrix}$. Dia menghitung

$$P=K^{-1}XC=\begin{bmatrix}2 & 8 & 14\\ 5 & 9 & 4\end{bmatrix}.$$

Dia mengkonversi dan mendapat "BEHIND". Jadi pesan "BEHIND" dapat diterima Niska (penerima) dengan baik dari Max (pengirim).

Kesimpulan

Dari hasil dan pembahasan diatas, kita dapat menyimpulkan bahwa:

1. Kita dapat memodifikasi Cipher Hill menggunakan kunci asimetris yaitu kunci publik dan kunci privat menggunakan matriks-matriks persegi panjang.
2. Cipher Hill modifikasi dengan kunci asimetris matriks persegi panjang lebih aman dari pada Hill Cipher.

Ucapan Terimakasih

Penelitian ini terlaksana dengan baik karena ada dukungan yang baik dari STMIK Atma Luhur Pangkalpinang. Untuk itu, penulis mengucapkan terima kasih atas dukungan dana dan kebijakan yang ada di STMIK Atma Luhur Pangkalpinang sehingga penelitian ini dapat dilakukan dan diselesaikan.

Pustaka

Anton, H., and Rorres, C., 2005, *Aljabar Linear Elementer Versi Aplikasi, Vol. 2, Ed. 8*, diterjemahkan oleh Hermein, I., dan Gressando, J., Jakarta: Erlangga.

Acharya, B., Patra, S. K., and Panda, G., 2009, Involutory, Permuted and Reiterative Key Matrix Generation Methods for Hill Cipher System, *International Journal of Recent Trends in Engineering*, 1(4): 106-108.

Adinarayana, R. K., Vishnuvardhan, B., Madhuviswanatham., and Krishna, A. V. N., 2012, A Modified Hill Cipher Based On Circulant Matrices, *Procedia Technology*, 4, 114-118.

Parmar, N. B., and Bhatt, K. R., 2015, Hill Cipher Modification: A Detailed Review, *International Journal of Innovative Research in Computer and Communication Engineering*, 3(3), 1467-1474.