KRIPTOGRAFI HILL CIPHER DENGAN MENGGUNAKAN OPERASI MATRIKS

Nikken Prima Puspita dan Nurdin Bahtiar
Jurusan Matematika FMIPA UNDIP
Jl. Prof. H. Soedarto, S.H., Semarang 50275

ABSTRAK. Diberikan matriks A berukuran 2×2 dengan determinan 1 atau -1. Setiap karakter pada plainteks dikonversikan kedalam angka berdasarkan kode ASCII. Proses enkripsi dilakukan dengan cara mengalikan matriks plainteks dengan matriks A. Hasil elemen matriks perkaliannya harus merupakan bilangan bulat modulo 95 yang kemudian ditambahkan dengan bilangan 32. Sedangkan proses dekripsi hill cipher dilakukan dengan cara yang sejalan tetapi matriks cipherteks dioperasikan dengan matriks A^{-1}.
Kata Kunci : cipherteks, dekripsi, enkripsi, plainteks.

1. PENDAHULUAN

Perkembangan teknologi informasi terutama komunikasi saat ini berkembang sangat pesat. Banyaknya media komunikasi umum ternyata menyebabkan ketidakamanan, karena setiap orang bebas untuk menggunakannya. Salah satu cara untuk menjaga kerahasiaan pesan antara pihak satu dan yang lainya adalah dengan konsep penyandian yang disebut dengan kriptografi. Kriptografi merupakan seni dalam menyimpan atau merahasiakan pesan dari penerima yang tidak berhak. Dalam hal ini pesan asli dari pengirim disebut dengan plainteks, sedangkan pesan yang disembunyikan disebut dengan cipherteks. Pada tulisan ini akan dibahas tentang penerapan aljabar linear khususnya operasi matriks untuk kriptografi. Idenya adalah dengan memilih matriks A berukuran $n\times n$, setiap huruf pada plainteks ditandai dengan angka berdasarkan penomoran menurut ASCII, kemudian plainteks di partisi menjadi sebuah matriks kolom $n\times 1$. Setiap matriks kolom tersebut dikalikan dengan matriks A. Hasil perkalian yang diperoleh dikonversikan kembali kedalam abjad dengan menggunakan aturan modulo aritmatika. Hasil inilah yang menjadi cipherteksnya. Untuk dapat membaca pesan asli dari pengirim, penerima harus mengkonversikan cipherteks ke plainteks dengan algoritma yang sama namun matriks yang digunakan adalah A^{-1}. Dalam kriptografi proses ini disebut sebagai deciphering.

Kriptografi yang dibahas dalam tulisan ini merupakan salah satu seni persandian yang sederhana karena hanya memainkan operasi-operasi dalam matriks. Dalam penggunaannya jika matriks yang digunakan berukuran cukup besar akan sedikit sulit untuk melakukan perhitungan. Sedikit saja melakukan kesalahan akan menyebabkan penerima salah membaca sandi. Oleh karena itu pada tulisan ini diberikan algoritma untuk menerjemahkan hill cipher dalam program Delphi sehingga dapat membantu pengirim dan penerima menjalankan proses konversi teks.

2. KRIPTOGRAFI

Bagian ini membahas konsep-konsep dasar dan istilah-istilah yang digunakan dalam kriptografi. Kriptografi (cryptography) berasal dari bahasa yunani yaitu kripto dan graphia. Kripto berarti menyembunyikan dan graphia artinya tulisan. Jadi secara utuh kriptografi artinya ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti kerahasian data, keabsahan data integritas data dan autentikasi data (Menezes, Oorshot and Vanstone 1996). Selain itu kriptografi juga dapat diartikan sebagai seni atau ilmu dalam menyembunyikan pesan.

Dalam konsep persandian dikenal istilah plainteks dan cipherteks. Pesan asli yang akan disembunyikan disebut sebagai plainteks sedangkan pesan yang akan disembunyikan disebut sebagai cipherteks. Enkripsi adalah proses konversi dari plainteks ke cipherteks sedangkan proses konversi dari cipherteks disebut sebagai dekripsi.

Kebalikan dari kriptografi yaitu ilmu untuk memecahkan kriptografi dengan cara mendapatkan kunci dari cipherteks untuk memperoleh plainteks disebut sebagai Kriptoanalisis (cryptanalysis). Menurut Menezes, Oorshot and Vanstone 1996, kriptografi mempunyai tujuan dasar anatara lain sebagai berikut:

1. Kerahasaian, yaitu aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang mempunyai kewenangan atau kunci rahasia untuk membuka informasi.

2. Integritas data, adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah.
3. Autentikasi, yaitu aspek yang berhubungan dengan identifikasi atau pengenalan baik secara kesatuan system maupun informasi itu sendiri.Pihak yang saling berkomunikasi harus saling memperkenalkan diri.
4. Non repudiation (menolak penyangkalan), merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan.

Algoritma kriptografi atau cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan deskripsi (Schneier, 1996). Algoritma kriptografi terbagi menjadi dua bagian yaitu algoritma simetris dan algortima asimetris.

Algoritma simetris adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci deskripsinya. Dalam hal ini pengirim dan penerima harus menyepakati kunci yang akan dipakai dalam proses komunikasi. Membocorkan kunci kepada orang yang tidak berhak menyebabkan hilangnya kerahasiaan pesan. Jadi keamanan algoritma ini tergantung pada kuncinya. Algoritma ini disebut juga sebagai algortima kunci rahasia atau algoritma satu kunci.

Algoritma asimetris yang disebut juga sebagai algoritma kunci publik menggunakan dua kunci yaitu kunci publik dan kunci rahasia. Kunci publik digunakan untuk mengenkripsi pesan sedangkan kunci rahasia digunakan untuk mendekripsi pesan.

III. OPERASI MATRIKS UNTUK KRIPTOGRAFI

Konsep kriptografi yang merupakan penerapan dari aljabar linier elementer khususnya matriks lebih dikenal dengan *Hill Cipher*. Pada tuliasan ini penulis menganggap bahwa pembaca sudah paham dengan operasi-operasi pada matriks seperti perkalian matriks, mencari determinan matriks dan invers matriks. Sebelum masuk pada algoritma enskripsi dan deksripsi Hill Cipher, penulis perlu menginformasikan bahwa setiap karakter yang ada dalam pesan terlebih dahulu harus dikonversikan kedalam angka-angka yang bersesuain berdasarkan *American Standart Code for Information Interchange (ASCII)*. (Daftar tabel ASCII dapat dilihat dalam lampiran). Pada tulisan ini matriks yang dipakai untuk proses enkripsi dan dekripsi diasumsikan sebagai berikut :

a. Matriks berukuran $2\times 2.$

b. Determinan matriks adalah 1 atau -1.

Berdasarkkan asumsi tersebut berikut diberikan algoritma untuk memperoleh cipherteks secara manual. Proses yang disebut enkripsi ini dilakukan oleh pengirim pesan.

1. Algoritma Enkripsi Hill Cipher

Langkah 1 : Pilih matriks A berukuran 2×2 yang mempunyai determinan 1 dan -1. Setiap elemen dari matriks A merupakan elemen $\mathbb{Z}_{95}$ (bilangan bulat modulo 95). Matriks A adalah kunci rahasia dan harus disepakati dulu antara penerima dan pengirim pesan. Misalkan dipilih matriks $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ berukuran $2\times 2.$

Langkah 2 : Setiap 2 karakter yang berurutan dalam plainteks dijadikan pasangan. Jika dibagian terakhir tersisa 1 karakter, maka tambahkan sebarang *dummy* untuk melengkapi pasangan yang terakhir.

Langkah 3 : Konversikan setiap pasangan plainteks p_1p_2 menjadi sebuah vector kolom $P_1=\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}.$ Kemudian bentuk matriks plainteks dengan setiap kolomnya merupakan vector-vektor kolom tersebut, sehingga diperoleh $P=\left(P_1\ P_2\ P_3.....P_n\ \right).$

Langkah 4 : Selanjutnya lakukan operasi perkalian antara matriks A dengan matriks $P.$

Langkah 5 : Setiap elemen matriks yang diperoleh di Langkah 4 dijadikan bilangan bulat modulo 95 dan hasilnya ditambahkan dengan 32. Terakhir konversikan angka yang diperoleh kedalam karakter yang bersesuain pada ASCII. Hasil bagi tiap elemen dengan 95 disertakan pada bagian terakhir cipherteks dengan aturan jika hasil bagi karakter pertama dengan 95 adalah 0, maka ditulis dengan P, jika hasilnya 1 ditulis Q, jika hasilnya 2 ditulis dengan R demikian seterusnya hingga karakter terakhir.

Sampai pada tahap 5 ini proses enkripsi selesai dan pengirim dapat mengirim pesanya berupa cipherteks yang diperoleh. Selanjutnya adalah tahapan dekripsi yang dilakukan oleh penerima untuk dapat membaca pesan asli dari pengirim. Untuk itu diberikan algoritmanya sebagai berikut.

2. Algoritma Dekripsi Hill Cipher

Algoritma dekripsi sejalan dengan proses enkripsi, namun matriks kunci yang digunakan adalah invers dari matriks $A.$

Langkah 1 : Setiap huruf pada cipherteks yang berupa karakter ASCII didikonversikan kedalam angka yang bersesuain, kemudian dikurangi dengan 32.

Langkah 2 : Setiap elemen matriks pada Langkah 1 dijumlahkan dengan kelipatan 95 sesuai dengan karakter hasil bagi pada cipherteks, yaitu 0 untuk P, 95 untuk Q, 190 untuk R dan seterusnya.

Langkah 3 : Matriks yang diperoleh pada Langkah 2 dikalikan dengan A^{-1}, sehingga diperoleh matriks plainteks P. Konversikan bilangan pada matriks P kedalam karakter ASCII yang bersesuaian.

Untuk dapat mengkonversikan dengan benar, pembaca diharapkan telah memahami aturan modulo (konsep sisa hasil bagi). Berikut diberikan contoh penggunaan algoritma diatas dengan perhitungan manual. Kemudian pada bagian selanjutnya algoritma tersebut akan dijalankan dalam program Delphi sehingga proses perhitungan konversi lebih cepat dan meminimumkan terjadinya kesalahan perhitungan.

Contoh: Agung akan mengirim sebuah pesan rahasia kepada Beni, untuk itu mereka telah menyepakati sebuah matriks rahasia sebagai kunci yaitu $A=\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}$. Pesan yang akan di kirim agung adalah kamu dimana?. Lakukan proses enkripsi dan dekripsi yang harus dilakukan Agung dan Beni.

Solusi :

a. Proses Enkripsi.

Plainteks dipasangkan sesuai dengan urutanya. Kemudian konversikan masing-masing karakter kedalam bilangan ASCII yang bersesuaian sehingga diperoleh matriks kolom

$$P_1=\begin{pmatrix}107\\ 97\end{pmatrix}, P_2=\begin{pmatrix}109\\ 117\end{pmatrix}, P_3=\begin{pmatrix}32\\ 100\end{pmatrix},$$

$$P_4=\begin{pmatrix}105\\ 109\end{pmatrix}, P_5=\begin{pmatrix}97\\ 110\end{pmatrix} \text{ dan } P_6=\begin{pmatrix}97\\ 63\end{pmatrix}.$$

Dengan menguunakan perkalian matriks diperoleh hasil berikut :

$$AP=\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}107 & 109 & 32 & 105 & 97 & 97\\ 97 & 117 & 100 & 109 & 110 & 63\end{pmatrix}$$

$$=\begin{pmatrix}97 & 117 & 100 & 109 & 110 & 63\\ 301 & 343 & 232 & 323 & 317 & 223\end{pmatrix}$$

$$=\begin{pmatrix}2_1 & 22_1 & 5_1 & 14_1 & 15_1 & 63_0\\ 16_3 & 58_3 & 42_2 & 38_3 & 32_3 & 33_2\end{pmatrix}.$$

Matriks cipherteks diperoleh dengan menambahkan setiap elemen matriks AP dengan 32. Sehingga diperoleh matriks

$$C=\begin{pmatrix}34_1 & 54_1 & 37_1 & 46_1 & 47_1 & 95_0\\ 48_3 & 90_3 & 74_2 & 70_3 & 64_3 & 65_2\end{pmatrix}.$$

Indeks pada matriks diatas merupakan hasil bagi bilangan dengan 95. Setelah dikonversikan kedalam ASCII cpherteksnya adalah "06Z%J.F/@_AQSQSQRQSQSPR.

b. Proses Dekripsi

Untuk dapat mengetahui banyaknya karakter cipherteks yang asli, maka jumlah karakter cipherteks yang diterima dibagi menjadi dua. Untuk pesan "06Z%J.F/@_AQSQSQRQSQSPR, ada sebanyak 12 karakter yang harus dibaca. Analog seperti proses enkripsi, setiap dua huruf pada pesan cipherteks dipasangkan, sehingga diperoleh pasangan "0 6Z %J .F /@ _A . Kemudian konversikan tiap pasangan kedalam angka berdasarkan kode ASCII, diperoleh

$$C_1=\begin{pmatrix}34\\ 48\end{pmatrix}, C_2=\begin{pmatrix}54\\ 90\end{pmatrix}, C_3=\begin{pmatrix}37\\ 74\end{pmatrix},$$

$$C_4=\begin{pmatrix}46\\ 70\end{pmatrix}, C_5=\begin{pmatrix}47\\ 64\end{pmatrix}, \text{ dan } C_6=\begin{pmatrix}95\\ 65\end{pmatrix}.$$

Setiap elemen vektor C_i dikurangi dengan 32 dan hasilnya dijumlahkan dengan kelipatan 95 berdasarkan karakter hasil baginya, sehingga diperoleh matriks

$$C'=\begin{pmatrix}97 & 117 & 100 & 109 & 110 & 95\\ 301 & 343 & 232 & 323 & 317 & 65\end{pmatrix}.$$

dan matriks plainteks

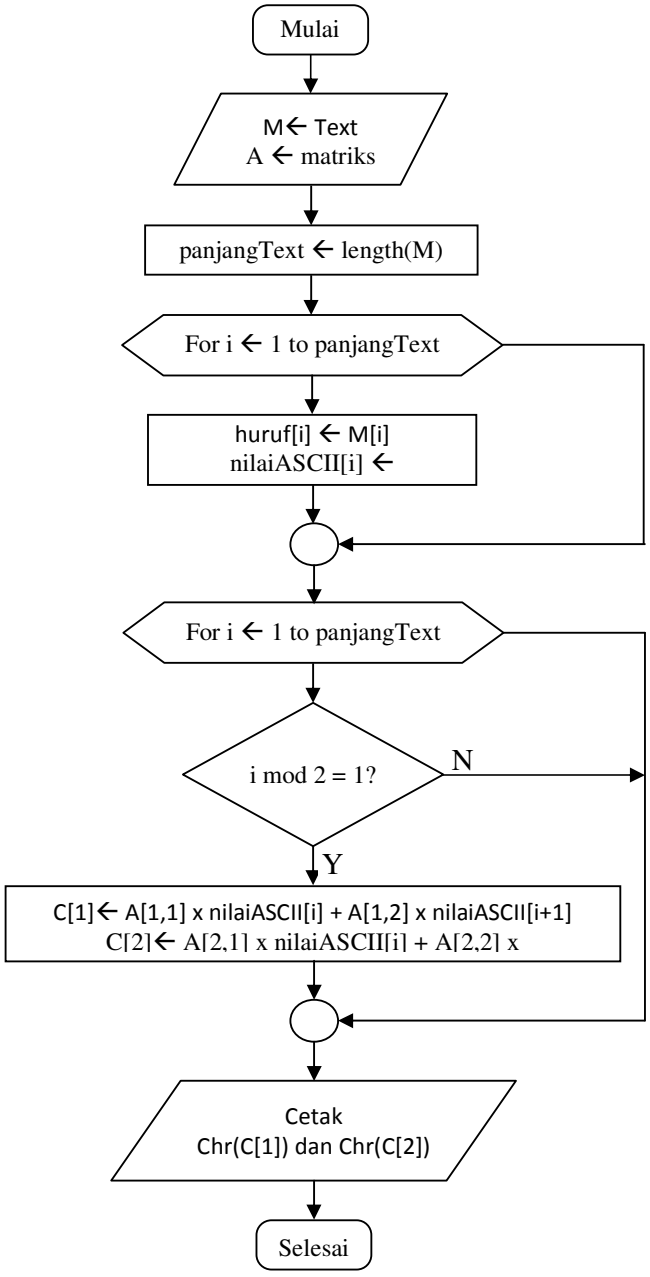
$$P=A^{-1}C'=\begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}97 & 117 & 100 & 109 & 110 & 95\\ 301 & 343 & 232 & 323 & 317 & 65\end{pmatrix}$$

$$=\begin{pmatrix}107 & 109 & 32 & 105 & 97 & 97\\ 97 & 117 & 100 & 109 & 110 & 63\end{pmatrix}.$$

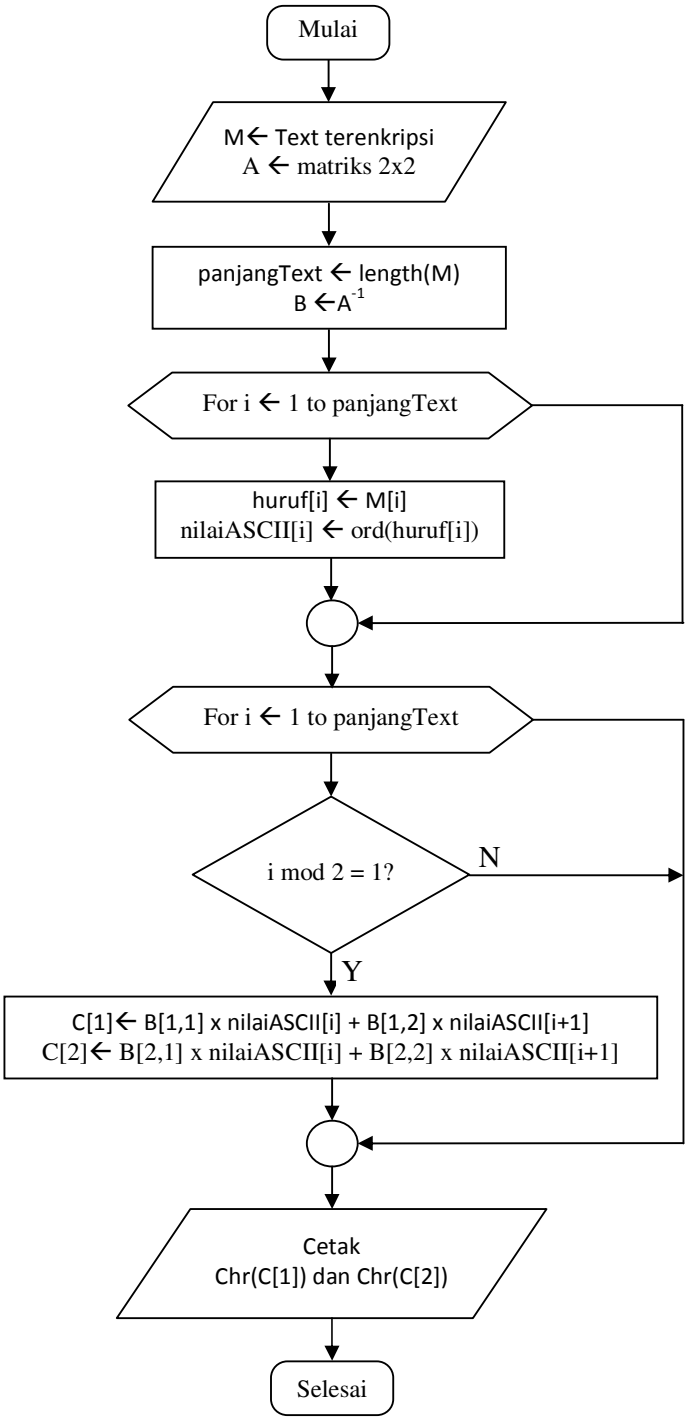
Setelah dikonversikan dapat terbaca pesan aslinya adalah kamu dimana? .

Jika teks yang akan dikirim dalam jumlah yang banyak, tentu saja cara manual ini akan sulit untuk dilakukan, untuk itu dalam paper ini juga diberikan program untuk melakukan proses enkripsi dan dekripsi. Algoritma program hill cipher ini digambarkan dalam diagram flow chart sebagai berikut :

FLOW CHART PROSES ENKRIPSI DAN DEKRIPSI TEKS HILL CIPHER DENGAN MATRIKS

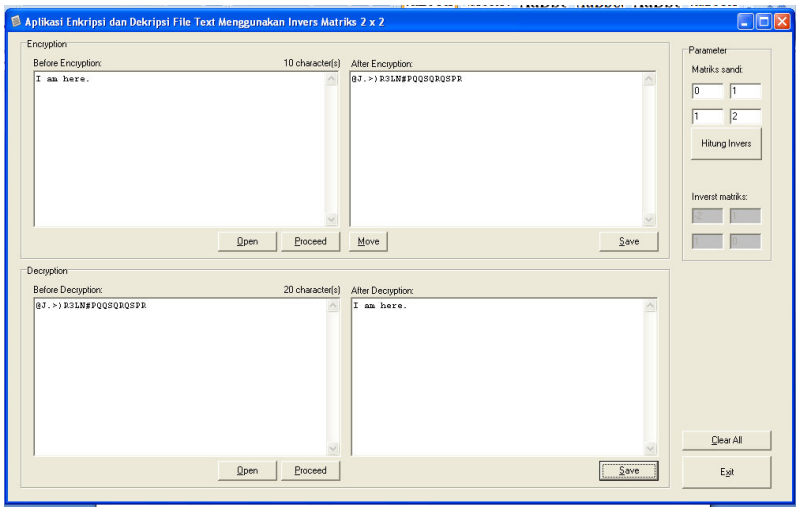


Gambar 1 Proses Enkripsi



Gambar 2 Proses Dekripsi

Berdasarkan Flow Chart Gambar 1 dan Gambar 2, berikut diberikan output Hill chiper yang dikerjakan dalam Delphi.



Gambar 3. Program Hill Chiper pada Delphi

3. KESIMPULAN

Hill Cipher dengan menggunakan operasi matriks ini merupakan salah satu contoh kriptografi yang sederhana. Dengan memanfaatkan kode karakter ASCII dan operasi matriks, proses enkripsi dan dekripsi dapat dilakukan oleh pengirim dan penerima pesan secara manual. Jika teks yang dikirim cukup panjang sehingga menyulitkan pengguna hill cipher untuk melakukan perhitungan secara manual, dapat dilakukan dengan menggunakan program komputer seperti yang sudah diberikan pada bagian sebelumnya.

4. SARAN

Hill Cipher yang dijelaskan dalam paper ini merupakan contoh sederhana dari kriptografi yang memanfaatkan kode ASCII. Beberapa tulisan telah menjelaskan algoritma hill chipper yang sedikit berbeda dan tidak menggunakan ASCII sebagai pengkonversi karakter pada teksnya. Paper ini masih bisa dikembangkan lebih luas dengan memperluas asumsi matriks kuncinya. Misalnya determinan matriks kunci tidak harus 1 dan -1 sehingga hasil invers matriks bukan merupakan bilangan bulat. Masalah ini dapat diselesaikan dengan menggunakan Modular aritmatika yaitu *reciprocal* atau *multiplicative inverse.*

5. DAFTAR PUSTAKA

[1]. Anonim, 2010, *Hill Cipher*, [online], (http://en.wikipedia.org/wiki/Hill_cipher, diakses tanggal 14 Juli 2010).

[2]. Anton, H., and Rorres, C., 2000, *Elementary Linear Algebra* Apllications Version, New York.

[3]. Menezes, Oorcshot, and Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, Inc. USA.

[4]. Riyanto, M., Z., 2007, *Pengamanan Pesan Rahasia Menggunakan Algortima Kriptografi Elgamal atau Grup Pergandaan* Z_{p^*}, Universitas Gadjah Mada, Yogyakarta.

[5]. Schneier, Bruce, 1996, *Applied Cryptography, Second Edition: Protocol, Algorithms and Source Code in C*, John Wiley and Sons, Inc.

[6]. Shiefloe, P., 2001, *Cryptography : Hill Ciphers*, [online], (http://www.math.washington.edu/~king/coursedir/m308a01/Projects/Cryptography.htm, diakses tanggal 14 Juli 2010).

[7]. Wikipedia, 2006, *Cryptography*, [online], (http://en.wikipedia.org/wiki/Cryptography, diakses 10 Juli 2010).