T – 22

Studi dan Implementasi Hill Cipher menggunakan binomial newton berbasis komputer

Rojali

Jurusan Matematika , School Of School of Computer Science
Binus University,
Jakarta, Indonesia 11480
email: rojali@binus.edu

Abstrak

Algoritma Hill Cipher adalah salah satu algoritma kunci simetris yang memiliki beberapa kelebihan dalam enkripsi data. Untuk menghindari matrik kunci yang tidak *invertible*, matrik kunci dibangkitkan menggunakan koefisien binomial newton. Proses enkripsi dan deskripsi menggunakan kunci yang sama, plaintext dapat menggunakan media gambar atau text. Menggunakan pengujian komputer dengan bahasa pemrograman Delphi 7.0, hasil pengujian komputer menunjukkan bahwa waktu yang diperlukan untuk proses enkripsi dan deskripsi tidak lebih dari 5 detik.

Keyword : Hill Cipher, Binomial Newton, Berbasis Komputer

Pendahuluan

Perkembangan teknologi informasi sekarang ini membuat komunikasi menjadi semakin mudah dan luas. Penyampaian pesan melalui internet merupakan sarana komunikasi yang sangat mudah dan efisien. Sejalan dengan hal itu kemunculan dari file-file multimedia yang beraneka ragam memberi pengaruh yang cukup besar dalam kemajuan teknologi informasi ini sehingga memungkinkan seseorang untuk dapat menyampaikan pesan menggunakan file-file multimedia tersebut. Faktor keamanan menjadi penting dalam proses pengiriman data melalui saluran internet. Apabila hal ini diabaikan, maka orang yang tidak berhak akan dengan mudah memanfaatkan data tersebut untuk tujuan tertentu. Jika hal ini terjadi ada dua pihak yang dirugikan yaitu pengirim data dan penerima data. Salah satu metode untuk mengamankan data tersebut adalah dengan menyamarkan menjadi tidak bermakna. Kriptografi adalah metode untuk menyamarkan data menjadi tidak bermakna. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu :

- Algoritma *simetris*

  Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama
- Algoritma *asimetris*

  Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

Sedangkan berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma kriptografi dapat dibedakan menjadi dua jenis yaitu :

- Algoritma *block cipher*

  Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-bit) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama.
- Algoritma stream cipher

  Informasi/data yang hendak dikirim dioperasikan dalam bentuk blok-blok yang lebih kecil (byte atau bit), biasanya satu karakter persatuan persatuan waktu proses, menggunakan tranformasi enkripsi yang berubah setiap waktu.

Pada makalah ini akan dibahas algoritma kunci simetris dengan menggunakan koefisien binomial newton sebagai pembangkit kunci.

Binomial Newton

Binomial Newton adalah uraian binomium (suku dua), yaitu bentuk (a+b). Apabila binom (a+b) dipangkatkan dengan n (n $\in$ bilangan asli), maka didapat bentuk :

$$(a+b)^n$$

Hasil penjabaran $(a+b)^n$ bergantung pada nilai n, sebagai contoh :

Untuk $n=1 \rightarrow (a+b)^1 = (1)\,a^1b^0 + (1)\,a^0b^1$

$n=2 \rightarrow (a+b)^2 = (1)\,a^2b^0 + (2)\,a^1b^1 + (1)\,a^0b^2$

$n=3 \rightarrow (a+b)^3 = (1)\,a^3b^0 + (3)\,a^2b^1 + (3)\,a^1b^2 + (1)\,a^0b^3$

$n=4 \rightarrow (a+b)^4 = (1)\,a^4b^0 + (4)\,a^3b^1 + (6)\,a^2b^2 + (4)\,a^1b^3 + (1)\,a^0b^4$

$n = 5 \rightarrow (a+b)^5 = (1)\, a^5b^0 + (5)\, a^4b^1 + (10)\, a^3b^2 + (10)\, a^2b^3 (5)\, a^1b^4 + (1)\, a^0b^5$

Bila di rumuskan, maka :

$$(a+b)^n = C_n^0\, a^n + C_n^1 a^{n-1}b^1 + ... + C_n^{n-1} ab^{n-1} + C_n^n a^n b^n$$

Koefisien-koefisien binomium :

$$C_n^0 = 1$$

$$C_n^1 = \frac{n!}{1!(n-1)!} = \frac{n(n-1)!}{(n-1)!} = \frac{n}{1}$$

$$C_n^2 = \frac{n!}{2!(n-2)!} = \frac{n(n-1)(n-2)!}{2!(n-2)!} = \frac{n(n-1)}{2!}$$

Rumus tersebut dapat juga ditulis sebagai :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^{n-k} b^k$$

Teknik Hill Cipher

Hill Cipher merupakan penerapan dari aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan proses enkripsi dan deskripsi. *Hill Cipher* diciptakan oleh Lester Hill pada tahun 1929 (Stallings, 2003). *Cipher* (kode) yang sudah diperoleh tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher* tidak mengganti setiap abjad yang sama pada plainteks dengan abjad lainnya yang sama pada cipherteks karena menggunakn perkalian matriks pada dasar enkripsi dan deskripsinya. Jika kriptanalis hanya mengetahui cipherteks saja maka akan sulit menemukan plainteks, namun jika kriptanalis memiliki berkas cipherteks dan potongan berkas plainteks maka teknik ini akan sangat mudah dipecahkan.

Algoritma Enkripsi Hill Cipher

Tahapan-tahapan algoritma enkripsi Hill Cipher sebagai berikut :

1. Korespondenkan abjad dengan numerik

   $A \rightarrow 1, B \rightarrow 2, ..., Z \rightarrow 26$
2. Buat matriks kunci berukuran m x m

$$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

3. Matrik K merupakan matriks *yang invertible* yaitu memiliki *multiplicative inverse* K^{-1} sehingga $K.K^{-1} = 1$

4. Plainteks $P = p_1 p_2 \dots p_n$, diblok dengan ukuran sama dengan baris atau kolom matrik K, sehingga

$$P_{qxm} = \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1m} \\ p_{21} & p_{22} & \dots & p_{2m} \\ \dots & \dots & \dots & \dots \\ p_{q1} & p_{q2} & \dots & p_{qm} \end{bmatrix}$$

5. Matrik P di transpose menjadi

$$P^t_{mxq} = \begin{bmatrix} p_{11} & p_{21} & \dots & p_{1q} \\ p_{12} & p_{22} & \dots & p_{2q} \\ \dots & \dots & \dots & \dots \\ p_{1m} & p_{2m} & \dots & p_{qm} \end{bmatrix}$$

6. Kalikan Matrik K dengan Matrik P transpose dalam modulo 26

$$C^t = K_{mxm} P^t_{mxq}$$

$$C^t = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \dots & p_{1q} \\ p_{12} & p_{22} & \dots & p_{2q} \\ \dots & \dots & \dots & \dots \\ p_{1m} & p_{2m} & \dots & p_{qm} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{21} & \dots & c_{m1} \\ c_{12} & c_{22} & \dots & c_{m2} \\ \dots & \dots & \dots & \dots \\ c_{1q} & c_{2q} & \dots & c_{mq} \end{bmatrix}$$

7. Kemudian ditransposekan

$$C = (C^t)^t = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1q} \\ c_{21} & c_{22} & \dots & c_{2q} \\ \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & \dots & c_{mq} \end{bmatrix}$$

8. Ubah hasil langkah ke-7 kedalam abjad menggunakan koresponden abjad dengan numerik pada langkah 1 sehingga diperoleh cipherteks

Algoritma Deskripsi Hill Cipher

1. Korespondekan abjad dengan numerik

   $A \to 1, B \to 2, \dots, Z \to 26$

2. Ubah cipherteks kedalam numerik

3. Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matrik kunci K_{mxm}
4. Menghitung K^{-1}
5. Kalikan invers matriks kunci dengan cipherteks transpose dalam modulo 26, diperoleh plainteks transpose $P^t = K^{-1}C^t$
6. Dari langkah ke-5 diperoleh $P = (P^t)^t$
7. Korespondensikan abjad dengan numerik hasil langkah 6 diperoleh plainteks

Pembahasan
Proses Enkripsi
Untuk membahas proses enkripsi dan dekripsi dipilih contoh plaintext "**SERANG**".

Matrik kunci yang diperoleh dari koefisien binomial ukuran 3 x 3 , $K_{3x3} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{bmatrix}$,

Koresponden plaintext dengan tabel abjad

S	E	R	A	N	G
19	5	18	1	14	7

Didapat bilangan desimal dalam Z_{26} untuk plainteks SERANG yaitu 19,5,18,1,14,7 sehingga diperoleh plainteks $P = [19 \quad 5 \quad 18 \quad 1 \quad 14 \quad 7]$. Karena matrik kunci berukuran 3x3 maka matriks plainteks yang diambil adalah $P = [19 \quad 5 \quad 15]$, matriks P di transpose menjadi $P^t = \begin{bmatrix} 19 \\ 5 \\ 15 \end{bmatrix}$. Kemudian matriks kunci dikalikan dengan matriks P yang sudah ditranspose $C^t = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 5 \\ 15 \end{bmatrix} = \begin{bmatrix} 42 \\ 47 \\ 48 \end{bmatrix} \bmod 26 = \begin{bmatrix} 16 \\ 21 \\ 10 \end{bmatrix}$,

$C = (C^t)^t = [16 \quad 21 \quad 10]$, korespondensikan matrik C dengan tabel abjad dengan **"PUJ"**, dengan cara yang sama untuk plainteks $P = [1 \quad 14 \quad 7]$, diperoleh cipherteks

$C = \left(C^t\right)^t = [22 \quad 10 \quad 12]$ dan dikorespondenkan diperoleh **"VJL"** , sehingga cipherteks dari plainteks "**SERANG**" adalah "**PUJVJL**"

Proses Dekripsi

Cipherteks yang sudah diperoleh akan di dekripsi sehingga akan menjadi kata yang mempunyai makna. Cipherteks "**PUJVJL**" dikoresponden dengan tabel abjad menjadi

P	U	J	V	J	L
16	21	10	22	10	12

Sehingga cipherteks menjadi $C = [16 \quad 21 \quad 10 \quad 22 \quad 10 \quad 12]$, karena ukuran matriks kunci 3x3 sehingga cipherteks dibagi menjadi 2 yaitu $C = [16 \quad 21 \quad 10]$ dan $C = [22 \quad 10 \quad 12]$.

Invers dari Matriks Kunci $K^{-1} = \begin{bmatrix} 1.5 & 0 & -0.5 \\ -1 & 1 & 0 \\ 0.5 & -1 & 0.5 \end{bmatrix}$, kalikan matriks K^{-1} dengan matriks C^t, $P^t = K^{-1}C^t = \begin{bmatrix} 1.5 & 0 & -0.5 \\ -1 & 1 & 0 \\ 0.5 & -1 & 0.5 \end{bmatrix} \begin{bmatrix} 16 \\ 21 \\ 10 \end{bmatrix} = \begin{bmatrix} 19 \\ 5 \\ -8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 5 \\ 18 \end{bmatrix}$, selanjutnya matriks P di transpose menjadi $P = (P^t)^t = [19 \quad 5 \quad 18]$. Dengan cara yang sama dengan mengambil $C = [22 \quad 10 \quad 12]$ diperoleh matriks $P = (P^t)^t = [1 \quad 14 \quad 7]$ dengan mengabungkan kedua plainteks maka nilai $P = [19 \quad 5 \quad 18 \quad 1 \quad 14 \quad 7]$ dan jika dikorespondesikan dengan tabel abjad menjadi "**SERANG**" sama dengan plainteks awal.

Kesimpulan

Berdasarkan pembahasan diatas kesimpulan yang dapat diambil adalah :

1. Koefisien binomial dapat dijadikan sebagai matrik kunci
2. Matriks kunci *hill cipher* harus matriks yang *invertible*
3. Setiap pesan yang dienkripsi harus mempunyai panjang kelipatan dari n yaitu banyaknya kolom pada matriks kunci.
4. Hasil enkripsi plainteks yang sama dengan menggunakan matriks kunci yang berbeda akan menghasilkan cipherteks yang berbeda.

Saran

1. Untuk meningkatkan keamanan algoritma hill cipher dapat dikombinasikan dengan teknik lain misalkan steganografi

Daftar Pustaka

1. Anton, Howard, Rorres, Chris, Elementary linear algebra, John Wiley & Sons, 2011

2. Forouzan, Behrouz, Cryptography and Network Security, McGraw-Hill, 2006

3. Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, 2006

4. Stallings, William, Cryptography and Network Security, Prentice Hall, 2003