PENERAPAN METODE VIGENERE PADA KRIPTOGRAFI KLASIK UNTUK PESAN RAHASIA

Hamdani

Program Studi Ilmu Komputer FMIPA Universitas Mulawarman
Email : hamdani@ilkom.unmul.ac.id

ABSTRAK

Pesan rahasia dapat diterapkan pada ilmu kritografi, kriptografi adalah studi mengenai ilmu dan seni dalam rangka menjaga keamanan data atau informasi yang dikirim serta merupakan ilmu untuk bagaimana memecahkan pesan yang terenkripsi (tersamar). Kriptografi juga merupakan ilmu seni penenksripsian dan deskripsian data dapat berupa teks, gambar, atau suara. Tujuan penerapan kriptografi adalah untuk membuat sesuatu yang tersembunyi, dapat suatu pesan rahasia berupa teks, suara, gambar dan video.

Penerapan metode *vigenere* kriptografi untuk membuat aplikasi kriptosistem dalam suatu teks rahasia yang dibutuhkan agar setiap pesan yang kita miliki tidak dapat dibaca oleh pembajak. Pengembangan sistem menggunakan metode *vigenere* dapat membuat suatu pesan rahasia tidak mudah dibaca langsung bagi orang lain. Pengirim (*sender*) pesan teks asli (*plaintext*) berupa suatu kalimat yang dienkripsi oleh kriptosistem untuk mengacak pesan aslinya dengan memberikan kunci (*key*) menjadi *ciphertext* dan dapat dikembalikan ke pesan aslinya atau didekripsikan.

Kata Kunci: *Pesan Rahasia, Kriptografi, Vigenere.*

PENDAHULUAN

Suatu pesan rahasia dapat diterapkan pada ilmu kriptografi yang merupakan suatu ilmu seni dengan filosofinya *the art of war*, dimana waktu tersebut pernah digunakan untuk mengirim pesan rahasia pada jaman romawi pada era raja Julius Caesar. Tujuannya agar pembajak surat rahasia tidak dapat membaca pesannya secara langsung oleh orang lain jika belum dideskripsikan dengan metode tertentu. Kritografi adalah studi mengenai ilmu dan seni dalam rangka menjaga keamanan data atau informasi yang dikirim dan juga merupakan ilmu untuk bagaimana memecahkan pesan yang terenkripsi (tersamar).

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim dan 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. Ada beberapa contoh macam-macam metode kriptografi untuk membuat pesan rahasia antara lain: *Caesar*, *Affine*, *Monoalphabetic*, *Polyalphabetic*, *Vigenere*, *Beaufort*, *Playfair*, Transposisi, MD5, DES, RSA, DSA, ElGamal, dan SHA. Metode pertama kriptografi adalah Caesar, yang mana metode mengikuti pola pesan rahasia yang dikirim oleh raja Caesar pada jaman romawi, kini banyak model untuk dapat diterapkan dalam kriptografi, diantaranya adalah *Vigenere*. *Vigenere* sudah cukup baik untuk mengirim pesan rahasia berupa pesan teks rahasia.

Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (*plaintext*) atau teks jelas atau asli (*cleartext*). Berdasarkan jurnal Informatika Mulawarman pada penulis Anindita Septiarini dan Hamdani pada judul " Sistem Kriptografi Untuk *Text Message* Menggunakan Metode *Affine*" Volume 6 Nomor 1 Edisi Februari 2011 Hal. 50-53. Maka diperlukan membuat aplikasi pesan rahasia berupa teks menggunakan metode lain seperti *Vigenere* yang merupakan perluasan dari *caesar* dan metode-metode kriptografi lainnya yang mengalihkan plainteks, [1,5].

LANDASAN TEORI

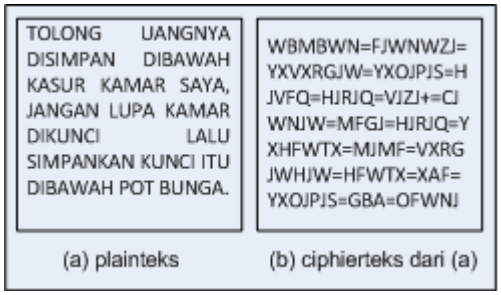
Kriptonologi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga [4]. Kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman (*secure*). Tujuan penerapan kriptografi adalah untuk membuat sesuatu yang tersembunyi, dapat suatu pesan rahasia berupa teks, suara, gambar dan video. Di

dalam kriptografi sering ditemukan berbagai istilah atau terminologi, beberapa istilah yang penting untuk diketahui diantaranya adalah, [2]:

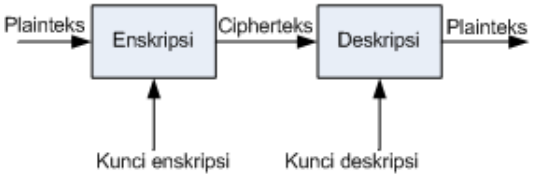
- Pesan (*message*) adalah data atau informasi yang dapat dibaca atau dimengerti maknanya. Nama lainnya untuk pesan adalah plainteks (*plaintext*) atau teks jelas (*clear text*).
- Pengirim (*sender*) adalah entitas yang melakukan pengiriman pesan kepada entitas lainnya.
- Kunci (*cipher*) adalah aturan atau fungsi matematika yang digunakan untuk melakukan proses enkripsi dan dekripsi pada plaintext dan *ciphertext*.
- Enkripsi adalah mekanisme yang dilakukan untuk merubah plaintext menjadi *ciphertext*.
- Dekripsi adalah mekanisme yang dilakukan untuk merubah *ciphertext* menjadi *plaintext*.
- Penerima (*recipient*) adalah entitas yang menerima pesan dari pengirim/entitas yang berhak atas pesan yang dikirim.

Pengubahan plainteks ke cipherteks agar suatu pesan rahasia tidak mudah dibaca.



Gambar 1. Proses Enskripsi Teks

Gambar 1. memperlihatkan contoh dua buah plainteks serta cipherteks berkoresponden. Yang mana suatu proses pesan yang dikembalikan, cipherteks dapat ditransformasikan kembali ke plainteks semula, [2]. Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti. Adapun gambar diagram proses plainteks ke enkripsi dan cipterteks ke deskipsi dapat dilihat pada gambar 2.



Gambar 2. Diagram proses enkripsi dan dekripsi

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui. Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M *(plaintext)* sehingga dihasilkan C *(ciphertext)*, notasinya :

$$\mathbf{E_e(M) - C} \qquad (1)$$

Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (*desciption*) menggunakan d (kunci dekripsi) pada C *(ciphertext)* sehingga dihasilkan M *(plaintext)*, notasinya :

$$\mathbf{D_d(C) = M} \qquad (2)$$

Sehingga dari dua hubungan diatas berlaku :

$$\mathbf{D_d(E_e(M)) = M} \qquad (3)$$

Vigenere Cipher

Vigenere cipher adalah sebuah contoh terbaik dari cipher alphabet-majemuk manual. Algoritma *vigenere* dipublikasikan oleh diplomat sekaligus seorang kriptologis di Prancis, yaitu Blaise de Vigenere pada abad 16. *Vigenere Cipher* menggunakan bujursangkar *vigenere* untuk melakukan enkripsi, [2].

Tahapan Vigenere

Untuk tahapan pertama yang perlu dipahami adalah tabel bujursangkar pada *vigenere* dalam membuat suatu kelomok huruf dalam pertemuan plainteks ke kunci. Adapun keterangan bujursangkar *vigenere* dapat dilihat seperti pada tabel 1.

Tabel 1. Bujursangkar *Vigenere*

Huruf	A	B	C	...	...	X	Y	Z
a	A	C	D	...	...	X	Y	Z
b	B	D	E	...	...	Y	Z	A
c	C	E	F	...	...	Z	A	B
d	E	F	G	...	...	A	B	C
e	F	G	H	...	...	B	C	D
...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...
z	Z	A	B	...	...	W	X	Y

Setiap huruf plainteks akan dienkripsi dengan setiap huruf kunci dibawahnya. Untuk mengerjakan enkripsi dengan *Vigenere Cipher*, dilakukan pada bujursangkar *Vigenere* sebagai garis vertical dari huruf plainteks ke bawah dan bujur mendatar dari kiri ke kanan. Perhatikan pertemuan (blok) plainteks huruf horizontal pada **Y** dan huruf vartikal pada kunci di huruf **E**, maka dapat

disimpulkan pertemuan huruf pada **C** atau dapat dilihat seperti pada tabel 2.

Tabel 2. Contoh Enkripsi huruf X dengan kunci E

Huruf	A	B	C	...	...	X	**Y**	Z
a	A	C	D	...	...	X	Y	Z
b	B	D	E	...	...	Y	Z	A
c	C	E	F	...	...	Z	A	B
d	E	F	G	...	...	A	B	C
e	F	G	H	...	...	B	**C**	D
...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...
z	Z	A	B	...	...	W	X	Y

Hal ini merupakan karakteristik dari cipher alfabet-majemuk. Pada cipher substitusi sederhana, setiap huruf cipherteks selalu menggantikan huruf plainteks tertentu, sedangkan pada cipher alphabet-majemuk setiap huruf cipherteks dapat memiliki kemungkinan banyak huruf plainteks. Maka, dengan menggunakan Vigenere Cipher, dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama sebagaimana yang diperlihatkan cipherteks substitusi sederhana (ciperteks alphabet-tunggal), [2].

Misal enkripsi contoh pada tulisan sebagai berikut:

Plainteks : Y A N T O K
Kunci : E K O E K O
Cipherteks : C K B X Y Y

Secara matematis, misalkan kunci dengan panjang m adalah rangkaian $K_1K_2 \ldots K_m$, plainteks adalah rangkaian $P_1P_2 \ldots P_t$ dan cipherteks adalah rangkaian $C_1C_2 \ldots C_t$, maka enkripsi pada *Vigenere Cipher* dapat dinyatakan sebagai berikut:

$$C_1 = (P_1 + K_r) \bmod 26 \quad (1 \le i \le t) \qquad (4)$$

dan

$$i = (\bmod m) \qquad (1 \le r \le t) \qquad (5)$$

Atau pada persamaan perhitungannya adalah sebagai berikut:

Y + E mod 26 = (24+4) mod 26 = 2 = **C**

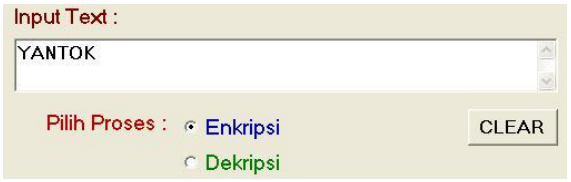
Tabel 3. Penginisialan Alfabet Huruf A-Z menjadi Angka 0 - 25

Huruf	A	B	C	...	...	X	Y	Z
Angka	0	1	2	...	...	23	24	25

HASIL DAN PEMBAHASAN

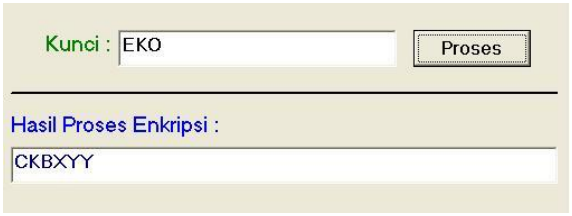
Gambaran Umum Sistem

Hasil penelitian yang didapatkan adalah telah diterapkan ilmu kriptografi dengan metode *Vigenere* untuk menghasilkan pesan teks rahasia. Teks asli dapat di ubah menjadi teks yang disamarkan dengan suatu metode *Vigenere*, dan teks yang telah di enksripsi dapat dikembalikan kembali menjadi teks asli (*plaintext*). Jika diujikan dengan plainteks **YANTOK** dengan Kata Kunci **EKO** seperti terlihat pada gambar 3.



Gambar 3. Inputan plainteks

Maka menghasilkan data yang akan di enkripsi seperti terlihat pada gambar 4.



Gambar 4. Hasil Enkripsi

Untuk menguji pada dekripsi pesan teks pesan rahasia tersebut dapat dilihat seperti pada gambar 5.

Gambar 5. Pensan Teks Dekripsi

Pesan teks yang di terima adalah hasil data yang telah didekripsikan oleh penerima dari *sender* (pengirim pesan).

Pengujian Plainteks

Pengujian data plainteks digunakan agar teks asli dapat di enskripsi menjadi *ciphertext*. Contoh data *plaintext* untuk pengujian system dapat dibutuhkan pesan rahasia sebagai berikut:

INI PESAN RAHASIA SAYA TOLONG JANGAN KAMU SAMPAIKAN KE ORANG LAIN KARNA INI SANGAT PENTING

Adapun pengujian aplikasi untuk enkripsi data pada pesan teks dapat dilihat seperti pada gambar 6.

Gambar 6. Pengujian Enkripsi Pada Pesan Rahasia

KESIMPULAN

Pesan teks rahasia dapat digunakan untuk mengirim pesan atau sesuatu yang sifatnya tidak dapat diketahui orang lain seperti mengirim pesan rahasia. Dimana teks asli (*plaintext*) di ekripsi menjadi teks yang samar (*ciphertext*) yang dapat membantu dalam pertukaran pesan berupa teks. Jumlah banyak teks pada plainteks yang di isi tidak dibatasi. Maka pesan dikirim dapat berupa isi surat rahasia yang mana pesan tersebut dipindahkan ke dalam system tersebut kemudian diproses untuk enkripsi, sedangkan penerima pesan harus memiliki aplikasi yang sama (metode yang sama) untuk dapat membuka pesan teks rahasia tersebut.

DAFTAR PUSTAKA

[1] Hamdani, 2007. Tugas Aplikasi Kriptografi, Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

[2] Munir, R., 2006, *Kriptografi*, Informatika, Bandung.

[3] Piper, F dan Sean, M. 2002. Cryptography, A Very short Introduction. Oxford.

[4] Stalling, W. 1998. Cryptography and Network Security, Principle and Practice 2nd Edition. Pearson Education, Inc.

[5] Septiarini, A. dan Hamdani. 2011. Sistem Kriptografi Untuk *Text Message* Menggunakan Metode *Affine*" Volume 6 Nomor 1 Hal. 50-53.