PERBANDINGAN METODE VIGENERE DAN AFFINE UNTUK PESAN RAHASIA

Hamdani

Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Mulawarman Samarinda, Kalimantan Timur
e-mail : iniemaildani@yahoo.com

Abstrak

Banyaknya metode pada kriptografi menjadi pilihan dalam mengembangkan sistem pengamanan data pada pengiriman pesan rahasia (*secret message*). Suatu aplikasi 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.

Perbandingan metode dapat diterapkan dalam membedakan tingkat keamanan pada metode *vigenere* dan *affine* di ilmu kriptografi untuk membuat aplikasi yang berguna mengirim pesan rahasia. Kebutuhkan agar setiap pesan yang dimiliki tidak dapat dibaca langsung oleh pembajak. Perbandingan metode juga bertujuan dalam mengupayakan mencari suatu metode yang tepat dan lebih baik untuk menyamarkan pesan rahasia. Pengembangan sistem menggunakan metode *vigenere* dan *affine* dapat digunakan untuk membuat suatu pesan rahasia dengan inputan kunci yang berbeda dengan inputan pesan *Plaintext* yang sama. 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. Adapun kunci pada *vigenere* burupa huruf alphabet sedangkan kunci pada *affine* menggunakan angka dengan bilangan prima.

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

.

LATAR BELAKANG

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 (*cipher*). Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal (*plain*). 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, RC4 atau RC5 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 *affine* dan *vigenere* metode kriptografi klasik. *Affine* dan *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 Plaintext (*Plaintext*) atau teks jelas atau asli (*cleartext*). Berdasarkan jurnal Informatika Mulawarman penulis Septiarini dan Hamdani pada judul " Sistem Kriptografi Untuk *Text Message* Menggunakan Metode *Affine*" Volume 6 Nomor 1 Edisi Februari 2011 Halaman 50-53. Dan jurnal Informatika Mulawarman penulis Hamdani dengan judul "Penerapan Metode Vigenere Pada Kriptografi Klasik untuk Pesan Rahasia" Volume 7 Nomor 1 Edisi Februari 2012 Halaman 23-26. Maka diperlukan perbandingan

metode antara algroritma *Vigenere* dan *Affine* untuk mendapatkan suatu perbandingan keamanan data yang berbeda.

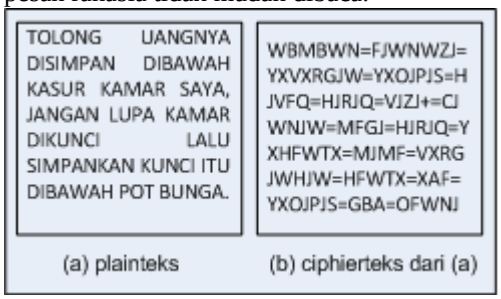
LANDASAN TEORI

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,[5]. 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 [3]:

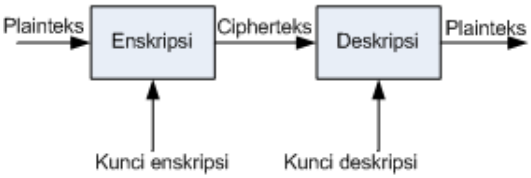
1. Pesan (*message*) adalah data atau informasi yang dapat dibaca atau dimengerti maknanya. Nama lainnya untuk pesan adalah Plaintext (*Plaintext*) atau teks jelas (*clear text*).
2. Pengirim (*sender*) adalah entitas yang melakukan pengiriman pesan kepada entitas lainnya.
3. Kunci (*cipher*) adalah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

Pengubahan *Plaintext* ke *ciphertext* agar suatu pesan rahasia tidak mudah dibaca.



Gambar 1. Proses Enskripsi Teks

Gambar 1. memperlihatkan contoh dua buah *Plaintext* serta *ciphertext* berkoresponden. Yang mana suatu proses pesan yang dikembalikan, *ciphertext* dapat ditransformasikan kembali ke *Plaintext* semula, [3]. Kriptografi 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 *Plaintext* 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 :

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

Metode 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 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

Setiap huruf *Plaintext* akan dienkripsi dengan setiap huruf kunci dibawahnya. Untuk mengerjakan enkripsi dengan *Vigenere Cipher*, dilakukan pada bujursangkar *Vigenere* sebagai garis

vertical dari huruf Plaintext ke bawah dan bujur mendatar dari kiri ke kanan. Atau 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

Misal ekripsi contoh pada tulisan sebagai berikut:

Plaintext: Y A N T O K
Kunci : E K O E K O
Ciphertext : C K B X Y Y

Secara matematis, misalkan kunci dengan panjang m adalah rangkaian $K_1K_2\ldots K_m$, *Plaintext* adalah rangkaian P1P2…Pt dan ciphertext adalah rangkaian C1C2…Ct, maka enkripsi pada *Vigenere Cipher* dapat dinyatakan sebagai:

$$C_1 = (P_1+K_r) \bmod 26 \text{ dan } i = (\bmod m) \qquad (4)$$

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 - 26

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

Metode Affine Cipher

Affine cipher pada metode *affine* adalah perluasan dari metode *Caesar Cipher*, yang mengalihkan Plaintext dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran *P* menghasilkan ciphertext *C* dinyatakan dengan fungsi kongruen [2]:

$$\mathbf{C \equiv m}\, P + b \,\mathbf{(mod}\, n\mathbf{)} \qquad (5)$$

Yang mana *n* adalah ukuran alphabet, *m* adalah bilangan bulat yang harus relatif prima dengan *n* (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan) dan b adalah jumlah pergeseran (*Caesar cipher* adalah khusus dari *affine cipher* dengan *m*=1). Untuk melakukan dekripsi, persamaan (5) herus dipecahkan untuk memperoleh *P*. Solusi kekongruenan tersebut hanya ada jika inver m (mod n), dinyatakan dengan m^{-1}. Jika m^{-1} ada maka dekripsi dilakukan dengan persamaan sebagai berikut:

$$\mathbf{P \equiv m}^{-1}\,(C - b\,)\,\mathbf{(mod}\, n\mathbf{)} \qquad (6)$$

HASIL DAN PEMBAHASAN

Gambaran Umum Sistem

Hasil penelitian yang didapatkan adalah telah diterapkan ilmu kriptografi dengan membandingkan metode *Vigenere* dan *Affine* untuk menghasilkan pesan teks rahasia (*secret message*). Kunci yang digunakan untuk vigenere adalah kunci huruf atau teks biasa (dalam kalimat teks) sedangkan kunci yang digunakan pada *Affine* adalah menggunakan angka kunci yang ada pada bilangan prima.

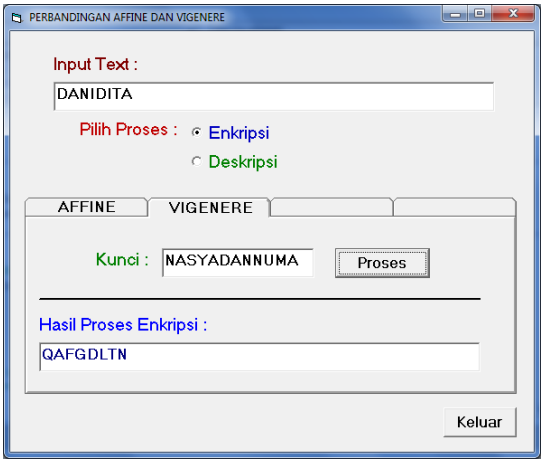
Pengujian Dengan Vigenere

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

Plainttext :
DANI DITA

Kunci:
NASYA DAN NUMA

Adapun pengujian aplikasi untuk enkripsi data teks dapat dilihat pada gambar 6, [2].

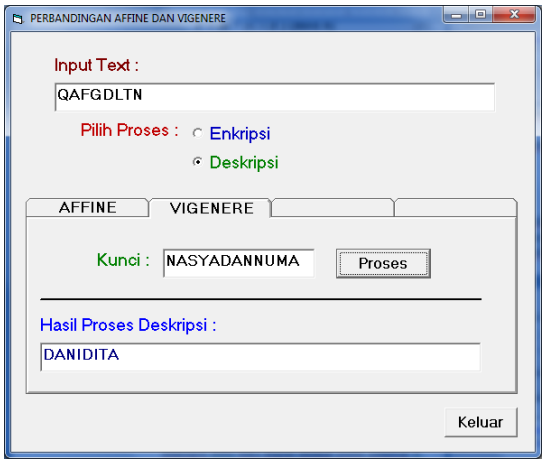


Gambar 3. Pengujian Enkripsi *Vigenere*

Maka dapat menghasilkan *ciphertext* sebagai berikut:

QAFGDLTN

Untuk proses dekripsi, *Plaintext* diinputkan ke dalam kolom isi Input Text, maka mengehasilkan seperti pada gambar 7.



Gambar 4. Proses Deksripsi *Vigenere*

Pengujian Dengan Affine

Pengujian data *Plaintext* digunakan agar teks asli dapat di enskripsi menjadi *Ciphertext*. Contoh data *Plaintext* untuk pengujianpertama dibutuhkan adalah sebagai berikut, [6]:

Tabel 4. Contoh Pesan Inputan Pada *Plaintext*

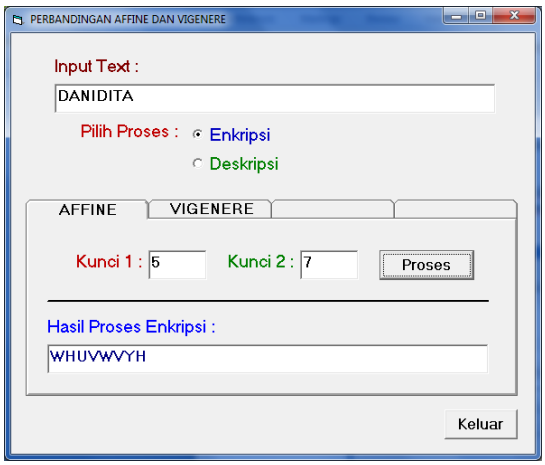
D	A	N	I	D	I	T	A
3	0	13	8	3	8	19	0

Plaintext:
D A N I D I T A

Ekivalen:
3 0 13 8 3 8 19 0

N = 26
K = Relatif Prima
(1,3,**5**,**7**,9,11,15,17,19,21,23,25)

Kunci pertama = 5
Kunci kedua = 7



Gambar 5. Proses Enskripsi *Affine*

Dienkripsi *affine cipher* dengan mengambil m = 5 (karena 5 relatif prima dengan 26) dan b= 7. Karena alphabet yang digunakan 26 huruf, maka n = 26. Enkripsi *Plaintext* dihitung dengan kekongruenan, [6]:

$$C \equiv 5P + 7 \pmod{26} \qquad (6)$$

Perhitungannya adalah sebagai berikut:
P1= 3 → c1 ≡ 5.3 + 7 ≡ 22 (mod 26) ≡ 22 = W
P2= 0 → c2 ≡ 5.0 + 7 ≡ 7 (mod 26) ≡ 7 = H
P3= 13 → c3 ≡ 5.13 + 7 ≡ 72 (mod 26) ≡ 20 = U
P4= 8 → c4 ≡ 5.8 + 7 ≡ 47 (mod 26) ≡ 21 = V
P5= 3 → c5 ≡ 5.3 + 7 ≡ 22 (mod 26) ≡ 22 = W
P6= 8 → c6 ≡ 5.8 + 7 ≡ 47 (mod 26) ≡ 21 = V
P7= 19 → c7 ≡ 5.19 + 7 ≡ 102 (mod 26) ≡ 24 = Y
P8= 0 → c8 ≡ 5.0 + 7 ≡ 7 (mod 26) ≡ 7 = H

Maka menghasilkan *Ciphertext* sebagai berikut : W H U V W V Y H

Pengujian data *ciphertext* digunakan teks yang telah di enskripsi dapat dideskripsikan kembali menjadi *Plaintext*, (liat persamaan 6). Contoh data *ciphertext* yang telah di enskripsi untuk pengujian sebelumnya adalah, sebagai berikut:

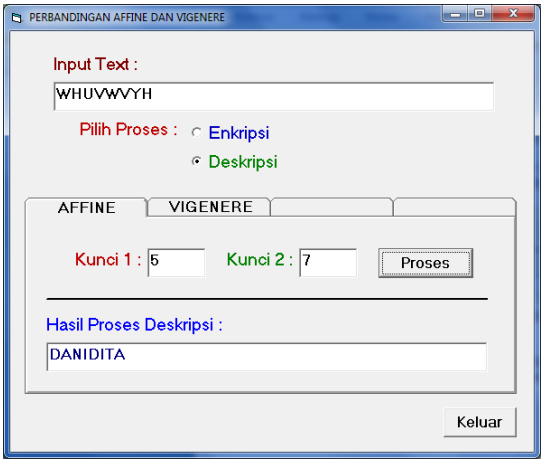
Tabel 5. Pesan Inputan Pada *Ciphertext*

W	H	U	V	W	V	Y	H
22	7	20	21	22	21	24	7

Ciphertext:
W H U V W V Y H

Ekivalen:
22 7 20 21 22 21 24 7

N = 26
K = Relatif Prima (1,3,**5**,**7**,9,11,15,17,19,21,23,25)
Kunci pertama = 5
Kunci kedua = 7



Gambar 6. Proses Dekripsi *Affine*

KESIMPULAN

Berdasarkan hasil perbandingan dalam pengujian, metode *affine* dan *vigenere* sama-sama menghasilkan keluaran data yang tersamarkan setelah diproses enkripsi, perbedaannya pada jenis masukan data kunci, dimana kunci yang digunakan pada *affine* menggunakan huruf alphabet sedangkan *vigenere* menggunakan angka bilangan prima serta memiliki dua data masukan kunci. Keluaran yang dihasilkan memiliki panjang data yang sama dengan data masukan (*plaintext*) baik pada metode *affine* ataupun *vigenere*. Dari sisi keamanan keduanya memiliki keamanan yang cukup baik untuk pesan rahasia, kelebihan *affine* memiliki dua kunci data yang dimasukan, tetapi disisi kelemahan data bilang prima masih dapat ditebak dikarenakan memiliki jumlah yang terbatas, sedangkan *vigenere* dengan satu kunci tetapi kebebasan dalam mengisi data kunci tanpa harus dibatasi panjang kunci dan jenis karakternya, baik huruf maupun angka.

DAFTAR PUSTAKA

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

[2] Hamdani. 2012. Penerapan Metode Vigenere Pada Kriptografi Klasik untuk Pesan Rahasia. Volume 7 Nomor 1 Edisi Februari. Hal. 23-26.

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

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

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

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