Sistem Kriptografi Untuk *Text Message* Menggunakan Metode Affine

ANINDITA SEPTIARINI & HAMDANI

Program Studi Ilmu Komputer, FMIPA Universitas Mulawarman
Jl. Barong Tongkok No. 5 Kampus Unmul Gn. Kelua Sempaja Samarinda 75119

Abstrak
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). 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 *affine* 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 *affine* 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 cipherteks dan dapat dikembalikan ke pesan aslinya atau dideskripsikan.

Kata Kunci: Kriptografi, Teks Rahasia, Affine.

LATAR BELAKANG

Kriptografi merupakan suatu ilmu seni dengan filosofinya *the art of war*, dimana waktu itu pernah digunakan untuk mengirim pesan rahasia pada jaman romawi pada era raja 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/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. 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 *affine*. *Affine* 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 (*cleartext*). Maka diperlukan membuat aplikasi pesan rahasia berupa teks menggunakan metode *Affine* yang merupakan perluasan dari *caesar* yang mengalihkan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran.

LANDASAN TEORI

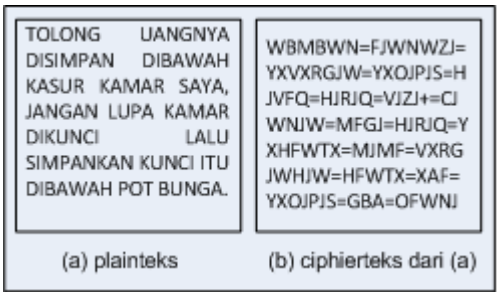
Kriptonologi

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 (Stalling, 1998). 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 (Munir, 2006):

a. Pesan (*message*) adalah data atau informasi yang dapat dibaca atau dimengerti maknanya. Nama lainnya untuk pesan adalah plainteks (*plaintext*) atau teks jelas (*clear text*).

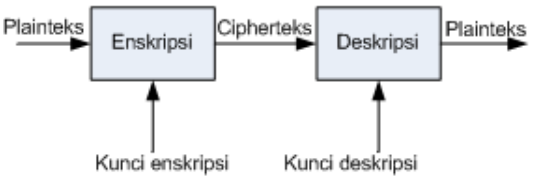
b. Pengirim (*sender*) adalah entitas yang melakukan pengiriman pesan kepada entitas lainnya.
c. Kunci (*cipher*) adalah aturan atau fungsi matematika yang digunakan untuk melakukan proses enkripsi dan dekripsi pada plaintext dan *ciphertext*.
d. Enkripsi adalah mekanisme yang dilakukan untuk merubah plaintext menjadi *ciphertext*.
e. Dekripsi adalah mekanisme yang dilakukan untuk merubah *ciphertext* menjadi *plaintext*.
f. 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, (Munir, 2006). 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 :

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

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

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

Sehingga dari dua hubungan diatas berlaku :

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

Affine Cipher

Affine cipher pada metode *affine* adalah perluasan dari metode *Caesar Cipher*, yang mengalihkan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran *P* menghasilkan cipherteks *C* dinyatakan dengan fungsi kongruen:

$$\mathbf{C \equiv m\,P + b \pmod{n}} \quad (4)$$

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 deskripsi, persamaan (4) 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:

$$\mathbf{P \equiv m^{-1}\,(C - b)\,(mod\ n)} \quad (5)$$

HASIL DAN PEMBAHASAN

Gambaran Umum Sistem

Hasil penelitian yang didapatkan adalah dapat diterapkan ilmu kriptografi dengan metode *Affine* untuk menghasilkan pesan teks rahasia. Teks asli dapat di ubah menjadi teks yang disamarkan dengan suatu metode *Affine*, dan teks yang telah di enksripsi dapat dikembalikan kembali menjadi teks asli (plainteks).

Tabel 1. Penginisialan Alfabet Huruf A-Z menjadi Angka 0 - 26

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

Pengujian Plainteks

Pengujian data plainteks digunakan agar teks asli dapat di enskripsi menjadi cipherteks. Contoh data plainteks untuk pengujian pertama dibutuhkan adalah sebagai berikut:

Tabel 2. Teks Inputan Plainteks

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

Plainteks:
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 3. Proses Enskripsi

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 plainteks dihitung dengan kekongruenan:

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

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 Cipherteks sebagai berikut : W H U V W V Y H

Pengujian Cipherteks

Pengujian data cipherteks digunakan teks yang telah di enskripsi dapat dideskripsikan kembali menjadi plainteks. Contoh data cipherteks yang telah di enskripsi untuk pengujian sebelumnya adalah, sebagai berikut:

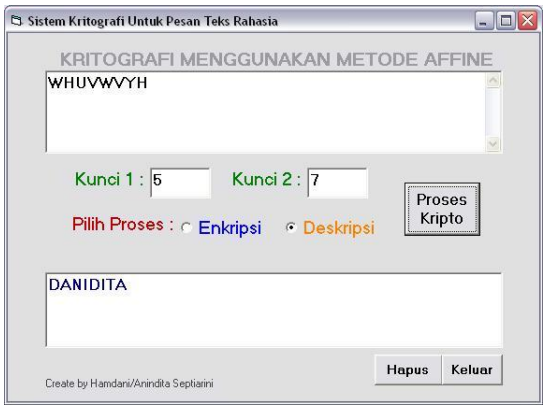
Tabel 2. Teks Inputan Plainteks

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

Cipherteks:
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 4. Proses Deskripsi

Untuk mengembalikan teks yang telah dienskripsi menjadi pesan rahasia dapat dilakukan pendekripsian, pertama-tama dapat dihitung 5^{-1} (mod 26), yang dapat dihitung dengan memecahkan kekongruenan lanjar.

$$5x \equiv 1 \pmod{26} \qquad (7)$$

Untuk deskripsi dengan hasil 1 maka solusinya adalah x =21 (mod 26) dikarenakan 5.21 = 105 mod 26 menghasilkan = 1.

$$P \equiv 21 (C - 7) \pmod{26} \qquad (8)$$

P1=22→c1 ≡ 21.(22 - 7) ≡ 315(mod 26) ≡ 3 = D
P2= 7 → c2 ≡ 21.(7 - 7) ≡ 0 (mod 26) ≡ 0 = A
P3=20→ c3 ≡ 21.(20 - 7) ≡ 273(mod 26)≡ 13 = N
P4=21→ c4 ≡ 21.(21 - 7) ≡ 294(mod 26) ≡ 8 = I
P5=22→ c5 ≡ 21.(22 - 7) ≡ 315(mod 26)≡ 3 = D
P6=21→ c6 ≡ 21.(21 - 7) ≡ 294 (mod 26) ≡ 8 = I
P7=24→ c7 ≡ 21.(24 - 7) ≡357(mod 26) ≡ 19 = T
P8=7→ c8 ≡ 21.(7 - 7) ≡ 0 (mod 26) ≡ 0 = A

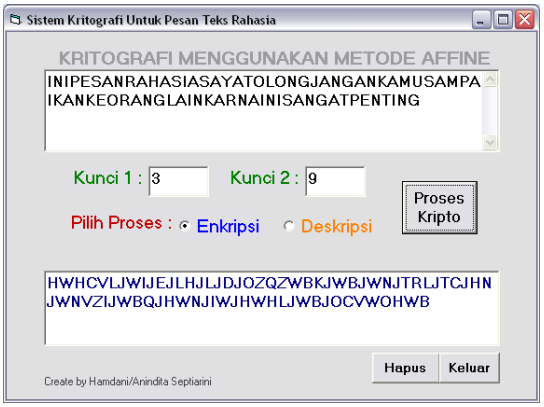
Maka menghasilkan Plainteks sebagai berikut :
D A N I D I T A

Proses pengujian enkripsi lainnya dengan plainteks untuk pesan rahasia dengan kunci pertama 3, dan kunci kedua 9.

INIPESANRAHASIASAYATOLONGJANGANKAMUSAMPAIKANKEORANGLAINKARNAINISANGATPENTING

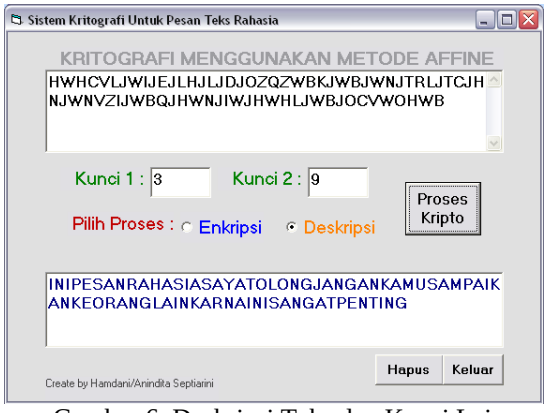
Maka menghasilkan ciphertesk seperti teks pesan yang diterima sebagai berikut:

HWHCVLJWIJEJLHJLJDJOZQZWBKJWBJWNJTRLJTCJHNJWNVZIJWBQJHWNJIWJHWHLJWBJOCVWOHWB



Gambar 5. Enkripsi Teks dan Kunci Lain

Untuk proses deskripsi, maka dapat dilihat jendela aplikasi pada gambar 6.



Gambar 6. Deskripsi Teks dan Kunci Lain

KESIMPULAN

Pesan teks rahasia ini dapat digunakan untuk mengirim pesan atau sesuatu yang sifatnya tidak dapat diketahui orang lain seperti mengirim pesan rahasia atau dokumen rahasia. Dimana teks asli (*plaintext*) di ekripsi menjadi teks yang samar (*ciphertext*) yang dapat membantu dalam pertukaran pesan berupa teks. Jumlah teks pada plainteks yang di isi tidak dibatasi.

DAFTAR PUSTAKA

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

Munir, R., 2006, *Kriptografi*, Informatika, Bandung.

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

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