Implementasi Kombinasi Caesar dan *Affine Cipher* untuk Keamanan Data Teks

Dian Rachmawati[1], Ade Candra[2]
[1,2]Program Studi S1 Ilmu Komputer Fasilkom – TI Universitas Sumatera Utara
e-mail: dee230783@gmail.com, dian.rachmawati@usu.ac.id , ade_candra@usu.ac.id

***Abstrak*— Petukaran data yang terjadi secara *offline* maupun online sangat rentan dengan ancaman pencurian data. Kombinasi Caesar dan Affine Cipher diharapkan mampu untuk menangani isu keamanan data. Caesar Cipher bekerja dengan memanfaatkan pergeseran atau dikenal dengan shift cipher sementara Affine Cipher bekerja dengan menggunakan kunci dua buah bilangan integer. Kombinasi dua buah algoritma ini mampu mengamankan data dan mengembalikan kembali ke bentuk aslinya (plainteks), sehingga tidak menyebabkan integritas datanya hilang.**

***Kata Kunci*—plainteks, cipherteks, Caesar cipher, Affine cipher.**

I. PENDAHULUAN

Perkembangan jaringan komputer di masa kini memungkinan kita untuk melakukan komunikasi atau pengiriman pesan melalui jaringan komputer.Salah satu bentuk komunikasi adalah dengan menggunakan tulisan. Ada banyak informasi yang dapat disampaikan melalui tulisan (teks) dan terkadang dalam teks tersebut terdapat informasi yang bersifat rahasia.

Untuk menjaga keamanan pesan yang bersifat rahasia, terdapat beberapa cara dan teknik tertentu yang dapat digunakan. Salah satunya dengan kriptografi yang berfungsi untuk menyamarkan pesan menjadi bentuk pesan tersandi.

Cæsar Cipher merupakan salah satu algoritma cipher tertua dan merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Kelemahan *Caesar Cipher* adalah kita bias memperoleh pesan asli dengan memanfaatkan metode Brute Force dan presentasi frekuensi huruf yang paling sering muncul dalam suatu kalimat.

Oleh karena itu penulis tertarik untuk mengkombinasikan *Caesar Cipher* dengan *Affine Cipher* untuk meningkatkan keamanan dari pesan. *Affine Cipher* adalah perluasan dari metode *Caesar Cipher* yang mengalikan pesan asli (plainteks) dengan sebuah nilai *intege*r dan menambahkannya dengan sebuah pergeseran (dalam *integer*) dinyatakan dengan fungsi kongruen.

II. URAIAN PENELITIAN

A. Kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem Kriptografi (*Cryptosystem*) adalah kumpulan dari fungsi enkripsi dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi. [7]
Menurut Katz, kriptografi adalah studi ilmiah atau teknik untuk mengamankan informasi digital, transaksi, dan komputasi yang terdistribusi. [10]
Kriptografi bertujuan untuk memberikan layanan keamanan [3] sebagai berikut:

1. Kerahasiaan (*Confidentiality*)
   Informasi dirahasiakan dari semua pihak yang tidak berwenang.
2. Keutuhan Data (*Integrity*)
   Pesan tidak berubah dalam proses pengiriman hingga pesan diterima oleh penerima.
3. Autentikasi (*Message Authentication*)
   Kepastian terhadap identitas setiap entitas yang terlibat dan keaslian sumber data.
4. Nirpenyangkalan (*Nonrepudiation*)
   Setiap entitas yang berkomunikasi tidak dapat menolak atau menyangkal atas data yang telah dikirim atau diterima.

Kriptografi memiliki beberapa istilah atau terminologi yang penting untuk diketahui antara lain:

1. Pengirim dan Penerima
   Pengirim (*sender*) adalah entitas yang mengirimkan pesan kepada penerima (*reciever*) dengan aman tanpa ada gangguan dari penyadap (*eavesdropper*). Penerima adalah entitas yang menerima pesan dari pengirim [4].
2. *Plaintext* dan *Ciphertext*
   Pesan murni pada kriptografi disebut dengan *plaintext*, sedangkan pesan murni yang telah disamarkan disebut *ciphertext* [7].
3. Enkripsi dan Dekripsi
   Dalam prosesnya, perubahan dari *plaintext* menjadi ciphertext dinamakan enkripsi (*encryption*) dan perubahan kembali dari ciphertext menjadi *plaintext* adalah dekripsi (*decryption*) [7].
4. Kriptografer, Kriptanalis, dan Kriptologis
   Seseorang yang mempelajari dan menggunakan metode kriptografi untuk mengamankan pesan dinamakan kriptografer. Sebaliknya, metode yang menggunakan teknik komputasi matematika untuk menyerang metode kriptografi dinamakan kriptanalis, dan orang yang mempelajari kriptanalisis dinamakan kriptanalis. Kata

kriptologi merupakan cabang ilmu yang mempelajari kriptografi sekaligus dengan kriptanalisis. Orang yang mempelajari kriptologi tersebut dinamakan kriptologis [5].

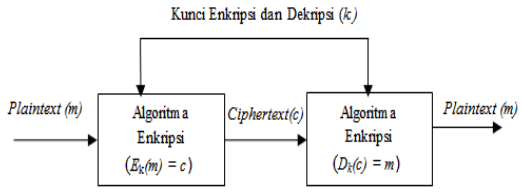
5. Cipher
   Algoritma kriptografi atau cipher adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Dalam menyelesaikan persoalaan *cipher*, dibutuhkan sebuah entitas yang disebut dengan kunci (dilambangkan K). Kunci mempunyai nilai bilangan yang sangat besar. Besar kecilnya nilai ini dinamakan *keyspace*. Beberapa algoritma kriptografi menggunakan *cipher* dengan kunci yang berbeda antara kunci untuk enkripsi dan dekripsi.

6. Penyadap (*Eavesdropper*)
   Penyadap (*eavesdropper*) adalah orang yang ingin mendapatkan informasi sebanyak-banyaknya dari pesan yang telah dikirim dan memecahkan *ciphertext* dari sistem kriptografi. Penyadap mempunyai akses komunikasi antara pengirim dan penerima [4].

Secara umum, sistem kriptografi digolongkan menjadi dua bagian, antara lain:

a. Sistem Kriptografi Simetrik (*Symmetric Cryptosystem*)

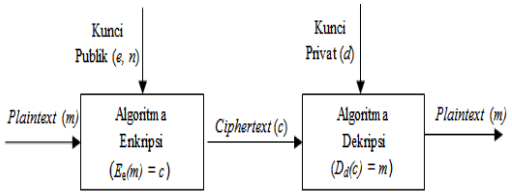
Sistem kriptografi simetrik adalah sistem kriptografi dengan metode dekripsi pesan merupakan kebalikan (*reverse*) dari metode enkripsinya. Seperti contoh, sebuah pesan dengan metode enkripsinya adalah mengganti huruf dari pesan (*plaintext*) tersebut menjadi huruf baru (*ciphertext*) yang mana merupakan lima langkah setelah huruf kata tersebut (a digantikan dengan f, b digantikan dengan g, c digantikan dengan h, dan seterusnya), maka metode dekripsinya adalah mengembalikan huruf-huruf *ciphertext* tersebut sebanyak lima langkah sebelumnya. Pada umumnya, pengirim dan penerima pada sistem kriptografi simetrik mempunyai kunci yang identik [5]. Contoh : *Caesar Cipher*, *Affine Cipher*, *Vigenere Cipher* dll.



Gambar 1 Proses Enkripsi dan Dekripsi Symmetric Cryptosystem [4]

b. Sistem Kriptografi Asimetrik (*Asymmetric Cryptosystem*)

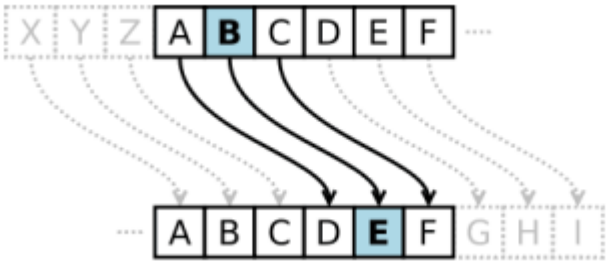
Asymmetric Cryptosystem atau yang disebut dengan *Public Key Cryptograhy* adalah sistem kriptografi yang mana mempunyai dua kunci yang berbeda dan unik satu dengan lainnya. Satu dari dua kunci tersebut dipublikasikan umum untuk mengenkripsikan pesan disebut dengan kunci publik (*public key*) dan satu kunci lainnya dirahasiakan untuk mendekripsikan pesan disebut kunci privat (*private key*). Contoh dari sistem ini antar lain Rivest-Shamir-Adleman (RSA), Diffie-Helman, dan Elgamal [6]. Proses Enkripsi dan Dekripsi diperlihatkan pada gambar 2.



Gambar 2 Proses Enkripsi dan Dekripsi Asymmetric Cryptosystem [4]

B. Caesar Cipher

Substitusi cipher yang pertama dalam dunia persandian pada waktu waktu pemerintahan Julius Caesar dikenal dengan *Caesar Cipher*, yakni mengganti posisi huruf awal dari alphabet [1] *Caesar Cipher* juga dikenal dengan nama *Shift Cipher*.



Gambar 3 Pegeseran pada Caesar Cipher

Dari gambar 3 menunjukkan terjadi pergeseran 3 yaitu B berubah menjadi E, C menjadi F dan A menjadi C dan seterusnya.*Caesar Cipher* dapat dipecahkan dengan cara *Brute Force*, yaitu suatu bentuk serangan yang mencoba kemungkinan – kemungkinan untuk menemukan kunci.

C. Affine Cipher

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

$$C=((a \times P) + k) \bmod 26 \ldots\ldots\ldots(1)$$

Dimana 26 adalah jumlah alphabet, persamaan 1 digunakan pada proses enkripsi. Proses dekripsi menggunakan persamaan 2 di bawah ini :

$$P=a^{-1}(Ci-k) \bmod 26 \ldots\ldots\ldots\ldots(2)$$

a adalah bilangan bulat yang harus relatif prima dengan 26. Dengan kata lain great common divisior gcd(a,26) harus sama dengan 1.

D. Kombinasi Caesar Cipher dan Affine Cipher

Kombinasi *Caesar Cipher* dan *Affine Cipher* digunakan bertujuan untuk mengatasi kelemahan dari Caesar Cipher. . Karena *Caesar Cipher* bekerja hanya dengan melakukan pergeseran karakter, sehingga dapat dipecahkan dengan menggunakan *Brute Force*. Metode *Brute Force* yang paling

sering digunakan adalah dengan menggunakan statistika frekuensi kemunculan huruf yang paling sering. Contoh : kita mendapat pesan YGEG. Karena di bahasa Indonesia kita tahu huruf yang paling sering muncul adalah A. Maka G yang memiliki frekuensi kemunculan 2 kali kita ganti dengan A. Jika G mengacu ke A maka kunci pergeserannya dari A ke G adalah 6. Lalu kita geser mundur pesan sisanya yaitu Y dan E sebanyak 6, sehingga diperoleh pesan SAYA.
Kombinasi *Caesar* dan *Affine Cipher* bekerja dengan cara mengenkripsi pesan terlebih dahulu dengan *Caesar* selanjutnya hasil dari *Caesar Cipher* dienkripsi lagi dengan *Affine Cipher*, sehingga pola kemunculan statistika dari pesan tidak dapat dideteksi

E. Inversi modulo

Jika a dan m relatif prima dan m > 1, maka inversi dari a mod m dapat ditemukan. Inversi dari a (mod m), disebut juga inversi perkalian, di mana bilangan bulat a-1 sedemikian sehingga
$aa^{-1} \equiv 1 \pmod{m}$…….(3) [2]

F. Great Common Divisior(Faktor Persekutuan Terbesar)

Faktor persekutuan terbesar adalah elemen terbesar pada himpunan divisor dua bilangan integer. Dua bilangan dapat saja memiliki beberapa elemen divisor yang sama namun hanya satu yang terbesar [9]. Misalnya, divisor 15 = { 1, 3, 5, 15 } dan divisor 45 = { 1, 3, 5, 9, 15, 45 }, maka himpunan divisor kedua bilangan tersebut ialah { 1, 3, 5, 15 } dan yang terbesar ialah 15. Dengan kata lain, faktor persekutuan terbesar 15 dan 45 dapat dinotasikan sebagai GCD(15, 45) = 15 [8].

III. HASIL DAN PEMBAHASAN

A. Perhitungan Kombinasi Metode Caesar Cipher dan Affine Cipher

Dari teori di atas untuk mengenkripsi suatu pesan teks dengan menggunakan kombinasi Caesar Cipher dan Affine Cipher maka membutuhkan 3 buah bilangan integer misalkan (x,a dan k). 1 buah bilangan digunakan untuk penentuan pergeseran (x) pada Caesar Cipher dan dua buah bilangan digunakan pada *Affine Cipher* (a dan k).

Contoh : Terdapat pesan plainteks ILMUKOMPUTER dengan kunci x = 9, a = 7 dan k = 10 maka langkah yang harus dikerjakan adalah :
1. Geser ILMUKOMPUTER ke kanan sebanyak 9 karakter sehingga menghasilkan RUVDTXVYDCNA (Caesar Cipher).
2. Lalu dengan memetakan alphabet A = 0 hingga Z =25 diperoleh nilai R = 17. Sehingga R berubah menjadi (7 x 17)+ 10 mod 26 = 25 (huruf Z). Langkah ini dilakukan terus menerus hingga karakter terakhir dalam string. Hasil akhirnya diperoleh *Ciphertek*s ZUBFNPBWFYXK
Langkah 1 dan 2 ini disebut proses enkripsi pada Kriptografi yaitu penyandian pesan.

Adapun cara pengembalian pesan (dekripsi) adalah sebagai berikut :
Lakukan pengembalian pesan ZUBFNPBWFYXK.
1. Petakan alphabet A = 0 hingga Z=25. Sehingga nilai Z= 25 dengan menggunakan rumus dekripsi Affine Cipher menjadi 7^{-1} x (25-10) mod 26. 7^{-1} dengan menggunakan invers modulo 26 menjadi 15. Sehingga perhitungan berubah menjadi 15 x (25-10) mod 26 = 17. Indeks 17 adalah huruf R. Langkah ini dilakukan terus menerus hingga karakter terakhir dalam string. Hasil akhirnya diperoleh RUVDTXVYDCNA.
2. Dengan menggeser 9 karakter ke kiri maka string RUVDTXVYDCNA berubah menjadi ILMUKOMPUTER (*Caesar Cipher*).

B. Pseudocode Caesar Cipher dan Affine Cipher

Adapun *pseudocode* yang digunakan untuk melakukan enkripsi dan dekripsi pada *Caesar Cipher* adalah sebagai berikut :

Enkripsi Caesar Cipher
```
for i:=1 to length(s) do
begin
c:= ord(upcase(s[i]))+indice;
if c>90 then c:=c-26;
s[i]:=chr(c);
end;
```

Dekripsi Caesar Cipher
```
for i:=1 to length(s) do
begin
c:= ord(upcase(s[i]))-indice;
if c<65 then c:=c+26;
s[i]:=chr(c);
end;
```

Pseudocode yang digunakan untuk enkripsi dan dekripsi dengan kombinasi *Caesar Cipher* dan *Affine Cipher* adalah sebagai berikut :

Enkripsi Kombinasi Caesar Cipher dan Affine Cipher
```
for i:=1 to length(pt) do
begin
c:= ord(upcase(pt[i]))+x;
if c>90 then c:=c-26;
pt[i]:=chr(c);
end;
   ct:=enkripsi_affin(a,k,pt);
   writeln('Cipher Text : '+ct);
```

Function enkripsi_affin adalah sebagai berikut :

```
for i:=1 to length(s) do
begin
pi:=ord(upcase(s[i]))-65;
hitung:=(a*pi+k) mod 26;
temp[i]:=chr(hitung+65);
```

```
end;
```

Dekripsi Kombinasi Caesar Cipher dan Affine Cipher

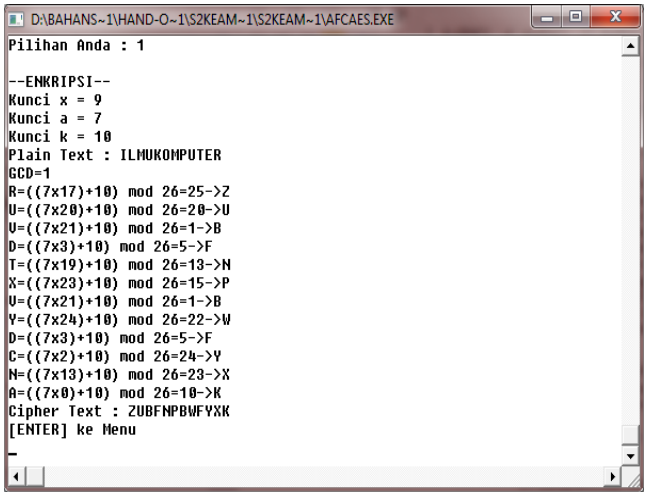
```
pt:=dekripsi_affin(a,k,ct);
for i:=1 to length(pt) do
begin
c:= ord(upcase(pt[i]))-x;
if c<65 then c:=c+26;
pt[i]:=chr(c);
end;
   writeln('Plain Text : '+pt);
```

Function dekripsi_affin adalah sebagai berikut :

```
for i:=1 to length(s) do
begin
pi:=ord(upcase(s[i]))-65;
hitung:=ainv*(pi-k) mod 26;
temp[i]:=chr(hitung+65);
end;
```

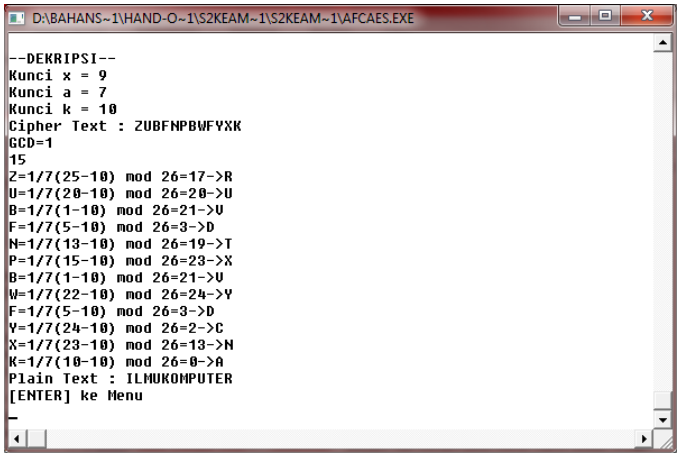
C. Tampilan Program

Dari *pseudocode* tersebut dapat dilihat tampilan enkripsi pada gambar 4 :



Gambar 4 Interface proses enkripsi

Dari *pseudocode* tersebut dapat dilihat tampilan dekripsi pada gambar 5 :



Gambar 5 Interface proses dekripsi

IV. KESIMPULAN/RINGKASAN

Kombinasi *Caesar Cipher* dan *Affine Cipher* dapat membantu meningkatkan keamanan data, jika dibandingkan hanya dengan menggunakan satu buat metode saja. Penggunaan angka 26 mengakibatkan karakter yang dapat diproses hanya A hingga Z dan berlaku *noncase sensitive*. Pengkombinasian kedua metode tersebut mampu mengembalikan pesan ke dalam bentuk semula sehingga isi pesan asli tidak mengalami perubahan. Jika nilai a tidak relative prima dengan 26 maka metode *Affine Cipher* tidak dapat digunakan.

DAFTAR PUSTAKA

[1] Ariyus, D. 2008. *Pengantar Ilmu Kriptografi: Teori, analisis dan implementasi*. ANDI: Yogyakarta.

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

[3] Paar, C. & Pelzl, J. 2010. *Understanding Cryptography*. Springer-Verlag: Berlin.

[4] Schneier, B. 1996. *Applied Cryptography: Protocols, algorithms and source code in C*. 2nd Edition. John Wiley & Sons, Inc.: New Jersey.

[5] Batten, L. M. 2013. *Public Key Cryptography: Application and Attacks*. IEEE Press: Australia.

[6] Smart, N. 2004. *Cryptography: An introduction*. 3rd Edition. University of Bristol.

[7] Mollin, R. A. 2007. *An Introduction to Cryptography*. 2nd Edition. Chapman & Hall/CRC: Boca Raton, Florida.

[8] Fauzana, 2013. *Analisis dan perancangan sistem autentikasi pengguna pada web menggunakan metode multiple-key RSA*. Skripsi. Universitas Sumatera Utara.

[9] Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. ANDI: Yogyakarta.

[10] Katz, J. & Lindell, Y. 2007. Introduction to Modern Cryptography. Chapman & Hall/CRC: United States.