Jurnal Mekanova
Vol 2. No. 1, April 2016
ISSN : 2502-0498

Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data

Muhammad Nurtanzis Sutoyo[1], Murhaban[2]
[1]Program Studi Sistem Informasi - FTI Universitas Sembilanbelas November Kolaka
[2]Program Studi Teknik Mesin – Fakultas Teknik Universitas Teuku Umar
e-mail: [2]mr.iyes@yahoo.co.id, [2]murhabani@gmail.com

Abstrak

Cara kerja CBR adalah dengan membandingkan kasus baru dengan kasus lama, jika kasus baru tersebut mempunyai kemiripan dengan kasus lama, maka CBR akan memberikan jawaban kasus lama untuk kasus baru. Penelitian ini mencoba untuk membangun suatu sistem Penalaran Berbasis Kasus untuk menentukan beasiswa. untuk menghitung kemiripan terlebih dahulu dilakukan proses indexing terhadap kasus lama. Hal ini dilakukan agar pada proses pencarian nilai similarity kasus baru terhadap basis kasus dapat lebih efisien karena cukup menghitung nilai similarity kasus baru terhadap data kasus yang memiliki indeks yang sama. Hasil uji coba sistem menunjukan bahwa sistem penalaran berbasis kasus ini membantu dalam menentukan usulan beasiswa.

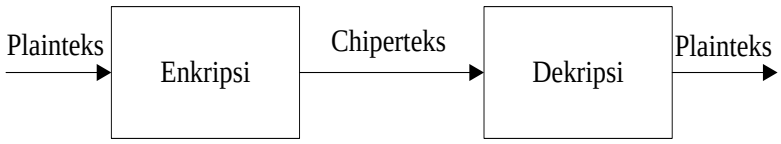
Kata kunci*—Kriptografi, Caesar Chiper, Vigenere Chiper*

1. PENDAHULUAN

Keamanan dan kerahasiaan data atau informasi merupakan salah satu aspek yang penting dari suatu data atau informasi. Dengan perkembangan teknologi saat ini, setiap orang akan mudah memperoleh data atau informasi. Apabila data atau informasi tersebut tidak dilindungi, maka secara mudah orang lain akan mengetahui data atau informasi yang dimiliki. Berbagai cara pun dilakukan untuk melindungi data atau informasi tersebut.

Ilmu yang mempelajari tentang proses pengamanan data atau informasi adalah kriptografi. Kriptografi (*cryptographi*) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia). Sedangkan "*graphein*" artinya "*writing*" (tulisan).Dimana pemanfaatan kriptografi oleh manusia sejak empat abad lalu. Secara umum ada dua jenis kriptografi, yaitu: kriptografi klasik dan kriptografi modern. Kriptografi klasik telah digunakan digunakan sebelum era komputer. Pada penelitian ini menggunakan kriptografi klasik. Kriptografi klasik umumnya merupakan teknik penyandian dengan kunci tertentu dan menyembunyikan pesan yang memiliki arti ke sebuah pesan yang tidak memiliki arti[1].

Dalam kriptografi terdapat dua konsep utama, yaitu: enkripsi dan dekripsi. Proses kriptografi secara umum disajikan seperti Gambar 1.



Gambar 1. Proses Enkripsi Deksripsi

Enkripsi adalah proses dimana data atau informasi diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. *Plainteks* adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.*Dekripsi* adalah proses mengubah kembali bentuk yang tersamar tersebut menjadi informasi awal.

Banyak algoritma yang digunakan untuk melakukan pengamanan data, diantaranya: Caesar Chiper, Vigenere Chiper, Hill Chiper, dan Affine Chiper. Sedangkan algoritma kriptografi yang digunakan dengan mengkombinasikan algoritma *Caesar Chiper* dengan *Vigenere Chiper*.

Caesar Chiper merupakan sistem persandian klasik berbasis substitusi sederhana. Sistem persandian Caesar Chiper menggunakan operasi *shift.* Operasi *shift* adalah operasi persansian dengan mensubstitusikan suatu huruf menjadi huruf pada daftar alfabet *k*. Sedangkan Vigenere Chiper merupakan sistem sandi poli-alfabetik yang sederhana. Sistem persandian Vigenere Chiper menggunakan operasi *shift*, sama seperti sistem persandian Caesar Chiper.

Telah banyak penelitian mengenai kriptografi klasik. Sasongko [2] menggunakan kriptografi klasik untuk pengamanan data. Fitriasih, dkk [3] dalam penelitiannya melakukan studi model kriptografi klasik. Dimana hasil dari penelitian tersebut, algoritma kriptografi klasik dapat dipecahkan dengan cara *brute force attack* dan lain sebagainya. Doni dan Walad [4] membandingkan antara algoritma klasik Caesar Chiper dengan Vigenere Chiper. Hasil penelitian menyebutkan bahwa kedua algoritma dapat dikembangkan, demi keamanan komputer. Agar algoritma kriptografi klasik tidak mudah dipecahkan, maka dalam penelitian ini mengkombinasikan algoritma *Caesar Chiper* dengan *Vigenere Chiper*.

2. LANDASAN TEORI

2.1 Kriptografi

Kriptografi merupakan salah satu ilmu seni dengan filosofinya *the art of war*. Dimana pada saat itu digunakan untuk mengirim pesan rahasia pada zaman Romawi pada era raja Julius Caesar. Kriptografi adalah suatu metode untuk melindungi suatu data atau informasi dengan menggunakan sandi, dimanasandi tersebut hanya bisa dimengerti oleh orang yang berhak menerima data atau informasi tersebut.Sedangkan tujuan kriptografi adalah melindungi data dari ancaman yang disengaja atau tidak disengaja. Dewasa ini ancaman bertambah karena semakin meluasnya akses melalui internet atau teknologi bergerak.Aspek-aspek keamanan data dalam kriptografi adalah sebagai berikut.

a. *Confidentiality*
Merupakan usaha untuk menjaga kerahasiaan data. Serangan dalam aspek ini antara lain dilakukan dengan penyadapan, misalnya sniffer atau logger.

b. *Integrity*
Memastikan bahwa informasi yang dikirim tidak mengalami modifikasi oleh pihak yang tidak berhak. Serangan dapat berupa pengubahan data oleh orang yang tidak berhak.

c. *Availability*
Informasi harus tersedia ketika dibutuhkan. Serangan dapat berupa menghilangkan atau menghapus data.

d. *Authentication*
Meyakinkan keaslian data, sumber data, orang yang mengakses data, dan server yang digunakan.

e. Access Control

Aspek ini berhubungan dengan mekanisme pengaturan akses ke informasi, untuk mengatur siapa yang boleh melakukan apa.

Dalam kriptografi sering ditemukan istilah-istilah penting untuk diketahui, diantaranya [5].

a. Pesan (*message)*, adalah data atau informasi yang dapat dibaca atau dimengerti maknanya.
b. Pengirim *(sender)*, adalah entitas yang melakukan pengiriman pesan kepada entitas lain.
c. Kunci *(chiper)*, adalah aturan atau fungsi yang digunakan untuk melakukan proses enkripsi dan dekripsi pada plainteks dan chiperteks.
d. Enkripsiadalah mekanisme yang dilakukan untuk merubah plainteks menjadi chiperteks.
e. Dekripsi adalah mekanisme yang dilakukan untuk merubah chiperteks menjadi plainteks.
f. Penerima *(recipient)*, adalah entitas yang penerima yang berhak menerima pesan dari pengirim.

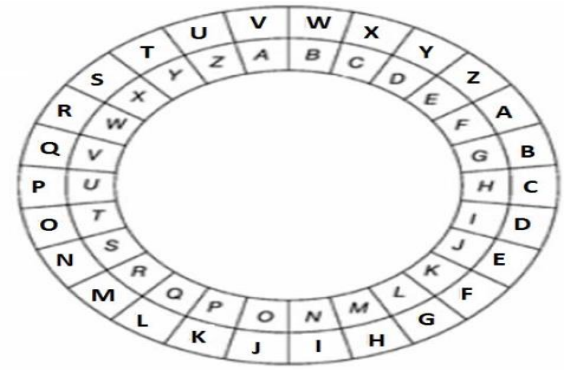
Algoritma kriptografi(*cipher)* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi [6]. Ada dua macam algoritma kriptografi, yaitu *algoritma simetris* (*symmetric algorithms*) dan *algoritma asimetris* (*asymmetric algorithms*).

Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Algoritma ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Keamanan algoritma simetris tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkripsi dan mendekripsi pesan. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan.Contoh dari algoritma kriptografi simetris adalah Cipher Permutasi, Cipher Substitusi, Cipher Hill, OTP, RC6, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi, DES dan IDEA[7].

Algoritma asimetris, sering juga disebut dengan *algoritma kunci publik*, menggunakan dua jenis kunci, yaitu *kunci publik* (*public key*) dan *kunci rahasia* (*secret key*). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Contoh dari algoritma asimetris adalah RSA, ElGamal, McEliece, LUC dan DSA (*Digital Signature Algorithm*).

2.2 Caesar Chiper

Caesar Cipher menggunakan roda yangberputar dalam enkripsi dan dekripsinya. Rodayang digunakan memiliki dua lingkaran, lingkaranroda yang paling luar dapat diputar bebas. Lingkaran roda disajikan seperti Gambar 1.



Gambar 2. Lingkaran Roda Caesar Chiper

Proses Enkripsi (E) pada algoritma *Caesar Chiper* dalam fungsi

$$E(x) = (P_i + K) \bmod 26 \quad (1)$$

Sedangkan proses Dekripsi (D) pada algoritma *Caesar Chiper* dalam fungsi

$$D(x) = (C_i - K) \bmod 26 \quad (2)$$

Dimana *Pi* = plainteks ke-*i*, *K* = kunci, *Ci* = chiperteks ke-*i*

Sebagai contoh diberikan plainteks “KUCING”, dengan kunci = 21, maka diperoleh chiperteks “FPXDIB”. Dimana proses enkripsi dengan menggunakan persamaan 1.

Plainteks : KUCING
Kunci : 21
K = (10 + 21) mod 26
= 5 → F
U = (20 + 21) mod 26
= 15 → P
C = (2 + 21) mod 26
= 23 → X
I = (8 + 21) mod 26
= 3 → D
N = (13 + 21) mod 26
= 8 → I
G = (6 + 21) mod 26
= 1 → B

Sedangkan proses dekripsi dengan menggunakan persamaan 2
Chiperteks : FPXDIB
Kunci : 21
F = (5 - 21) mod 26
= 5 → K
P = (15 - 21) mod 26
= 20 → U
X = (23 - 21) mod 26
= 2 → C
D = (3 - 21) mod 26
= 8 → I
I = (8 - 21) mod 26
= 13 → N
B = (1 - 21) mod 26
= 6 → G

2. 3Vigenere Chiper

Vigenere Cipher merupakan metodeenkripsi dengan menggunakan deret *Caesar Cipher*dengan huruf-huruf sebagai kuncinya. Kelebihanmodel ini tidak begitu rentan dengan metodepemecahan dibandingkan dengan *Caesar Cipher*.*Vigenere Cipher* menggunakan bujur sangkarVigenere dalam proses enkripsi dan dekripsinya[3]. Di dalam

Vigenere Chiper, kunci yang digunakan berupa suatu kata kunci. Proses Enkripsi (E) pada algoritma *Vigenere Chiper* dalam fungsi

$$E(x) = (P_i + K_i) \bmod 26 \quad (3)$$

Sedangkan proses Dekripsi (D) pada algoritma *Vigenere Chiper* dalam fungsi

$$D(x) = (C_i - K_i) \bmod 26 \quad (4)$$

Dimana *Pi* = plainteks ke-*i, Ki* = kata kunci ke-*i, Ci* = chiperteks ke-*i*

Sebagai contoh diberikan plainteks "BELAJAR", dengan kata kunci "SAMA DIA" maka diperoleh chiperteks "TEXAMIR". Dimana proses enkripsi dengan menggunakan persamaan 3.

Plainteks : BELAJAR
Kunci : SAMADIA

B; S = (1 + 18) mod 26
= 19 → T
E; A = (4 + 0) mod 26
= 4 → E
L; M = (11 + 12) mod 26
= 23 → X
A; A = (0 + 0) mod 26
= 0 → A
J; D = (9 + 3) mod 26
= 12 → M
A; I = (0 + 8) mod 26
= 8 → I
R; A = (17 + 0) mod 26
= 17 → R

Sedangkan proses dekripsi dengan menggunakan persamaan 4

Chiperteks : TEXAMIR
Kunci : SAMADIA
T; S = (19 - 18) mod 26
= 1 → B
E; A = (4 - 0) mod 26
= 4 → E
X; M = (23 - 12) mod 26
= 11 → L
A; A = (0 - 0) mod 26
= 0 → A
M; D = (12 - 3) mod 26
= 9 → J
I; I = (8 - 8) mod 26
= 0 → A
R; A = (17 - 0) mod 26

= 17 → R

3. HASIL DAN PEMBAHASAN

3.1 Gambaran Umum Sistem

Hasil penelitian yang diperoleh adalah dapat diterapkannya algoritma kriptografi klasik dengan mengkombinasikan algoritma Caesar Chiper dan Vigenere Chiper untuk menghasilkan pesan teks rahasia. Teks asli dapat di ubah menjadi teks yang dirahasiakan (chiperteks) dengan mengkombinasikan algoritma Caesar Chiper dan Vigenere Chiper, serta teks yang telah di enkripsi dapat dikembalikan menjadi teks asli (plainteks). Sedangkan penginisialan huruf alfabet A-Z menjadi angka 0 – 25 disajikan seperti Tabel 1 berikut.

Tabel 1. Penginisialan Huruf Alfabet

Huruf	A	B	C	D	...	Z
Angka	0	1	2	3	...	25

3.2 Pengujian Plainteks

Pengujian data plainteks digunakan agar teks asli dapat di enskripsi menjadi c ipherteks. Contoh data plainteks untuk pengujian adalah seperti berikut.

Plainteks : MINGGUDEPANMENIKAH
Kunci Caesar : 21
Kunci Vigenere : MUHNURTANZISSUTOYO

Caesar Chiper

Ubah plainteks menjadi nilai yang ekivalen

M	I	N	G	G	U	D	E	P	A	N	M	E	N	I	K	A	H
12	8	13	6	6	20	3	4	15	0	13	12	4	13	8	10	0	7

Lakukan proses enkripsi dengan menggunakan persamaan 1.

M = (12 + 21) mod 26
= 7
I = (8 + 21) mod 26
= 3
N = (13 + 21) mod 26
= 8
G = (6 + 21) mod 26
= 1
G = (6 + 21) mod 26
= 1
U = (20 + 21) mod 26
= 15
D = (3 + 21) mod 26
= 24
E = (4 + 21) mod 26
= 25
A = (0 + 21) mod 26
= 21
N = (13 + 21) mod 26
= 8
M = (12 + 21) mod 26
= 7
E = (4 + 21) mod 26
= 25
N = (13 + 21) mod 26
= 8
I = (8 + 21) mod 26
= 3
K = (10 + 21) mod 26
= 5
A = (0 + 21) mod 26
= 21

P = (15 + 21) mod 26
= 10

H = (7 + 21) mod 26
= 2

Menghasilkan chiperteks sebagai berikut.

7	3	8	1	1	15	24	25	10	21	8	7	25	8	3	5	21	2
H	D	I	B	B	P	Y	Z	K	V	I	H	Z	I	D	F	V	C

Vigenere Chiper

Dimana yang menjadi plainteks adalah chiperteks yang dihasilkan dari *Caesar Chiper.*
Plainteks : HDIBBPYZKVIHZIDFVC
Kunci : MUHNURTANZISSUTOYO

Ubah plainteks menjadi nilai yang ekivalen

H	D	I	B	B	P	Y	Z	K	V	I	H	Z	I	D	F	V	C
7	3	8	1	1	15	24	25	10	21	8	7	25	8	3	5	21	2

Ubah kunci menjadi nilai yang ekivalen

M	U	H	N	U	R	T	A	N	Z	I	S	S	U	T	O	Y	O
12	20	7	13	20	17	19	0	13	25	8	18	18	20	19	14	24	14

Lakukan proses enkripsi dengan menggunakan persamaan 3.

H; M = (7 + 12) mod 26
= 19

D; U = (3 + 20) mod 26
= 23

I; H = (8 + 7) mod 26
= 15

B; N= (1 + 13) mod 26
= 14

B; U= (1 + 20) mod 26
= 21

P; R = (15 + 17) mod 26
= 22

Y; T= (24 + 19) mod 26
= 17

Z; A= (25 + 0) mod 26
= 25

K; N = (10 + 13) mod 26
= 23

V; Z = (21 + 25) mod 26
= 20

I; I = (8 + 8) mod 26
= 16

H; S = (7 + 18) mod 26
= 25

Z; S = (25 + 18) mod 26
= 17

I; U = (8 + 20) mod 26
= 2

D; T = (3 + 19) mod 26
= 22

F; O = (5 + 14) mod 26
= 19

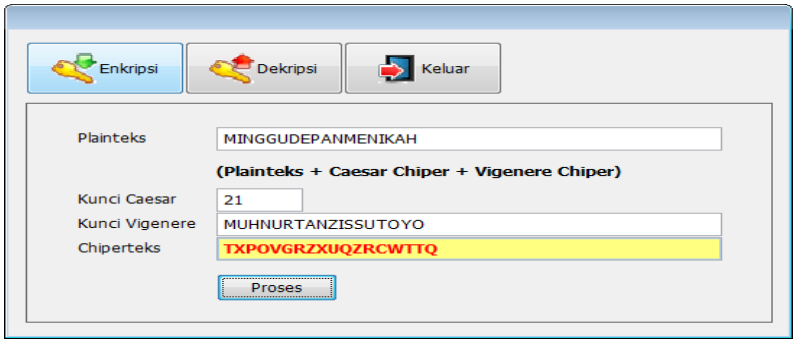
V; Y = (21 + 24) mod 26
= 19

C; O = (2 + 14) mod 26
= 16

Sehingga chiperteks yang dihasilkan sebagai berikut.

19	23	15	14	21	6	17	25	23	20	16	25	17	2	22	19	19	16
T	X	P	O	V	G	R	Z	X	U	Q	Z	R	C	W	T	T	Q

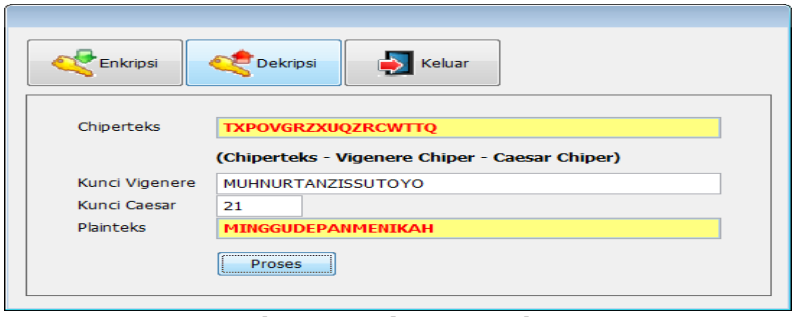
Dengan menggunakan sistem kombinasi *Caesar Chiper* dan *Vigenere Chiper* hasil enkripsi disajikan seperti Gambar 3.



Gambar 3. Hasil Proses Enkripsi

3.3 Pengujian Chiperteks

Pengujian data chiperteks digunakan agar teks yang telah terenkripsi dapat dikembalikan lagi menjadi plainteks (teks asli). Persamaan yang digunakan adalah persamaan 4, kemudian persamaan 2. Dengan menggunakan sistem kombinasi *Caesar Chiper* dan *Vigenere Chiper* hasil dekripsi disajikan seperti Gambar 4.



Gambar 4. Hasil Proses Dekripsi

4. KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa:

1. Kombinasi algoritma kriptografi *Caesar Chiper* dan *Vigenere Chiper* dapat digunakan untuk mengirim pesan rahasia.
2. Dengan mengkombinasikan algoritma *Caesar Chiper* dan *Vigenere Chiper* sulit untuk dapat dipecahkan dengan cara *brute force attack.* Sandi akan dapat dipecahkan jika kunci telah ditemukan (diketahui).

DAFTAR PUSTAKA

[1] Sadikin, R., 2012, *Kriptografi Untuk Keamanan Jaringan*, Andi, Yogyakarta

[2] Sasongko, J., 2005, Pengamanan Data Informasi Menggunakan Kriptografi Klasik, *Jurnal Teknologi Informasi DINAMIK Vol X No. 3 ISSN 0854-9524 pp 160-167.*

[3] Fitriasih, I., Prayitno, TB., Sidopekso, S., 2012, Studi Model Kriptografi Klasik (Review), *Jurnal Fisika dan Aplikasinya Vo. 13 Edisi 1 pp 6-11.*

[4] Doni, dan Walad, A., 2012, Caesar Chiper VS Vigenere Chiper, *Jurnal LPKIA Vol 1 No 3 pp 12-16.*

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

[6] Schneier, B., 2006, *Applied Cryptography, Second Edition: Protocol, Algorithms and Source Code in C,* John Wiley and Sons, Inc.

[7] Riyanto, MZ., 2007, *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Elgamal ata Grup Perganda Zp*,* Skripsi FMIPA UGM Yogyakarta.