IMPLEMENTASI PENGAMANAN DATA MENGGUNAKAN ENKRIPSI CAESAR CIPHER DENGAN KOMBINASI TABEL ASCII

Zulfidar[1)], Achmad Fauzi[2)]

[1), 2)] Program Pasca Sarjana Teknik Informatika Universitas Sumatera Utara
Jl. Universitas No. 24 A, Medan, Sumatera Utara, 20155
Email : zulfidarkun@gmail.com[1)], fauzyrivai88@gmail.com[2)]

Abstrak

Pada zaman yang semakin maju ini, keamanan merupakan hal yang paling penting untuk menjaga kerahasiaan data. Karena sering terjadinya banyak pihak yang tidak bertanggung jawab melakukan penyadapan terhadap informasi dan dapat merugikan pihak lain. dalam hal ini sangat terkait betapa pentingnya informasi dikirim dan diterima oleh orang yang dituju/menerima informasi.Informasi tidak akan berguna lagi apabila di tengah jalan informasi tersebut disada.Cara yang ditempuh adalah dengan kriptografi yang mengubah pesan sehingga pesan yang dikirimkan tidak dapat dibaca oleh pihak ketiga, karena itulah untuk menghindari kejadian tersebut maka pesan harus diubah sehingga pihak ketiga tidak bisa mengetahui isi pesan tersebut, salah satu teknik pengubahan pesan adalah dengan Caesar Cipher.

Caesar cipher termasuk dalam salah satu teknik enkripsi kriptografi yang menggunakan cara substitusi. Tapi untuk memperkuat keamanan dalam caesar cipher maka caesar cipher itu dimodifikasi dengan cara menambahakan penggunaan tabel ASCII. Dengan memanfaatkan penggabungan caesar cipher dengan tabel ASCII maka kerahasian/keamanan dari pesan lebih terjaga dan akan tidak mudah diketahui oleh pihak lain karena pesan yang ada atau plaintext akan diubah menjadi deretan angka dan huruf yang tidak bisa ditebak.

Kata kunci: *Kriptografi, keamanan, caesar cipher, substitusi, tabel ASCII.*

1. Pendahuluan

Dalam dunia sekarang ini , keamanan merupakan masalah besar dan mengamankan data yang penting sangat penting , sehingga data tersebut tidak dapat disadap atau disalahgunakan untuk tujuan ilegal dan dapat merugikan pihak lain. Bisa kita ambil contoh misalnya seorang komandan perang mengintruksikan anak buahnya mengenai taktik ataupun strategi untuk menyerang musuh tapi strategi itu malah disadap oleh pihak musuh sehingga pihak musuh dapat menggunakan kembali strategi itu untuk menyerang balik. Ini bisa sangat fatal karena akan terjadi banyak sekali jatuh korban. Untuk itulah pemerintah dan lembaga lainnya seperta bank berusaha mengamankan data mereka. Biarpun begitu tetap aja ada pihak-pihak yang berusaha membobol itu dengan menggunakan berbagai kunci dan juga metode. Untuk menghindari hal tersebut maka ubah data kedalam data yang tidak dapat dibaca oleh sang pengirim kemudian ubah kembali data tersebut dalam bentuk yang bisa dibaca oleh penerima. Teknik dan ilmu untuk membuat data yang tidak dapat dibaca sehingga hanya orang yang berwenang yang mampu membaca data tersebut itulah yang disebut Kriptografi[1].

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain.

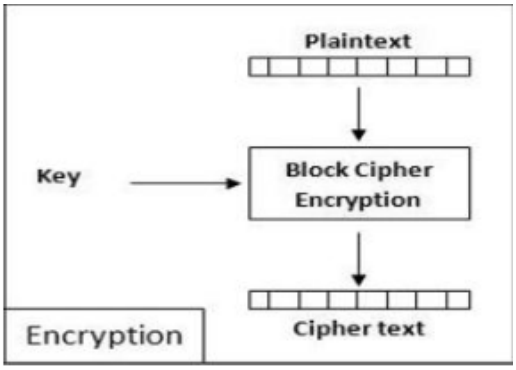
Ada empat tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi yaitu :[2]

a. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
b. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya
c. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
d. Non repudiasi, adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman / terciptanya suatu informasi oleh yang mengirimkan / membuat informasi tersebut.

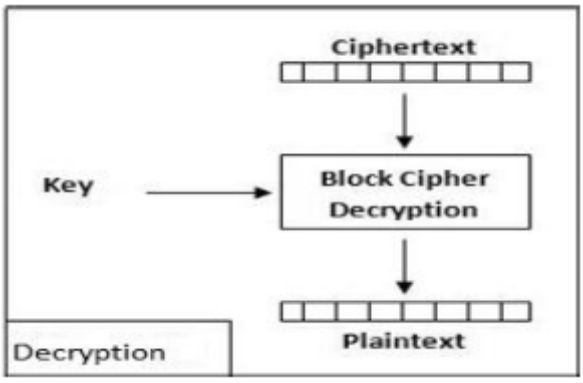
Dalam Kriptografi terutama di kriptografi klasik terdapat sebuah teknik substitusi yang digunakan pada jaman pemerintahan Yulius Caesar yang dikenal dengan *Caesar Cipher*[3].

Pada *Caesar Cipher* cara kerjanya adalah dengan mensubtitusi *plaintext* dengan kata kunci yang ada kemudian mengganti setiap huruf pada *plaintext* dengan

huruf yang ada pada kunci. Seperti yang ditunjukkan pada gambar 1 dan 2.



Gambar 1. *Plaintext ke chipertext*



Gambar 2. *Ciphertext ke Plaintext*

Untuk memperkuat keamanan/kerahasian *plaintext* atau pesan dengan menggunakan teknik *caesar cipher* yang ada. Teknik tersebut dimodifikasi dengan menggunakan proses enkripsi yang sama tapi proses enkripsi pada *caesar cipher* digabungkan/ditambah menggunakan tabel *ASCII*. Dengan mengunakan tabel *ASCII* maka kerahasian/keamanan dari pesan akan tidak mudah diketahui oleh pihak lain karena pesan akan diubah menjadi deretan angka dan huruf yang tidak bisa ditebak atau dipecahkan dengan mudah.

2. Pembahasan

2.1 Kriptografi

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[3].

Dalam bahasa kriptografi pesan yang dikirim disebut dengan *plaintext* dan pesan yang sebenarnya akan dikirim disebut dengan *ciphertext*[1].

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Proses enkripsi adalah mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi dari pesan tersebut tidak bisa dimengerti. Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M (*plaintext*) sehingga dihasilkan C (*ciphertext*), notasinya :
$C = E_e (M)$

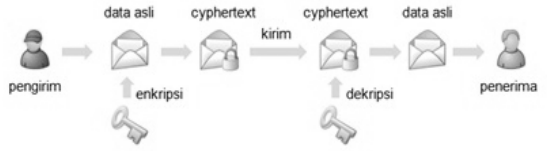
Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (dekripsi) menggunakan d (kunci dekripsi) pada C (*ciphertext*) sehingga dihasilkan M (*plaintext*), notasinya[4]:

$D_d(C) = M$

Berdasarkan kunci yang digunakan kriptografi terbagi atas dua jenis yaitu kriptografi simetris dan kriptografi simetris.

2.2 Kriptografi Simetris

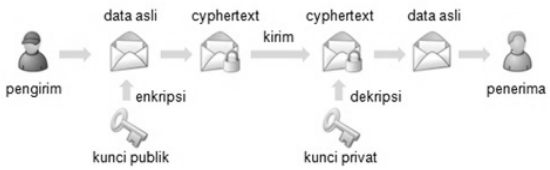
Kriptografi dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi[4]. Contoh : *Caesar cipher, Vigenere Cipher.*



Gambar 3. *Proses enkripsi dan deskripsi pada kriptografi simetris*

2.3 Kriptografi Asimetris

Kriptografi dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik *(public key)* dan kunci privat *(private key)*[4]. Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan payah mengetahui kunci privat yang digunakan. Contoh : RSA, DSA.



Gambar 4. *Proses enkripsi dan deskripsi pada kriptografi asimetris*

3. Perancangan Algoritma

Metode ini tidak jauh beda dengan *caesar cipher* yang di tambahkan pengurutan angka dan desimal huruf, heksadesimal dan oktal dari tabel *ASCII* yang dapat dilihat di gambar 5

Huruf	Decimal	Hexa	Oktal
A	65	41	101
B	66	42	102
C	67	43	103
D	68	44	104
E	69	45	105
F	70	46	106
G	71	47	107
H	72	48	110
I	73	49	111
J	74	4A	112
K	75	4B	113
L	76	4C	114
M	77	4D	115
N	78	4E	116
O	79	4F	117
P	80	50	120
Q	81	51	121
R	82	52	122
S	83	53	123
T	84	54	124
U	85	55	125
V	86	56	126
W	87	57	127
X	88	58	130
Y	89	59	131
Z	90	5A	132

Gambar 5. *Tabel ASCII*

Metode digunakan agar pesan yang dikirim tidak mudah untuk di ketahui oleh pihak lain, dengan kata lain bersifat *private* / rahasia.

3.1 Cara Kerja

Adapun cara kerja dari *caesar cipher* yang telah dimodifikasi sebagai berikut :

a. *Plaintext* di enkrip menggunakan *caesar cipher* menggunakan 1 kata kunci, dan *plaintext* yang akan di enkripsi harus dibagi menjadi masing-masing 5 huruf, apabila di kelompok terakhir kurang atau tidak mencukupi 5 hutuf maka dapat di lengkapi dengan huruf x atau menggunakan huruf terakhir dari kelompok huruf yang dibagi.
b. Hasil enkripsi di langkah pertama dikelompokkan menjadi 5 kelompok huruf yang kemudian dienkripsi lagi menggunakan tabel yang berisi huruf, urutan angka, desimal, hexa dan oktal dari tabel *ASCII* yang ditambah kata kunci yang tersedia. Tabel yang digunakan untuk enkripsi ditunjukkan pada gambar 6.

Huruf	Urut	Decimal	Hexa	Oktal
A	27	65	41	101
B	28	66	42	102
C	29	67	43	103
D	30	68	44	104
E	31	69	45	105
F	32	70	46	106
G	33	71	47	107
H	34	72	48	110
I	35	73	49	111
J	10	74	4A	112
K	11	75	4B	113
L	12	76	4C	114
M	13	77	4D	115
N	14	78	4E	116
O	15	79	4F	117
P	16	80	50	120
Q	17	81	51	121
R	18	82	52	122
S	19	83	53	123
T	20	84	54	124
U	21	85	55	125
V	22	86	56	126
W	23	87	57	127
X	24	88	58	130
Y	25	89	59	131
Z	26	90	5A	132

Gambar 6. *Tabel ASCII yang digunakan untuk enkripsi*

Enkripsi dilakukan dengan urutan huruf pertama dengan angka urutan huruf, huruf kedua dengan bilangan decimal, huruf ketiga dengan hexa, huruf keempat dengan oktal dan huruf kelima dengan kata kunci. Hasil dari enkripsi akan menghasilkan pola 2 2 2 3 1 yang berisikan huruf dan angka

c. Hasil enkripsi di langkah kedua digabung dan dipecah dengan pola 2 2 2 2 2 kemudian dienkripsi lagi menggunakan tabel yang ditunjukkan pada gambar 7

Huruf	Urut	Huruf	Urut
A	1	A	27
B	2	B	28
C	3	C	29
D	4	D	30
E	5	E	31
F	6	F	32
G	7	G	33
H	8	H	34
I	9	I	35
J	10		
K	11		
L	12		
M	13		
N	14		
O	15		
P	16		
Q	17		
R	18		
S	19		
T	20		
U	21		
V	22		
W	23		
X	24		
Y	25		
Z	26		

Gambar 7. *Tabel yang digunakan pada enkripsi langkah 3*

Hasil terakhir dari enkripsi pada langkah ketiga inilah *ciphe text* dari metode *caesar cipher* yang sudah dimodifikasi ini.

d. Untuk proses dekripsinya dapat diulang dari langkah ketiga, dengan cara dicocokkan kembali dengan tabel 3

Uji coba

Plaintext :

MUSUH SUDAH SAMPAI DAERAH PARIS

Kata Kunci : BURUNG ELANG

Dengan menerapkan langkah pertama maka *plain text* dipisah menjadi 5 kelompok huruf.

MUSUH SUDAH SAMPA IDAER AHPAR ISXXX

Setelah dipisah menjadi 5 kelompok huruf enkripsi dengan menggunakan 1 kata kunci yaitu BURUNG ELANG seperti yang ditunjukkan gambar 6.

huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
katakunci	B	U	R	N	G	E	L	A	C	D	F	H	I	J	K	M	O	P	Q	S	T	V	W	X	Y	Z

Gambar 6. *Enkripsi dengan kata kunci*

Setelah dienkripsi dengan menggunakan kata kunci seperti yang kelihatan di gambar 1. Maka didapatlah hasil enkripsi pertama yaitu :

Plaintext :
MUSUH SUDAH SAMPA IDAER AHPAR ISXXX
Hasil Enkripsi :
ITQTA QTNBA QBIMB CNBGP BAMBP CQXXX

Enkripsi kembali dengan menggunakan tabel 2 seperti pada gambar 8

huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
urut	27	28	29	30	31	32	33	34	35	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
desimal	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
HEX	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A
OKTAL	101	102	103	104	105	106	107	110	111	112	113	114	115	116	117	120	121	122	123	124	125	126	127	130	131	132
katakunci	B	U	R	N	G	E	L	A	C	D	F	H	I	J	K	M	O	P	Q	S	T	V	W	X	Y	Z

Gambar 8. *Enkripsi menggunakan tabel 2*

Dari enkripsi langkah dua didaptlah hasil enkripsinya sebagai berikut :

Hasil Enkripsi Pertama :
ITQTA QTNBA QBIMB CNBGP BAMBP CQXXX
Hasil Enkripsi Kedua :
358451124B 17844E102B 176649115U 297842107M
28654D102M 298158130x

Hasil enkripsi kedua dibuat lagi dengan pola 2 2 2 2 2 dan kemudian di enkripsi lagi dengan menggunakan tabel 3 seperti yang kelihatan di gambar 9

huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
urut	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
huruf	A	B	C	D	E	F	G	H	I																	
urut	27	28	29	30	31	32	33	34	35																	

Gambar 9. *Enkripsi dengan menggunakan tabel 3*

Dari situ didapatlah Hasil terakhir dari enkripsi pada langkah ketiga inilah *ciphertext*nya seperti yang ditunjukkan pada tabel 1

Tabel 1. *Tabel Hasil Akhir dari enkripsi*

Hasil Enkrispi 2 yang telah dibuat pola	Hasil Akhir dari enkripsi
35 84 51 12 4B	I 84 51 L 4B
17 84 4E 10 2B	Q 84 4E J 2B
17 66 49 11 5U	Q 66 49 K 5U
29 78 42 10 7M	C 78 42 J 7M
28 65 4D 10 2M	B 65 4D J 2M
29 81 58 13 0X	C 81 58 M 0X

4. Kesimpulan

Implementasi dari percobaan yang dilakukan dengan pengubahan cara enkripsi pada *caesar cipher* ini yang telah ditambahkan tabel *ASCII* dan juga tabel huruf perulangan maka plaintext diubah menggunakan pola yang ada akan menghasilan deretan yang terdiri dari angka dan huruf.
Dengan begitu keamanan data atau pesan yang dikirim dapat lebih aman dan tidak mudah dibobol oleh orang lain karena pesan yang dikirim berupa deretan angka dan huruf yang tidak beraturan maka pihak lain yang berniat jahat akan kesulitan untuk memecahkannya.

Daftar Pustaka

[1] Kashish Goyal, Kinger Supriya, "Modified Caesar Cipher for Better Security Enhancement",International Journal of Computer Applications Vol. 73,No 3, 2013.
[2] Ariyus, Dony,"*Computer Security*".Penerbit Andi, Yogyakarta, 2006
[3] Ariyus, Dony," Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi".Penerbit Andi, Yogyakarta, 2008
[4] Hermawati, Kuswari, "Implementasi Cipher Hill pada kode ASCII dengan memanfaatkan Digit Desimal Bilangan Euler", Prosiding Seminar Nasional MIPA, 2006.

Biodata Penulis

Zulfidar, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2011. Saat ini sedang mengikuti Program Studi Magister Teknik Informatika di Universitas Sumatera Utara Medan. Mempunyai sebuah perusahaan yang bergerak dalam penjualan action figure/mainan dari jepang. Perusahaan yang berjalan dengan sistem penjualan secara *online* dengan nama toko OuKi SHOP.

Achmad Fauzi, memperoleh gelar Ahli Madya (A.Md), Jurusan Teknik Komputer Manajemen D3 AMIK POLIBISNIS Medan, lulus tahun 2010.. Memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika Komputer, lulus tahun 2012 Saat ini sedang mengikuti Program Studi Magister Teknik Informatika di Universitas Sumatera Utara Medan. Menjabat sebagai Dosen di AMIK POLIBISNIS MEDAN.

ISSN : 2302-3805