MULTIPLE ENCRYPTION DENGAN MENGGUNAKAN METODE VIGENERE CHIPER DAN BLOWFISH

Danang Haryo Sulaksono
Jurusan Teknik Informatika
Institut Teknologi Adhi Tama Surabaya
Email: danang_h_s@itats.ac.id

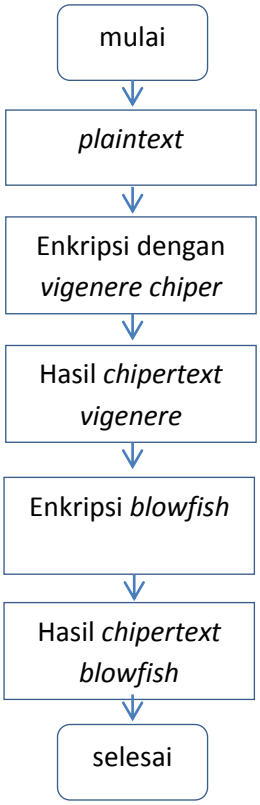
Abstrak. *Algoritma enkripsi bermain penting dalam sistem sekuritas data-text digital. Di lain sisi, pemecahan kode enkripsi juga ikut berkembang sehingga satu algoritma saja tidak cukup mengamankan data-text digital. Dibutuhkan multiple encryption untuk pengamanan yang lebih baik. Penelitian dalam paper menggunakan metode Vigenere dan Blowfish. Vigenere chiper adalah sebuah metode dari enkripsi text alfabet dengan menggunakan sebuah seri dari Caesar Chiper. Blowfish adalah sebuah feistel network, melakukan iterasi sebuah fungsi sederhana enkripsi sebanyak 16 kali. Penelitian ini mengambil avalanche effect sebagai pengujian dengan nilai 28,62% untuk vigenere chiper, 68,53% untuk blowfish, dan 69,60% untuk multiple encryption. Hal ini membuktikan multiple encryption lebih baik dari pada single encryption.*

Kata Kunci: *Data-text, Multiple Encryption, Vigenere Chiper, Blowfish, Key, Avalanche Effect*

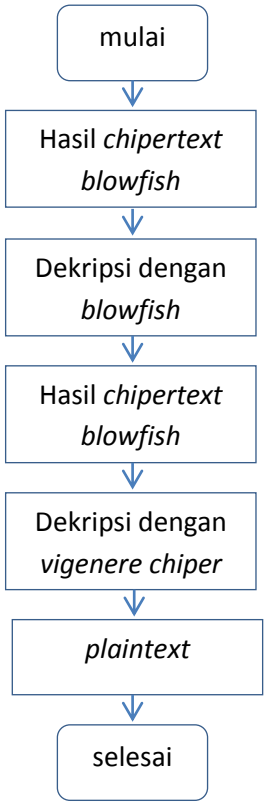
Penyimpanan data-text dalam bentuk digital menjadi salah satu pilihan yang terbaik, karena tidak membutuhkan tempat penyimpanan yang besar. Selain itu pemilik data-text dapat dengan mudah membuat, mengubah, dan menghapus kapanpun serta mengirim data-text kemanapun, sehingga data-text digital mempunyai *fleksibilitas* dan *mobilitas* yang sangat tinggi. Namun di balik manfaat tersebut ada bahaya yang tidak disadari oleh pemilik data-text digital, yaitu rentannya data-text untuk dicuri atau dibajak oleh orang lain. Sehingga butuh suatu mekanisme untuk mengamankan data-text. Algoritma enkripsi berperan penting dalam sekuritas data-text digital. Di sisi lain, perkembangan pemecahan kode enkripsi juga ikut berkembang sehingga tidak cukup mengamankan data-text digital. Dibutuhkanlah beberapa level algoritma atau yang dapat juga disebut *multiple encryption* untuk mengamankan *data-text* tersebut. *Multiple encryption* adalah sebuah teknik yang dapat meningkatkan keamanan data-text dengan melakukan proses enkripsi dengan beberapa kali menggunakan algoritma yang sama atau berbeda sehingga dapat meningkatkan kompleksitas enkripsi [6]. Penelitian dalam paper ini menggunakan metode *Vigenere Chiper* dan *Blowfish* untuk implementasi *multiple encryption*. *Vigenere chiper* adalah sebuah metode dari enkripsi text alfabet dengan menggunakan sebuah seri dari *Caesar Chiper* yang berdasarkan pada *keyword*. *Vigenere chiper* adalah sebuah bentuk sederhana dari *polyalphabetich subtitutions*. *Blowfish* adalah sebuah *feistel network*, melakukan iterasi sebuah fungsi sederhana enkripsi sebanyak 16 kali. Ukuran bloknya adalah 64 bit, dan *keynya* dapat sepanjang 448 bit sehingga *blowfish* mempunyai *key* bervariasi yang berupa *block chiper* [2]. Dengan metode ini diharapkan pengamanan data-text akan lebih baik lagi.

I. Metodologi

Penelitian ini mengimplementasikan sebuah metode dengan dua level enkripsi yaitu *multiple encryption*, Algoritma yang digunakan adalah *vigenere chiper* dan *blowfish*. *Plaintext* yang telah dienkripsi oleh *vigenere chiper* akan dienkripsi lagi oleh *blowfish*, begitu juga ketika proses dekripsi, hasil *chipertext* akan didekripsi oleh *blowfish* lalu *vigenere chiper*. Secara garis besar alur enkripsi dan dekripsi penelitian ini ditunjukkan dalam *flowchart* pada gambar 1.1 :



Gambar 1.1 Alur kerja enkripsi pada aplikasi



Gambar 1.2 Alur kerja dekripsi pada aplikasi

Proses enkripsi vigenere Chiper

Vigenere chiper sebenarnya merupakan pengembangan dari sandi *caesar*. Pada *caesar chiper*, setiap huruf teks digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet.

Dimisalkan, pada *caesar chiper* dengan penggeseran, A menjadi D, B menjadi E dan seterusnya. *Vigenere chiper* terdiri dari beberapa sandi *caesar* dengan nilai geseran yang berbeda. Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut *vigenere square* yang ditunjukkan pada gambar dibawah ini.

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

Gambar 1.1 *Vigenere square*

Dasar *vigenere chiper* adalah *sebuah polyalphabetic chiper*, dimana *chipertextnya* diperoleh dengan tambahan modular dari perulangan atau iterasi pada *key phase* dan sebuah *plaintext* dimana keduanya mempunyai panjang yang sama. Rumus dasarnya adalah :

$$C_i \equiv T_i + K_i \, mod(m)$$

C_i = karakter dari *chipertext* ke i
T_i = karakter *plaintext* ke i
K_i = karakter dari *key phase* (jika *key phase* lebih pendek dari *plaintext*, dari *key phase* maka akan diiterasi sesuai dengan panjang dari *plaintext*)
m = panjang dari alfabet

Algoritma *vigenere chiper* adalah sebagai berikut :

```
for i to m
C[i] = (T[i] - a + key[i % m]
- a) % 26 + A
```

m = adalah variabel yang menyimpan panjang text
T[i] = adalah variabel array yang menyimpan *plaintext*
C[i] = adalah variabel array yang menyimpan hasil enkripsi

Untuk mengenkripsi *plaintext*, pertama yang harus dilakukan adalah menjumlah huruf pertama dari *plaintext* dan *key phase*, huruf kedua, ketiga dan seterusnya. Untuk mengenkrip huruf ke n dari *plaintext* diasumsikan adalah "L" menggunakan *vigenere square*, maka akan ditemukan huruf pada *horizontal axis* pada tabel dan akan ditemukan huruf ke n dari *key phase* dalam *vertical axis* diasumsikan adalah "T". Pada persimpangan baris dan kolom yang ada menghasilkan huruf ke n yaitu adalah "E".

Sebagai contoh adalah kalimat ATTACK AT DAWN mempunyai kunci CAT, panjang alfabet adalah 26, maka perhitungannya adalah:

```
A + C = 0  + 2  = 2  = C
T + A = 19 + 0  = 19 = T
T + T = 19 + 19 = 12 = M
A + C = 0  + 2  = 2  = C
C + A = 2  + 0  = 2  = C
K + T = 10 + 19 = 3  = D
A + C = 0  + 2  = 2  = C
T + A = 19 + 0  = 19 = T
D + T = 3  + 19 = 22 = W
A + C = 0  + 2  = 2  = C
W + A = 22 + 0  = 22 = W
N + T = 13 + 19 = 6  = G
```

Maka *chipertext* yang dihasilkan adalah CTMCCDCTWCWG [5].

Enkripsi Vigenere Chiper

Implementasi algoritma *vigenere chiper* dengan menggunakan 306 karakter adalah sebagai berikut :

Plaintext :

```
Algoritma enkripsi bermain penting
dalam sistem sekuritas data-text
digital. Di lain sisi, pemecahan kode
```

Kata kunci : MULTIPLEENCRYPTION

Chipertext :

```
Ngsiayfrf sqcqyjbx prmyurd bjshlff
tuupa fdennc ejpiuasqm mphn-oqrc
tulnhdd. Cy fjxb fdec, yuyjhoksm aimt
safdcyiu ozud ajkn ktfxzyvjds xjvlffwu
bphh vxaxhuyro vsiq nrsox xgedf
yjsudezdejc rnom-nnnf inullzb.
```

Proses Enkripsi Blowfish

Blowfish adalah sebuah enkripsi berbentuk *chiper* yang mempunyai blok simetris, dan mempunyai 16 putaran. Algoritma ini mempunyai panjang *key* yang bervariasi, dari 32 bit sampai dengan 448 bit, sehingga sangat ideal untuk memproteksi data. Algoritma *blowfish* adalah sebuah *Feistel Network* yang melakukan iterasi sebuah fungsi enkripsi sederhana sebanyak 16 kali [c].

Blowfish menggunakan sejumlah besar *subkey*. Semua *subkey* ini harus dikomputasi sebelum data enkripsi dan deskripsi, proses *subkey* adalah :

```
P-array terdiri dari 18 subkey 32
bit : P1, P2,..., P18.
Empat S-box 32 bit dengan 256
masukan, yaitu :

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.
```

Algoritma enkripsi *blowfish* adalah sebagai berikut :

```
for i = 1 to 16{
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
    If i=16{
    swap xL
    swap xR
    }
Then, xR = xR XOR P17 and xL = xL
XOR P18.
}
chiperText = xL AND xR
```

x = variabel input dengan data elemen 64 bit
xL, xR = variabel penyimpan hasil bagi 32 bit, dimana setiap variabel mempunyai 16 bit
chipherText = variabel untuk menyimpan *chipertext*

Algoritma *blowfish* mempunyai dua bagian yaitu sebuah *key-expansion* dan sebuah *data-encryption*. *Key-expansion* mengubah sebuah *key* dari kurang lebih 448 bit menjadi beberapa *subkey* berbentuk *array* dengan total 4168 bit. Data yang terenkripsi terjadi melalui sebuah *feistel network* dengan 16 putaran, setiap putaran mempunyai sebuah permutasi dengan *key-dependent*, sebuah *key* dan subtitusi *data-dependent*. XOR dan tambahan dari kata 32 bit.

Enkripsi Blowfish

Seperti yang telah dijelaskan pada alur program sebelumnya bahwainputan enkripsi *blowfish* adalah *chipertext* hasil dari enkripsi *vigenere chiper*, sehingga enkripsi dengan algoritma *blowfish* adalah :

Chipertext vigenere chiper :

```
Ngsiayfrf sqcqyjbx prmyurd bjshlff
tuupa fdennc ejpiuasqm mphn-oqrc
tulnhdd. Cy fjxb fdec, yuyjhoksm aimt
safdcyiu ozud ajkn ktfxzyvjds xjvlffwu
bphh vxaxhuyro vsiq nrsox xgedf
yjsudezdejc rnom-nnnf inullzb.
```

Kata Kunci : TEKNIKINFORMATIKA

Chipertext blowfish :

```
1b08eb159e705be61172215cbf45b250
0fa800ff646d436a28ad8c6e1b3d3827
b619a866cb09b5ebacb9560256e89693
e152d1186b93300d1c121d2d37e58f99
50cc6e17546dbda369cda2da3efa0c1f
3e63441fda7ad08a6421a1d95ee4dbb2
356b8f40e4425c06555a1934fa881dd4
4e758a7c4a838b34542d01cff72c91a7
480d15bb8ee6a5222c741d839d3dd423
fcf76490cd1a3f72f08ccffbbfe8d889
05d4661584534d90f9f3d26482c7eb0a
44e7a61d3b54da8c3408ab1397d91a07
78b1ad753a59359f1d9cc2350e8985fa
```

Dekripsi Blowfish

Proses dekripsi *blowfish* sama dengan proses enkripsi, kecuali p-arrays digunakan dengan cara terbalik. Karena itu, algoritma *blowfish* mengenkripsi dengan membagi setengah blok (32 bit) menjadi 8 bit *quarter* kedalam S-box. Hasil dari s-box lalu ditambahkan dan di XOR. Proses dekripsi *blowfih* sangat sederhana dan diselesaikan dengan hanya membalik p17 dan p18 blok *chiper* dan menggunakan masukkan p dengan cara terbalik.

s-box dan p-box diinisialisasi dengan nilai digit hex dari pi. Panjang *key* variabel yang user masukkan lalu di XOR kan dengan masukkan P. Lalu blok nol di enkripsi, dan hasil ini digunakn untuk masukkan p1 dan p2. *Chipertext* hasil dari enkripsi blok nol lalu dienkripsi lagi dan digunakan untuk p3 dan p4. Proses ini dilakukan sampai setiap masukkan p–box dan s-box tergantikan, menghasilkan 521 generasi *key*. Hal ini termasuk juga data proses sebesar 4KB. Dekripsi dengan algoritma *blowfish* adalah :

Chipertext blowfish :

```
1b08eb159e705be61172215cbf45b250
0fa800ff646d436a28ad8c6e1b3d3827
b619a866cb09b5ebacb9560256e89693
e152d1186b93300d1c121d2d37e58f99
50cc6e17546dbda369cda2da3efa0c1f
3e63441fda7ad08a6421a1d95ee4dbb2
356b8f40e4425c06555a1934fa881dd4
4e758a7c4a838b34542d01cff72c91a7
480d15bb8ee6a5222c741d839d3dd423
fcf76490cd1a3f72f08ccffbbfe8d889
05d4661584534d90f9f3d26482c7eb0a
44e7a61d3b54da8c3408ab1397d91a07
78b1ad753a59359f1d9cc2350e8985fa
```

Chipertext ouput dari *blowfish* :

```
Ngsiayfrf sqcqyjbx prmyurd bjshlff tuupa fdennc ejpiuasqm mphn-oqrc tulnhdd. Cy fjxb fdec, yuyjhoksm aimt safdcyiu ozud ajkn ktfxzyvjds xjvlffwu bphh vxaxhuyro vsiq nrsox xgedf yjsudezdejc rnom-nnnf inullzb.
```

Dekripsi Vigenere Chiper

Dekripsi pada *vigenere chiper* mempunyai proses yang hampir sama dengan enkripsi, kecuali hasil *plaintext* didapatkan dengan mengurangi huruf dari *key* yang terduplikasi dari huruf *chipertext*. Dekripsi pada *vigenere chiper* mempunyai rumus dasar :

$$T_i \equiv C_i - K_i \, mod(m)$$

C_i = karakter dari *chipertext* ke i
T_i = karakter *plaintext* ke i
K_i = karakter dari *key phase* (jika *key phase* lebih pendek dari *plaintext*, dari *key phase* maka akan diiterasi sesuai dengan panjang dari *plaintext*)
m = panjang dari alfabet

maka output dari proses dekripsi dari *vigenere chiper* adalah :

Chipertext dari blowfish :

```
Ngsiayfrf sqcqyjbx prmyurd bjshlff tuupa fdennc ejpiuasqm mphn-oqrc tulnhdd. Cy fjxb fdec, yuyjhoksm aimt safdcyiu ozud ajkn ktfxzyvjds xjvlffwu bphh vxaxhuyro vsiq nrsox xgedf yjsudezdejc rnom-nnnf inullzb.
```

Kata kunci : MULTIPLEENCRYPTION

Hasil plaintext :

```
Algoritma enkripsi bermain penting dalam sistem sekuritas data-text digital. Di lain sisi, pemecahan kode enkripsi juga ikut berkembang sehingga satu algoritma saja tidak cukup mengamankan data-text digital.
```

II. Hasil dan Pembahasan

Analisa penelitian ini menggunakan *avalanche effect*, yaitu perubahan bit yang terjadi antara sebuah input dan output sebuah algoritma enkripsi. nilai *avalanche affect* didapatkan dengan rumus :

$$avalanche\ e. = \frac{jbt}{jbc}\ x\ 100\%$$

jbt = jumlah bit yang terbalik dalam *chipertext*
jb = jumlah bit keseluruhan dalam *chipertext*

Hasil *avalanche effect* yang dihitung ada tiga jenis adalah hasil enkripsi *vigenere chiper*, *blowfish* dan metode *multiple encryption*.

Avalanche Effect Vigenere Chiper

Hasil perbandingan *avalanche effect vigenere chiper* adalah dengan perbandingan antara *plaintext* dengan *vigenere chiper*. Dari hasil penelitian diketahui jbt = 474 bit dan jbc = 1664, maka :

$$avalanche\ e. = \frac{474}{1664}\ x\ 100\%$$

Hasilnya adalah 28,62%

Avalanche Effect Blowfish

Hasil perbandingan *avalanche effect* ini adalah dengan membandingkan antara *plaintext* dengan *blowfish*. Dari hasil penelitian diketahui jbt = 2281 bit dan jbc = 3328, maka :

$$avalanche\ e. = \frac{2281}{3328}\ x\ 100\%$$

Hasilnya adalah 68,53%

Avalanche Multiple Encryption

Hasil dengan metode ini adalah dengan membandingkan *chipertext* dari *vigenere chiper* dengan *chipertext* dari *blowfish*. Dari hasil penelitian diketahui jbt = 2316 bit dan jbc = 3328, maka :

$$avalanche\ e. = \frac{2316}{3328}\ x\ 100\%$$

Hasilnya adalah 69,60%

III. Simpulan

Hasil penelitian dengan metode diatas dapat disimpulkan bahwa Keamanan enkripsi dari *vigenere chiper* adalah yang terendah, hal ini dibuktikan dengan nilai *avalanche effect* 28,62%. Sedangkan keamanan dari *blowfish* masih lebih baik dibandingkan dengan *vigenere chiper* dan dalam penelitian ini menempati urutan kedua dalam hal sekuritas enkripsi, karena mempunyai nilai *avalanche effect* sebesar 68,53%. Nilai *avalanche effect* dimiliki oleh metode *multiple encryption* dengan nilai *avalanche effect* sebesar 69,60%. Hal ini membuktikan bahwa *multiple encryption* mempunyai kemampuan enkripsi yang lebih baik dibandingkan dengan *single encryption*.

IV. Daftar Pustaka

[1] Chris Christensen, Cryptography of the Vigenère Cipher, Fall 2006

[2] PocketBrief, Blowfish Encryption Algorithm

[3] Bill Gatliff, Encrypting data with the Blowfish algorithm, Gdbstubs Library

[4] D. S. Abdul. Elminaam, Performance Evaluation of Symmetric Encryption Algorithms

[5] http://www.programming-algorithms.net/article/45623/Vigenere-cipher

[6] MD Asif Mushtaque, Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014

[7] Himanshu Gupta, Role Of Multiple Encryption In Secure Electronic Transaction

[8] Jawahar Thakur, DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011

[9] Ganesh Patidar, A block based Encryption Model to improve Avalanche Effect for data Security.