

IMPLEMENTASI ENKRIPSI PESAN TEXT MENGUNAKAN ALGORITMA VIGÉNERE CHIPER (STUDI KASUS PEMOGRAMAN DEV- C++)

Eva Darnila, Munirul Ula, Abdul Halim

Teknik Informatika Universitas Malikussaleh, Lhokseumawe
Jl. Kampus Unimal BI Blang Pulo, Aceh Utara, Indonesia

E-mail : abdulhalimm424@gmail.com

ABSTRAK

Data dan informasi saat ini menjadi hal yang tidak dapat dipisahkan lagi. Tetapi pada saat tertentu kita melupakan aspek-aspek penting, yaitu keamanan aspek informasi dan data tersebut. Karena itu kita harus selalu waspada ketentuan keamanan data. Teknik enkripsi dan deskripsi penulis yang mana akan menerapkan pesan text, teknik keamanan yang diadopsi dari keamanan kuno teknik, yang penulis terapkan pada bahasa pemrograman. Ubah dari teks biasa ke teks sandi adalah fungsi dasar teknik enkripsi dan deskripsi ini. Teknik enkripsi dan deskripsi saya, menggunakan algoritma Vigénere Cipher mampu mengamankan data, dengan bantuan aplikasi Dev- C++.

Kata kunci : *Data, Informasi, Teknik, Keamanan, Pesan Text, Enkripsi, Deskripsi, Algoritma Vigénere Chiper, Dev- C++*

1. PENDAHULUAN

Perkembangan teknologi saat ini memungkinkan manusia untuk berkomunikasi dan saling bertukar informasi dengan jarak jauh. Pertukaran informasi jarak jauh seperti antar kota, antar wilayah dan bahkan antar benua sudah tidak menjadi kendala lagi namun dilain hal keamanan atau sekuritas terhadap kerahasiaan informasi saat inilah yang menjadi persolan.

Banyak pengguna internet yang saat ini khawatir terhadap pengiriman informasi diketahui oleh pihak lain. Untuk mengatasi persoalan ini sebuah metode untuk keamanan informasi yang dikenal dengan kriptografi. Dalam kriptografi dikenal dengan dua konsep utama yakni enkripsi dan dekripsi.

2. METODE PENELITIAN

Dalam penelitian ini terdapat dua proses penting di dalam kriptografi yang berperan sangat penting dalam merahasiakan suatu informasi yaitu Enkripsi (*Encryption*) dan Dekripsi (*Decryption*). Enkripsi adalah bentuk transformasi data (*plaintext*) ke dalam bentuk yang hampir tidak dapat dibaca (*Ciphertext*) tanpa pengetahuan yang cukup. Tujuan dari Enkripsi adalah untuk menjamin kerahasiaan dengan menjaga informasi tersembunyi dari siapapun yang bukan pemilik atau memiliki akses terhadap data yang telah dienkripsi. Sedangkan Dekripsi adalah kebalikan dari Enkripsi yaitu transformasi dari data yang telah dienkripsi (*Ciphertext*) kembali ke bentuk semula (*Plaintext*). Proses enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, yang sering disebut dengan kunci (*Key*)

3. HASIL DAN PEMBAHASAN

3.1 Algoritma Vigénere Chiper

Vigénere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul *La Cifra del. Sig.* Giovan Battista Bellaso pada tahun 1553. Nama Vigénere sendiri diambil dari seorang yang bernama Blaise de Vigénere.

Vigénere Cipher merupakan polyalphabetic substitution cipher yang paling sederhana dan paling banyak dikenal. Sandi Vigénere sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E dan seterusnya. Sandi Vigenère terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda. Kelebihannya dibanding Caesar Cipher dan cipher monoalfabetik lainnya adalah cipher ini tidak begitu rentan terhadap metode pemecahan cipher yang disebut analisis frekuensi.

Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenere. Tabel Vigenere berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.

	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. Tabel Vigenere

3.2 Program Dev- C++

C++ merupakan bahasa pemrograman yang diciptakan pada tahun 1980, ketika Bjarne Stroustrup melakukan pekerjaan untuk memperoleh gelar Ph.D. sedangkan Dev- C++ adalah sebuah IDE (Integrated Development Environment) C / C++ yang sudah dilengkapi dengan TDM-GCC Compiler (bagian dari *GNU Compiler Collection / GCC*). Dev- C++ merupakan IDE gratis dan full featur yang didistribusikan dibawah

lisensi *GNU General Public License* untuk pemrograman C dan C++. IDE sendiri adalah Lembar kerja terpadu untuk pengembangan program.

Bahasa C++ adalah bahasa pemrograman komputer yang merupakan pengembangan dari bahasa C yang disempurnakan oleh Bjarne Stroustrup pada tahun 1980 menjadi C dengan kelas (C With Classes) dan berganti nama pada tahun 1983 menjadi C++. awalnya C++ disebut "a better C" kemudian berganti nama pada tahun 1983 menjadi C++. Symbol ++ merupakan operator C untuk operasi increment (penaikan), digunakan untuk menunjukkan bahwa bahasa baru ini merupakan versi yang lebih canggih dari C. Fungsi Dev- C++ sebagai berikut :

- 1) Menulis Program/Source Code
- 2) Mengkompilasi Program (Compile)
- 3) Melakukan Pengujian Program (Debugging)
- 4) Mengaitkan Object dan Library ke Program (Linking)
- 5) Menjalankan Program (Running).

Source Kode Program Enkripsi Algoritma Vigénere Chiper :

```
#include <stdio.h>
#include <string.h>
int main()
{
    char plain[500];
    printf("Enter plaintext : ");
    gets(plain);

    char key_str[25];
    printf("Enter key : ");
    gets(key_str);

    int cipher = 0;
```

```
int j = 0;

printf("Cipher text: ");
for (int i = 0; i < strlen(plain); i++)
{
    int index = j % strlen(key_str);
    int key = key_str[index];
    if (key_str[index] >= 'A' && key_str[index] <= 'Z')
    {
        key = key - 'A';
    }
    else if (key_str[index] >= 'a' && key_str[index] <= 'z')
    {
        key = key - 'a';
    }
    if ((plain[i] >= 'A' && plain[i] <= 'Z') || (plain[i] >= 'a' && plain[i] <= 'z'))
    {
        j++;
    }

    cipher = plain[i];
    if (plain[i] == ' ')
    {
        cipher = ' ';
    }
    else if (plain[i] < 'A' || (plain[i] > 'Z' && plain[i] < 'a') || plain[i] > 'z')
    {
        cipher = plain[i];
    }
}
```

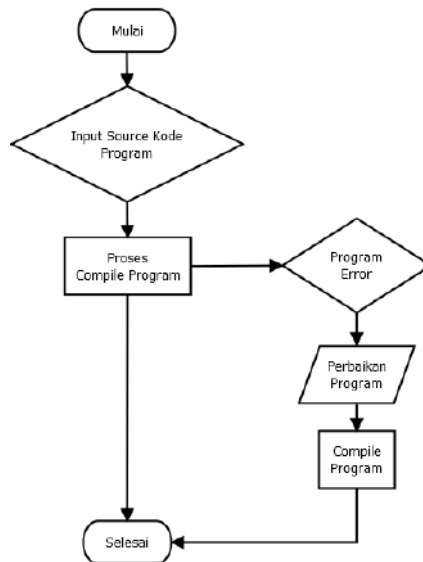
```
    }  
    else if (plain[i] >= 'A' && plain[i] <= 'Z')  
    {  
        cipher = ((plain[i] + key - 'A') % 26) + 'A';  
    }  
    else if (plain[i] >= 'a' && plain[i] <= 'z')  
    {  
        cipher = ((plain[i] + key - 'a') % 26) + 'a';  
    }  
    printf("%c", cipher);  
}  
printf("\n");  
return 0;  
}
```

3.3 Skema Sistem

Skema sistem digunakan untuk mengilustrasikan beberapa informasi tentang file suara yang terkait dengan aplikasi yang akan dibangun. Dari beberapa pengambilan *sample* yang sudah dilakukan semuanya akan diilustrasikan dalam bentuk skema yang berkaitan dengan sistem yang berkaitan antara satu dengan lainnya. Skema sistem adalah struktur dan mekanisme untuk menghubungkan sekumpulan unsur atau elemen yang saling berkaitan dan saling mempengaruhi dalam melakukan kegiatan bersama untuk mencapai suatu tujuan.

1) Skema Dev- C++

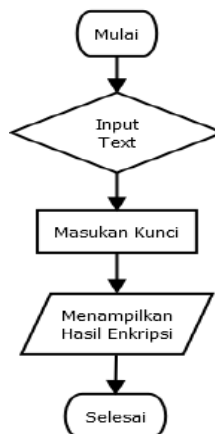
Skema *Dev- C++* adalah rancangan *flowchart* yang menggambarkan proses penulisan source kode dan pengkompiler untuk mengetahui hasilnya apakah source kode program tersebut error yang telah *diinput*.



Gambar 2. Flowchart Dev- C++

2) Skema Enkripsi Pesan Text

Skema *Enkripsi Pesan Text* adalah rancangan *flowchart* yang menggambarkan proses penginputan text untuk mengetahui hasil yang telah diinput.



Gambar 3. Flowchart Enkripsi Pesan Text

3.4 Contoh Proses Enkripsi Pesan Text

Plaintext : Terstruktur Adalah urutan barisan langkah-langkah yang digunakan harus disusun sedemikian rupa proses penyelesaian tidak berbelit sehingga bagian proses dapat dibedakan dengan jelas mana bagian input, proses dan output sehingga memudahkan pengguna melakukan pemeriksaan ulang.

Kunci : UNIMAL

Chipertext :

Dan hasilnya sebagai berikut :

Chipertext : Nrzetcoxbgr lxntmh flhbm mueqay fnvsklb-yizgvuu
gmnr xvognlenv tacof lusfmhv eooyzqwilh ecba albaqs
ayagqlpmnqmn ecqiw bplomxie mrpunran jmgtua xdodyf
lmpln qqneouxiz dphtiz jpfna yayu oisilh vvbue, jweed xnv
auejhb eescaosa xyzcpasenv beyatcza xyyiwuvua
xqmplvsealh htmnr.



```

C:\Users\ACER\Documents\Algoritma Vigenere Chiper.exe
Enter plaintext : Terstruktur adalah urutan barisan langkah-langkah yang digunak
an harus disusun sedemikian rupa proses penyelesaian tidak berbelit sehingga bag
ian proses dapat dibedakan dengan jelas mana bagian input, proses dan output seh
ingga memudahkan pengguna melakukan pemeriksaan ulang.
Enter key : UNIMAL
Cipher text: Nrzetcoxbgr lxntmh flhbm mueqay fnvsklb-yizgvuu gmnr xvognlenv ta
cof lusfmhv eooyzqwilh ecba albaqs ayagqlpmnqmn ecqiw bplomxie mrpunran jmgtua x
dodyf lmpln qqneouxiz dphtiz jpfna yayu oisilh vvbue, jweed xnv auejhb eescaosa
xyzcpasenv beyatcza xyyiwuvua xqmplvsealh htmnr.

-----
Process exited after 207.8 seconds with return value 0
Press any key to continue . . .

```

Gambar 4. Hasil Enkripsi

4. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian pada program Dev- C++ yang telah dilakukan dapat disimpulkan :

- 1) Pemrograman Dev- C++ dapat digunakan dalam membangun aplikasi enkripsi dan dekripsi.
- 2) Dalam pengujian program aplikasi pengetikan Deskripsi sudah dapat diterapkan dengan baik sesuai dengan algoritma yang digunakan.
- 3) Algoritma Vigénere Chiper lebih mudah dan sederhana dalam melakukan enkripsi dan dekripsi pesan teks, dengan cara menggunakan kombinasi kunci yang di inginkan.

DAFTAR PUSTAKA

- [1] Ariyus, Doni, 2006 Kriptografi Keamanan Data dan Komunikasi, Graha Ilmu Yogyakarta
- [2] Aidilof , Hafizh Al Kautsar. 2014. Sistem Pengenalan Ayat Al-Qur'an melalui Suara menggunakan Metode Support Vector Machine. Lhokseumawe : Skripsi.
- [3] Zuhra, Fatimah. 2015. Identifikasi Pola Iris Mata Menggunakan Discrete Fourier Transform (DFT) Untuk Pengamanan Sistem. Prodi Teknik Informatika Fakultas Teknik Universitas Malikussaleh. Reuleut-Aceh Utara
- [4] Binanto, Iwan, 2005, Konsep Bahasa Pemrograman, Andi Offset, Yogyakarta
- [5] Cahyadi, Tri, 2012, Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG, ISSN : 2302-9927, 282 Semarang No 4, diakses pada tanggal [23 Mei 2020 pukul 10:25 WIB](#).
- [6] Nurdin, Defry Hamdhana, M. Johan Setiawan, 2017. Sistem Pendeteksi Pola Lafadz Allah dan Muhammad pada Citra Al-Quran Menggunakan Metode Pierce, Jurnal TECHSI Vol. 9, No. 2, diakses pada tanggal [20 Mei 2020 pukul 09:11 WIB](#).