APLIKASI JAVA KRIPTOGRAFI MENGGUNAKAN ALGORITMA VIGENERE

Muhammad Fikry
Teknik Informatika, Universitas Malikussaleh
e-mail: muh.fikry@unimal.ac.id

Abstract

Data merupakan aset yang paling berharga untuk dapat menghasilkan informasi penting. Untuk menjaga keamanan data yang tersimpan, salah satu caranya dengan menggunakan metode kriptografi untuk menyembunyikan data asli tersebut sehingga tidak dapat dilihat oleh pihak yang tidak berhak. Salah satu bagian dari metode kriptografi adalah algoritma Vigenere yang termasuk dalam algoritma Simetrik dengan cara kerja enkripsi dilakukan secara mengalir menggunakan enkripsi dengan kunci yang mengalir juga. Algoritma Vigenere dianalisa dan disimulasikan kinerjanya pada *Personal Computer*, lalu dibangun aplikasi menggunakan pemrograman Java sebagai *user interface*.

Kata Kunci : Kriptografi, Algoritma, Vigenere, Java

PENDAHULUAN

Dunia teknologi informasi semakin berkembang dengan cepat dan pesatnya, bahkan ilmu pengetahuan tentang teknologi informasi mulai bermunculan. Hal ini membuat antara laju teknologi inforamsi terus beriringan dengan ilmu pengetahuan. Banyak informasi yang bermunculan, baik itu inforamsi yang layak dipublikasikan secara luas maupun yang bersifat pribadi dengan kata lain dirahasiakan. Dalam banyak kasus permasalahan, data dan informasi yang sangat rahasia dapat di ambil dan dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh sebab itu ilmu pengetahuan terkait keamanan data sangat penting.

Kriptografi merupakan ilmu yang menyandikan suatu data menjadi kode tertentu yang sulit dimengerti. Dengan menggunakan kriptografi data asli yang dikirim (plaintext) diubah ke dalam bentuk data tersandi (ciphertext), kemudian data tersandi tersebut hanya dapat dikembalikan ke bentuk data

sebenarnya hanya dengan menggunakan kunci (key) tertentu yang hanya dimiliki oleh pihak yang berhak menerimanya.Saat ini banyak bermunculan algoritma kriptografi yang terus dianalisis, dicoba dan disempurnakan untuk mencari algoritma yang dianggap memenuhi standar keamanan. Salah satunya adalah algoritma Vigenere yang mungkin dapat dijadikan pertimbangan dalam penggunaan dan perkembangan algoritma-algoritma dalam metode kriptografi.

TINJAUAN PUSTAKA

Menurut kamus besar bahasa indonesia aplikasi berasal dari kata *application* yang artinya penerapan; lamaran; penggunaan. Aplikasi sering juga disebut program aplikasi adalah program yang dibuat oleh pemakai yang ditujukan hanya untuk melakukan suatu tugas khusus (Kadir, 2003). Jadi, dapat disimpulkan bahwa aplikasi merupakan program siap pakai yang dibuat untuk melaksanakan suatu fungsi bagi pengguna agar tercapai sasaran yang dituju.

Kriptografi atau kriptologi berasal dari bahasa Yunani yaitu kryptós yang berarti tersembunyi atau rahasia dan graphein yang berarti menulis atau ilmu. Kriptografi adalah suatu metode yang sering sekali digunakan untuk melindungi berbagai macam data yang prosesnya disebut dengan *encryption*, yaitu adalah suatu proses yang mengkonversi sebuah pesan plaintext menjadi sebuah ciphertext yang bisa dibalik ke bentuk asli seperti semula, yang juga bisa disebut sebagai proses *decoding* atau *decryption* (Ariyus, 2008). Teknik yang digunakan dalam kriptografi adalah mengubah data menjadi berbeda dari aslinya menggunakan algoritma matematika dengan tujuan kerahasian, intergritas data, autentikasi dan non-repudiasi. Prosedur-prosedur kriptografi juga bisa digunakan untuk authentifikasi pesan, digital signature, dan identifikasi pribadi untuk mengotorisasi data melalui suatu jaringan.

Ada beberapa istilah-istilah yang penting dalam kriptografi, yaitu :

1. Plaintext (Cleartext)

   suatu data yang tidak disandikan.
2. Ciphertext

   suatu data yang telah disandikan.
3. Key

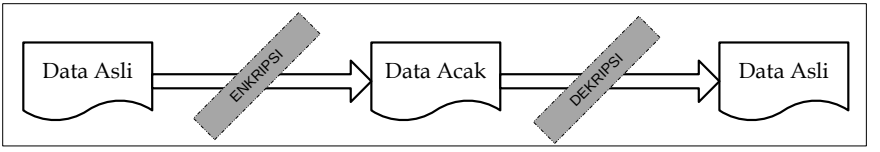
   Parameter yang digunakan untuk transformasi enkripsi dan dekripsi. *Key* biasanya berupa string atau deretan bilangan.
4. Enkripsi

Proses yang dilakukan untuk mengubah plaintext menjadi ciphertext.

5. Dekripsi

   Proses untuk mengubah ciphertext kembali ke plaintext.

Secara sederhana proses kerja dari istilah-istilah diatas dapat digambarkan sebagai berikut :



Gambar 1. Proses Enkripsi dan Dekripsi Sederhana

Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua jenis yaitu :

1. Algoritma Simetrik

   Pada algoritma ini kunci dekripsi dapat ditentukan dari kunci enkripsinya, begitu pula sebaliknya, oleh sebab itu keamanan kriptografi simetri terletak pada kerahasiaan kuncinya. Algoritma kriptografi simetri dikelompokkan menjadi dua kategori, yaitu (Lung dan Munir, 2005):

   a) Cipher aliran (stream cipher)

      Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal, yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit.

   b) Cipher blok (block cipher)

      Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya.

2. Algoritma Asimetrik

   Pada algoritma ini kunci yang digunakan untuk proses dekripsi berbeda dengan kunci proses enkripsi. Kunci untuk enkripsi dibuat umum, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan. Jadi hanya orang tertentu saja yang berhak terhadap kunci dekripsi, walaupun kunci enkripsi dapat diketahui dan digunakan oleh orang lain.

Algortima Vigenere menggunakan kunci sama untuk proses enkripsi dan dekripsi yang mengatur substitusi berdasarkan dari kata kunci yang digunakan.

Data yang pada plainteks akan di penggal menghasilkan bit-bit tunggal, lalu di subsitusi menggunakan kunci yang ditetapkan untuk mendapatkan rangkaian bit per bit baru.

Ilmu Matematika mengambil peranan penting dalam keilmuan kriptografi. Operasi matematika yang banyak diimplementasikan dalam metoda kriptografi adalah aritmatika modular operasi XOR dan operasi AND. Kedua operasi tersebut melibatkan bilangan 0 dan 1.

Tabel 1. Operasi XOR

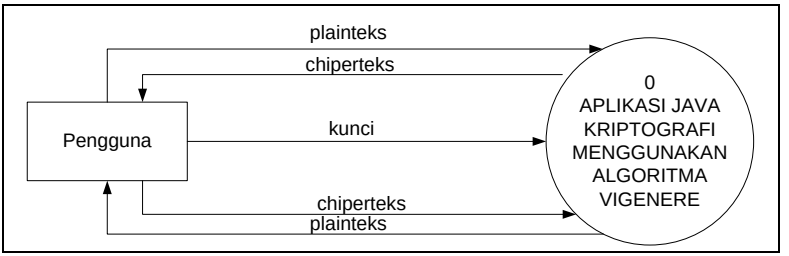
A	B	XOR
0	0	0
0	1	0
1	0	0
1	1	1

Tabel 2. Operasi AND

A	B	AND
0	0	0
0	1	0
1	0	0
1	1	1

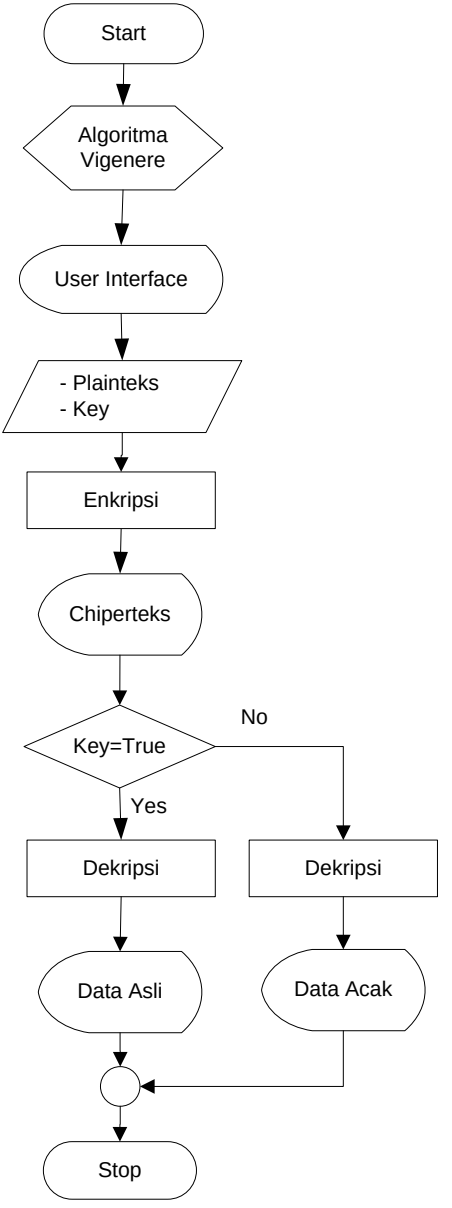
METODE PENELITIAN

Pada metode penelitian akan dijelaskan mengenai langkah-langkah dalam menyelesaikan permasalahan yang dibahas, agar dapat berjalan dengan baik. Langkah-langkah penyelesaian masalah tersebut akan digambarkan dengan rancangan logika menggunakan Data Flow Diagram (DFD). Dengan menggunakan Data Flow Diagram memudahkan pemakai yang kurang menguasai bidang komputer untuk mengerti sistem yang akan dikerjakan. Rancangan proses menggunakan bentuk Data Flow Diagram dapat dilihat pada gambar berikut ini:



Gambar 2. Data Flow Diagram

Untuk rancangan program yang dibuat dengan pemrograman Java, gambar 3 memperlihatkan secara rinci langkah-langkah dari proses program bekerja dalam mengubah plainteks menjadi chiperteks menggunakan algoritma vigenere. Alat bantu yang digunakan untuk menerangkan logika program ini adalah *flowchart*.



Gambar 3. Flowchart

HASIL DAN PEMBAHASAN

Pada pembahasan ini, dijelaskan mengenai cara kerja algoritma Vigenere pada pemrograman Java.

Diberikan : plainteks $x_1, x_2, x_3, \ldots, x_n$ dengan $x_i \in Z_{26}$

kunci $k_1, k_2, k_3, \ldots, k_n$ dengan $k_i \in Z_{26}$

Cipherteks $y_1, y_2, y_3, \ldots, y_n$ diperoleh dengan proses enkripsi sebagai berikut :

$$y_i = x_i + k_i,\ y_{n+1} = x_{n+1} + k_{n+1} \pmod{26}$$

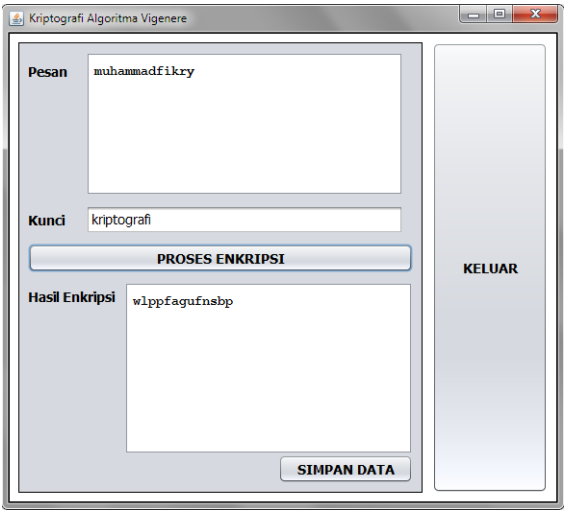
Dapat dilihat bahwa proses enkripsi berlangsung secara mengalir. Diberikan korespondensi huruf abjad dengan bilangan sebagai berikut, a dengan 0, b dengan 1, c dengan 2, dan seterusnya sampai z dengan 25.

Sebagai contoh, misalkan dipunyai pesan "**muhammadfikry**" dan kunci rahasia "**kriptografi**". Proses enkripsi diberikan dalam tabel di bawah ini.

Tabel 2. Proses Enkripsi

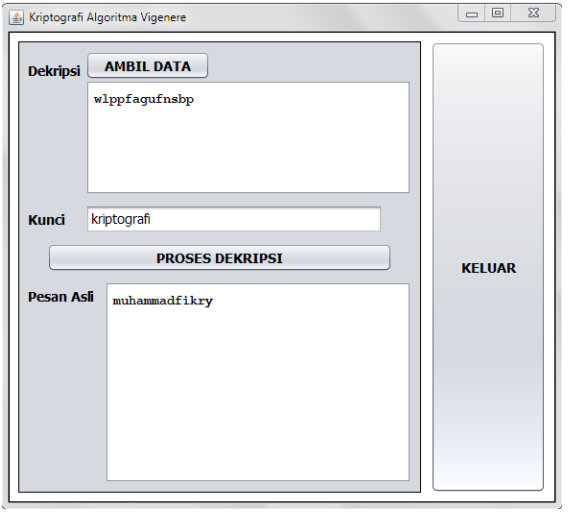
Huruf	xi	Kunci	ki	yi = xi + ki (mod 26)	Huruf
m	12	k	10	22	w
u	20	r	17	11	l
h	7	i	8	15	p
a	0	p	15	15	p
m	12	t	19	5	f
m	12	o	14	0	a
a	0	g	6	6	g
d	3	r	17	20	u
f	5	a	0	5	f
i	8	f	5	13	n
k	10	i	8	18	s
r	17	k	10	1	b
y	24	r	17	15	p

Pada program, pengirim harus melakukan *input* di *form* enkripsi. Pada *form* tersebut langkah-langkah yang dilakukan pengirim adalah memasukkan data dan kata kunci, lalu melakukan proses enkripsi dan penyimpanan data. Tampilan untuk form enkripsi dapat dilihat pada gambar 4.



Gambar 4. Form Enkripsi

Sedangkan pada sisi penerima bekerja di *form* dekripsi. Pada *form* tersebut langkah-langkah yang dilakukan penerima adalah mengambil data yang tersimpan atau memasukkan data tersebut secara manual, memasukkan kunci yang diberikan oleh pengirim, lalu melakukan proses dekripsi. Tampilan untuk form dekripsi dapat dilihat pada gambar 5.



Gambar 5. Form Dekripsi

KESIMPULAN

Berdasarkan proses yang dilakukan dalam membangun Aplikasi Java Kriptografi menggunakan Algoritma Vigenere ini dapat ditarik kesimpulan sebagai berikut:

1. Aplikasi yang telah dibangun menggunakan pemrograman Java ini telah dapat berfungsi sesuai tujuan, yaitu mengamankan data ataupun informasi dan mengembalikan data ataupun informasi tersebut hanya untuk pihak yang berhak.
2. Proses enkripsi dan dekripsi memerlukan waktu yang sama untuk data dan metoda yang sama.
3. Semakin kompleks metode pengacakan yang digunakan maka semakin sulit untuk membongkar pesan yang terenkripsi ke dalam bentuk aslinya.

REFERENSI

Ariyus, Doni. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Andi Offset. Yogyakarta.

Kadir, Abdul. 2003. *Pengenalan Sistem Informasi*. Andi. Yogyakarta.

Wahana. 2003. *Memahami Model Enkripsi dan Security Data*. Andi Offset. Yogyakarta.