PENGAMANAN DATA MENGGUNAKAN ALGORITMA VIGENERE DENGAN TABEL DINAMIS BERBASIS ANDROID

Wahyu Farabi Firmansah[1)], Ari Eko Wardoyo S. T, M. Kom[2)],
Mudafiq R. Pratama S. Kom[3)]

Program Studi Teknik Informatika – S1 Fakultas Teknik
Universitas Muhammadiyah Jember

ABSTRAK

Berkembangnya jaringan komunikasi sangat bermanfaat untuk pertukaran berbagai informasi, baik dalam bentuk teks, gambar, audio ataupun video. Seiring berkembangnya jaringan komunikasi, semakin berkembang pula kejahatan yang membuat khawatir dengan keamanan data yang akan dikirim, sehingga perlu keamanan dari pesan yang akan dikirim agar tidak bisa dilihat oleh orang yang tidak bertanggung jawab. Pengamanan data bisa dilakukan dengan menggunakan kriptografi, salah satu metode kriptografi adalah algoritma vigenere cipher. Semakin berkembangnya zaman banyak metode untuk memecahkan algoritma vigenere cipher, dan tujuan pembuatan penelitian ini untuk membuat algoritma vigenre cipher tidak mudah dipecahkan dengan cara membuat tabel dinamis, yaitu mengubah urutan tabel sesuai dengan kata kunci yang di inputkan. Metode vigenere tabel dinamis berhasil untuk enkripsi dan deskripsi hampir semua karakter dengan akurasi 99,99% tetapi gagal dalam enkripsi maupun dekripsi karakter ENTER.

Kata Kunci : Informasi, Kata Kunci, Kriptografi, Tabel Dinamis, Vigenere Cipher

ABSTRACT

The development of the communication network is very useful for the exchange of information, whether in the form of text, images, audio or video. As the development of communication networks, growing crime also makes concerned about the security of data do be sent, so it needs the security of a message to be sent so as not to be seen by people who ari not responsible. Data security can be done by using cryptography, one of the methods of cryptography is vigenere cipher algorithm. The continued development of methods to solven many times vigenere cipher algorithm, and goals of this research to create vigenre cipher algorithms are not easily solved by creating a dynamic table, changing the order of the Table according to the keyword fed. Vigenere method tables dynamically managed for The encryption and description of almost all the characters with an accuracy of 99.99% but failed in the encryption and decryption code ENTER.

Keywords: *Information, Keywords, Cryptography, Dynamic Table, Vigenere Cipher*

PENDAHULUAN

Latar Belakang

Berkembangnya jaringan komunikasi sangat bermanfaat untuk pertukaran berbagai informasi, baik dalam bentuk teks, gambar, audio ataupun video. Seiring berkembangnya jaringan komunikasi, semakin berkembang pula kejahatan yang membuat khawatir dengan keamanan data yang akan dikirim, sehingga perlu keamanan dari pesan yang akan dikirim agar tidak bisa dilihat oleh orang yang tidak bertanggung jawab.

Pengamanan data bisa dilakukan dengan menggunakan kriptografi, dimana kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita (Scheiner, B.,1996). Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integrasi data, serta autentifikasi (Meneres et al,1996).

Semakin berkembangnya zaman banyak metode untuk memecahkan kriptografi sehingga penulis ingin membuat hal yang baru agar pertukaran data lebih aman, dimana penulis ingin memodifikasi hal yang sudah ada seperti algoritma vigenere cipher. Modifikasi yang dilakukan adalah membuat tabel dinamis di kriptografi vigenere cipher, tabel yang akan berubah sesuai kata kunci yang di masukan. Sehingga Dari permasalahan tersebut maka penulis dapat mengambil

judul **“Pengamanan Data Menggunakan Algoritma Vigenere Dengan Tabel Dinamis Berbasis Android”**

Rumusan masalah

Berdasarkan latar belakang masalah di atas, rumusan masalahnya adalah :

1. Bagaimana memodifkasi tabel vigenere cipher sehingga berubah sesuai kata kunci.
2. Bagaimana memperkuat algoritma vigenere cipher sehingga tidak mudah dipecahkan.

Batasan Masalah

Adapun batasan masalah adalah :

1. Enkripsi menggunakan algoritma kriptografi *vigenere cipher*
2. Data yang bisa di enkripsi berupa huruf A sampai Z
3. Data yang bisa di enkripsi berupa huruf a sampai z
4. Data yang bisa di enkripsi berupa angka 0 sampai 9
5. Data yang bisa di enkripsi berupa beberapa simbol yaitu : / ? ! . - , @ # * ( ) : & $ % + ; = _ [ ] { } ^ ~ ‘ ` |
6. Data yang tidak bisa di enkripsi yaitu : Enter
7. Data yang bisa di enkripsi berupa file .txt

Tujuan Penulisan

Adapun tujuan dari penulisan ini adalah :

1. Untuk memodifikasi tabel vigenere cipher sehingga berubah sesuai dengan kata kunci.
2. Untuk membuat algoritma vigenere cipher tidak mudah untuk dipecahkan.

Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Membuat algoritma vigenere cipher tidak mudah dipecahkan.
2. Membuat data terjaga kerahasiannya.

METODE PENELITIAN

Kriptografi

Menurut Dony Ariyus (2006) dalam bukunya “Kriptografi Keamanan Data Dan Komunikasi”, kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu cryptos artinya rahasia (secret) dan graphein artinya tulisan (*writing*). Jadi kriptografi berarti tulisan rahasia (*secret writing*). Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai arti atau nilai, dengan cara mengacak menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu. Menurut Bruce Scheiner kriptografi adalah ilmu pengetahuan dan seni menjaga pesan – pesan agar tetap aman

(*secure*)(Scheiner, B.,1996). Sedangkan menurut Menezer kriptografi adalah ilmu yang mempelajari teknik teknik matematik yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi (Meneres et al,1996). Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

1. *Plaintext* (M) adalah pesan asli yang hendak dikirimkan (berisi data asli).
2. *Ciphertext* (C) adalah pesan bersandi yang merupakan hasil enkripsi.
3. Enkripsi (fungsi E) adalah proses pengubahan *plaintex*t menjadi *ciphertext*.
4. Dekripsi (fungsi D) adalah kebalikan dari skripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
5. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Vigenere Cipher

Vigenere Cipher termasuk dalam *cipher* abjad majemuk (*polyalphabetic substitution Cipher*) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, *Blaise de Vigenere* pada abad 16 (tahun 1586). Vigenere Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci.

Tabel dinamis

Tabel dinamis adalah tabel yang urutannya akan berubah ubah sesuai dengan kunci yang dimasukkan. Pada vigenere cipher di gunakan tabel berupa huruf berurutan a,b,c...z sehingga seandainya kuncinya diketahui oleh pihak yang tidak bertanggung jawab mudah untuk memecahkannya karena tabel yang berupa huruf yang berurutan. Oleh karena itu digunakanlah tabel dinamis, seandainya kuncinya diketahui oleh orang yang tidak bertanggung jawab pun akan sulit memecahkannya karena tabel yang digunakan tidak berurutan contoh :

Tabel 4.1 Tabel awal

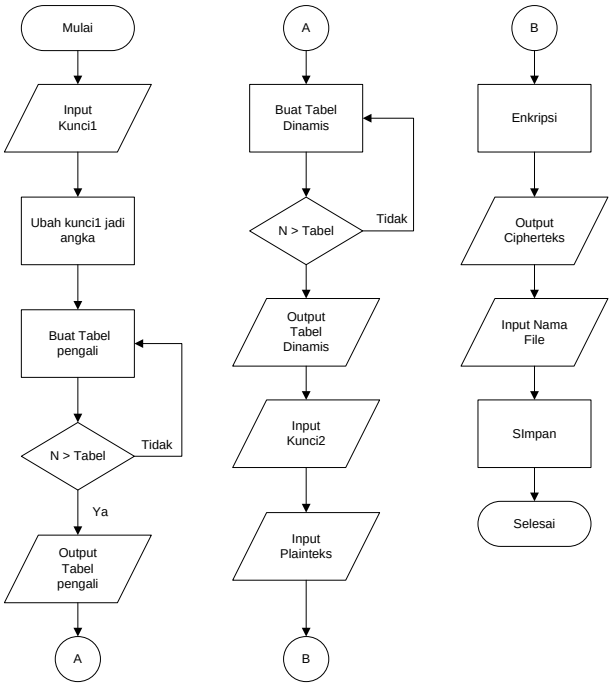
A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	1	2	3	4
5	6	7	8	9	0	SPASI	/	?	!

Tabel dinamis dengan menggunakan kunci : BOM

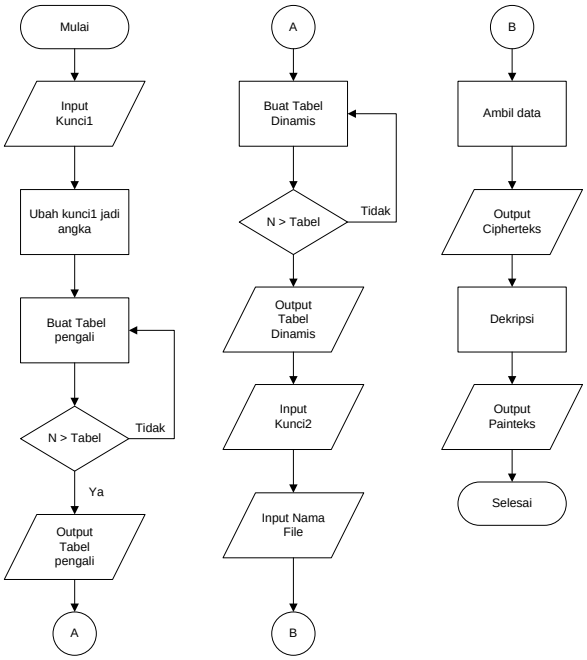
Tabel 4.2 Tabel dinamis kunci : BOM

A	Q	T	W	I	R	G	9	Z	M
!	1	N	J	P	S	V	F	O	C
U	SPASI	K	5	3	/	6	2	Y	7
X	L	8	4	0	?	B	E	H	D

Flowchart



Gambar 3.2 Flowchat enkripsi



Gambar 3.3 Flowchat deskripsi

Pengujian

Pengujian akan dilakukan dengan dua cara yaitu :

1. Pengujian dengan mengenkripsi dan mendekripsi data.
2. Pengujian dengan menggunakan metode kasiski\

Hasil Pengujian Didapat :

Pada proses pengujian enkripsi dan dekripsi untuk huruf besar algoritma vigenere tabel dinamis berhasil dalam enkripsi maupun dekripsi dengan akurasi 99,99% dan dapat dilihat pada lampiran.

Pada proses pengujian enkripsi dan dekripsi untuk huruf kecil algoritma vigenere tabel dinamis berhasil dalam enkripsi maupun dekripsi dengan akurasi 99,99% dan dapat dilihat pada lampiran.

Pada proses pengujian enkripsi dan dekripsi untuk angka algoritma vigenere tabel dinamis berhasil dalam enkripsi maupun dekripsi dengan akurasi 99,99% dan dapat dilihat pada lampiran.

Pada proses pengujian enkripsi dan dekripsi untuk simbol algoritma vigenere tabel dinamis berhasil dalam enkripsi maupun dekripsi dengan akurasi 99,99% dan dapat dilihat pada lampiran.

Pada proses pengujian enkripsi dan dekripsi untuk kalimat algoritma vigenere tabel dinamis berhasil dalam enkripsi maupun dekripsi dengan akurasi 99,99% tetapi apabila dalam kalimat terdapat karakter ENTER maka algoritma vigenere tabel dinamis akan terjadi kegagalan dalam proses enkripsi maupun dekripsi dan dapat dilihat pada lampiran.

Jadi kesimpulan dalam pengujian algoritma vigenere tabel dinamis didapat bahwa algoritma vigenere tabel dinamis berhasil dalam enkripsi dan dekripsi untuk hampir semua karakter dengan akurasi 99,99% tetapi gagal dalam enkripsi maupun dekripsi karakter ENTER.

Keseimpulan

1. Metode vigenere tabel dinamis berhasil untuk enkripsi dan deskripsi hampir semua karakter dengan akurasi 99,99% tetapi gagal dalam enkripsi maupun dekripsi karakter ENTER.
2. Dari hasil uji terhadap algoritma kasiski, metode ini tidak dapat dipecahkan.
3. Metode vigenere tabel dinamis berhasil dengan panjang karakter yang tidak terbatas kecuali adanya karakter ENTER.

Saran

1. Dari pengujian terhadap karakter ENTER metode vigenere chiper tabel dinamis mengalami kegagalan pada saat enkripsi maupun deskripsi. Harapannya kelemahan metode ini bisa di kembangkan pada penelitian berikutnya.
2. Harapannya kedepannya aplikasi ini bisa di jalankan di OS yang lain selain Android.

Daftar Pustaka

A. Menezes, P. van Oorschot and S. Vanstone.1996. *Handbook of Applied Cryptography.*

Ariyus,Dony. 2006. Kriptografi Keamanan Data Dan Komunikasi

Schneier, Bruce. 1996.*Applied Cryptography*

Supardi, Yuniar. 2011. Semua Bisa Menjadi Programmer Android bisa. Jakarta : PT Elex Media Kamputindo

Yakub, Putu H. Arjana, Tri Puji Rahayu dan Hariyanto. 2012. Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper. Tangerang: Seminar Nasional Teknologi Informasi dan Komunikasi 2012.