P-ISSN :2548-5997 E-ISSN : 2685-1768

MODIFIKASI ALGORITMA *VIGENERE CIPHER* UNTUK PENGAMANAN PESAN RAHASIA

Jesmon Simangunsong[1] Zekson Arizona Marondang[2]
STMIK Kristen Neumann Indonesia Jl. Letjen Jamin Ginting KM. 10,5 Medan
simangunsongjesmon12@gmail.com[1] zekson.arizona@yahoo.com[2]

Program Studi Teknik Informatika

ABSTRACT

The confidentiality of messages or data owned by someone is important in sending messages so that the message can only be given by certain people who can access the information. Cryptography is the study of how to safeguard data or messages with the aim of preventing others from wanting to know their contents, by using certain codes and rules and other methods so that only authorized people can find out the true contents of the message. In the Vigenere Cipher algorithm the message security uses only a single key and the alphabet as an encoding key to replace or substitution the character of the message which makes the strength in the message transmission limited only to the use of the alphabet. In this research, the Vegenere Cipher algorithm was modified with 3 keys used and the vegenere cipher table modified by adding numbers and 10 symbols so that the characters of the table are 46 characters from the previous 26 characters. The results of this algorithm are able to encrypt secret messages and decrypt them back into their original messages.

Keywords: Secret Message Security, Cryptography, Vegenere Cipher algorithm

1. PENDAHULUAN

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi kalau data tersebut berada dalam suatu jaringan komputer yang terkoneksi dengan jaringan publik misalnya internet. Tentu saja data yang sangat penting tersebut tidak boleh dilihat atau dibajak oleh orang yang tidak berwenang. Sebab kalau hal ini sampai terjadi kemungkinan data kita akan rusak bahkan bisa hilang yang akan menimbulkan kerugian material yang besar.

Pemakaian teknologi komputer sebagai salah satu aplikasi dari teknologi informasi dan pengelolaan data sudah menjadi suatu kebutuhan saat ini, karena banyak pekerjaan yang dapat diselesaikan dengan cepat, akurat dan efisien. Dengan demikian perlu diterapkan prosedur keamanan pada sebuah informasi yang ingin dikirimkan. Seiring perkembangan teknologi informasi, sistem pengaman informasi juga semakin ditingkatkan. Muncul berbagai cara untuk mengatasi persoalan keamanan data yang pada intinya adalah bagaimana agar orang yang tidak berhak, tidak dapat membaca, merubah atau bahkan merusak data yang bukan miliknya atau ditujukan kepadanya disebut dengan istilah kriptografi**.** Tentu hal ini akan sangat bermanfaat untuk menjaga kerahasiaan data atau informasi tertentu.

Pada penelitian Nurnawati, E. K. (2008) yang berjudul Analisis Kriptografi Menggunakan Algoritma *Vigenere cipher* Dengan Mode Operasi *Cipher Block Chaining* (CBC), dilakukan penggabungan kriptografi algoritma *Vigenere cipher* dengan mengadopsi cara kerja mode operasi *Cipher Block Chaining* (CBC). Hasil percobaan adalah pada saat proses enkripsi dan dekripsi dibutuhkan memori yang sangat besar yang mengakibatkan proses menjadi lama. Untuk itu penulis membatasi

panjang kunci sampai dengan 10 karakter. Algoritma *Vigenere cipher* asli hanya menampung 26 huruf alfabeth dalam bentuk huruf kecil sedangkan tanda baca lain tidak dapat terbaca. Sehingga perlu dilakukan suatu pengevaluasian yaitu dengan memperluas jangkauan 26 huruf alfabeth tersebut menjadi 256 karakter ASCII.

Caesar cipher dan *Vigenere cipher* merupakan contoh metode kriptografi dengan model pengamanannya penggantian karakter atau subtitusi (*substitution*). Metode *Caesar Cipher* menggunakan kunci berupa angka sebagai nilai untuk mengganti karakter pesan dengan karakter yang lain. Hal yang berbeda pada *Vigenere cipher* karena hanya menggunakan abjad sebagai kunci penyandian untuk melakukan penggantian atau subtitusi karakter pesan yang membuat kekuatan dalam penyadian pesan hanya terbatas pada penggunaan abjad saja. Melihat keterbatasan ini, penulis memutuskan untuk membahas teknik kriptografi yang sudah ada ini untuk dikembangkan dengan tujuan menambah keleluasaan dan kekuatan dalam pengamanan informasi, dengan harapan bisa digunakan suatu saat baik untuk penulis sendiri maupun untuk orang lain.

1.1 Rumusan Masalah

Dalam sebuah penelitian, pada dasarnya membutuhkan perumusan masalah untuk memberikan gambaran mengenai masalah yang akan diteliti. Sebelum membahas tentang masalah yang akan diteliti, alangkah baiknya apabila penulis memberikan pemaparan tentang topik utama permasalahan yang menjadi fokus dalam penulisan proposal ini. Adapun topik utama permasalahan yang muncul adalah sebagai berikut :

a. Bagaimana cara membangun suatu aplikasi untuk melindungi data atau informasi dari pihak pihak yang tidak berhak sehingga tidak bisa diketahui, dimodifikasi maupun dirusak ?
b. Bagaimana cara untuk memodifikasi teknik pengaman data (kriptografi) yang sudah ada (algoritma *vigenere cipher*) dengan tujuan untuk menambah kekuatan dalam pengaman data atau informasi ?

1.2 Batasan Masalah

Dalam sebuah sistematika penelitian, pada umumnya ada batasan batasan masalah yang akan dibahas agar pembahasan materinya lebih terarah dan sistematis. Maka dari itu, dalam proposal ini pun penulis mencantumkan hal hal yang akan menjadi ruang lingkup pembahasan materi proposal sebagai berikut :

a. Adapun fokus utama dalam penelitian ini adalah metode pengamanan data yakni kriptografi dan difokuskan lagi hanya pada Algoritma *Vigenere cipher*.
b. Bahasa Pemprograman yang digunakan adalah bahasa pemprograman basic
c. Hasil aplikasi yang dibangun hanya membaca file yang ber-extensi .txt.
d. Informasi yang sudah dienkripsi akan tersimpan dalam bentuk file baru.

Adapun tujuan dari penulisan Penelitian ini adalah :

1. Untuk membangun suatu aplikasi yang berfungsi untuk melindungi suatu data atau informasi
2. Untuk memodifikasi teknik pengamanan data yang sudah ada agar sistem pengamanan yang dibuat lebih baik

Adapun manfaat dari penelitian ini adalah sebagai berikut :

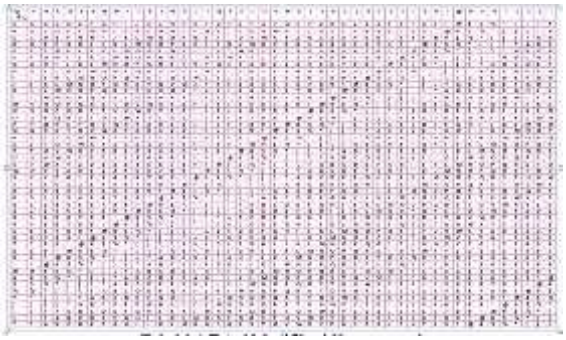
1. Aplikasi yang dibangun dapat digunakan sebagai aplikasi pengamanan data atau informasi baik untuk penulis sendiri maupun orang lain.
2. Dengan adanya penelitian ini diharapkan bagi yang ingin menggunakan aplikasi yang dibuat dapat bermanfaat untuk myang ber-ektensi .txt.

2 TINJAUAN PUSTAKA

Pada penelitian ini penulis melakukan modifikasi algoritma *Vigenere cipher* untuk pengamanan pesan rahasia berupa teks.

Modifikasi dilakukan pada penambahan karakter pada tabel Vigenere serta penggunaan 3 buah kunci. Pada pengembangan penambahan karakter yaitu penambahan angka dan simbol, dengan demikian maka ukuran tabel yang digunakan untuk melakukan enkripsi dan dekripsi menjadi lebih besar menjadi 46 karakter. Adapun tabel modifikasi *Vigenere cipher* dapat dilihat seperti pada

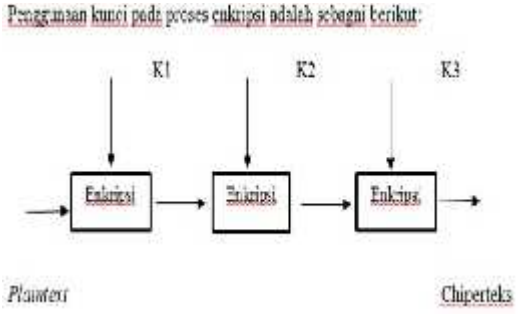
Tabel 1 Tabel Modifikasi *Vigenere cipher*



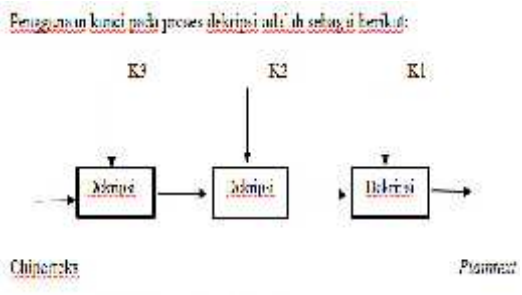
Dalam modifikasi algoritma Vigenère Cipher ini, dilakukan penambahan karakter angka dan simbol, sehingga *Plaintext* yang bisa dienkripsi tidak hanya sebatas alfabet saja, melainkan juga angka dan simbol.

Dan dengan dibuatkannya 3 buah kunci maka kelemahan penggunaan kunci pada algoritma *Vigenere cipher* dapat teratasi. Dalam penelitian ini, penulis mencoba membuat lapisan kunci sebanyak 3 lapis.

Dengan dibuatkannya 3 buah kunci maka kelemahan penggunaan kunci pada algoritma *Vigenere cipher* dapat teratasi. Dalam penelitian ini, penulis mencoba membuat lapisan kunci sebanyak 3 lapis yang dapat dilihat pada Gambar 1 dan 2.



Gambar 1. Enkripsi dengan kunci 3 lapis



Gambar 2. Deskripsi dengan kunci 3 lapis

3. ANALISA DAN PERANCANGAN

Pada pengujian perangkat lunak kriptografi Algoritma Vigenere Cipher dilakukan dengan pemasukan plainteks serta kunci serta Load Plainteks yang menghasilkan cipherteks.

3 Enkripsi dan Dekripsi Dengan Input Plainteks

Pengujian enkripsi dengan input plainteks dilakukan cara pemasukan plainteks melalui keybord dengan jumlah huruf 13, 24, 53, 65, serta 89 dengan kunci1= a, kunci2=b dan kunci3=c. Hasil enkripsi Algoritma Vigenere Cipher dengan input teks dapat dilihat pada Tabel 2.

Tabel 2. Hasil Pengujian Enkripsi Algoritma Vigenere Cipher Input Plainteks

Tabel 3 Hasil Pengujian Dekripsi Algoritma Vigenere Cipher Input Plainteks

No	Ciphertext	Plaintext	Hasil
1	VWPLNQIIXPDQQ	STMIK NEUMANN	SUKSES
2	VWPLNQHXPDQQPHCIDQ334@	STMIK NEUMANN MEDAN 2018	SUKSES
3	VWPLNQHXPDQQPHCIDQ334@SHIDQ JNDWQ XQDNNULSWRJUDIL	STMIK NEUMANN MEDAN 2018 PERANGKAT LUNAK KRIPTOGRAFI	SUKSES
4	VWPLNQIIXPDQQPIGDQL!!@SIIUDQJ	STMIK	SUKSES

4. HASIL DAN PEMBAHASAN

Setelah melakukan perancangan perangkat lunak kriptografi modifikasi Algoritma *Vigenere Cipher* untuk pengamanan pesan rahasia, maka tahap selanjutnya adalah penulisan kode program (*coding*). Perangkat lunak yang akan di-*coding* adalah berupa menu utama serta program Kriptografi algoritma *Vigenere Cipher*, program Bantuan serta Keterangan.

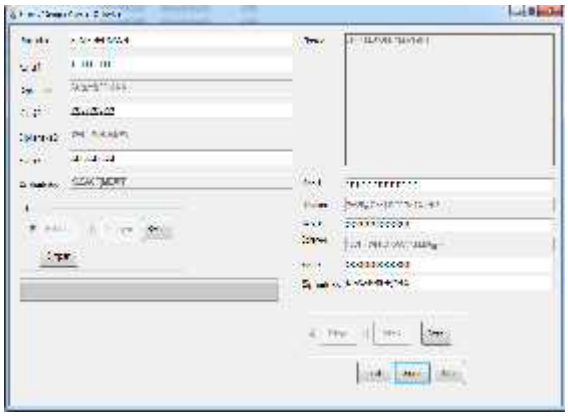
3.1 Tampilan Interface "Menu Utama"

Tampilan Menu Utama adalah berfungsi untuk menampilkan menu-menu aplikasi. Pada rancangan ini terdapat judul aplikasi, gambar latar serta sub menu antara lain Kriptografi *Vigenere Cipher*, *Bantuan*, *Keterangan* serta *Tutup*. Tampilan Menu Utama terlihat seperti pada Gambar 3.

Gambar 3. Menu Utama

3.2 Tampilan Interface "Vigenere Cipher" Aplikasi

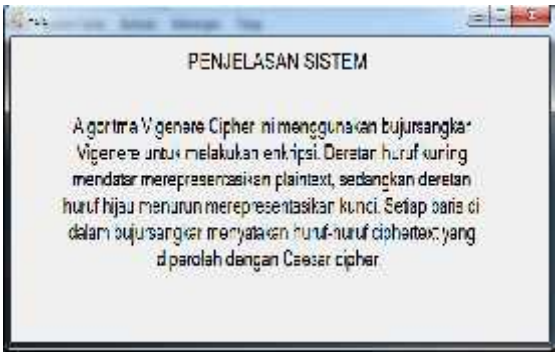
Tampilan Kriptografi Vigenere Cipher berfungsi untuk melakukan enkripsi dan dekripsi dengan algoritma *Vigenere Cipher*. Tampilan Kriptografi Vigenere Cipher dapat dilihat seperti pada Gambar 4.



Gambar. 4. Tampilan Kriptografi Vigenere Cipher

4.3 Tampilan Bantuan

Tampilan Bantuan adalah tampilan berfungsi untuk menampilkan informasi bantuan pengoperasian aplikasi Kriptografi Vigenere Cipher. Untuk lebih jelasnya rancangan Bantuan dapat dilihat pada Gambar 5.



Gambar 5. Tampilan Bantuan

4.4 Tampilan Keterangan

Tampilan Keterangan berfungsi untuk menampilkan informasi tentang profil penulis. Profil penulis meliputi biodata singkat penulis serta data-data akademik berupa nama mahasiswa, Nomor Induk Mahasiswa, Nama Perguruan Tinggi tempat

mahasiswa, serta gambar latar belakang seperti yang dapat dilihat pada Gambar 6.

Gambar 6. Tampilan Keterangan

5. KESIMPULAN

Setelah melakukan implementasi perangkat lunak kriptografi modifikasi Algoritma *Vigenere Cipher* untuk pengamanan pesan rahasia, maka dapat disimpulkan:

1. Perangkat lunak Kriptografi Modifikasi Algoritma *Vigenere Cipher* untuk Pengamanan Pesan Rahasia dapat melakukan enkripsi dan dekripsi teks serta file teks.
2. Perangkat lunak Kriptografi Modifikasi Algoritma *Vigenere Cipher* untuk Pengamanan Pesan Rahasia dapat menggunakan kunci berlapis 3 dan menginput 46 karakter yg ada pada table untuk melakukan enkripsi dan dekripsi teks serta file teks.
3. Hasil pengujian pengujian enkripsi dan dekripsi pesan rahasia dengan sampel pesan rahasia berhasil dengan tingkat keberhasilan 100 %.

DAFTAR PUSTAKA

[1] Amalarethinam, D.I.G dan Greetha, J. S, 2005. Aspek Keamanan Dari Suatu Informasi.

[2] Arjana, P. H., Rahayu,T. P., Yakub & Hariyanto. 2012. Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper. Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012) Yogyakarta, 10 Maret 2012. Program Studi Teknik Informatika, STMIK Dharma Putra Tangerang.

[3] Arjana, 2012 Implementasi Enkripsi Data Dengan Algoritma *Vigenere Cipher*“

[4] Andhika, F. R. 2011, *Modifikasi Vigenere Cipherdengan Menggunakan Caesar Chiper dan Enkripsi berlanjut untuk pembentukan keynya*, Institut Teknologi Bandung.

[5] Dony Ariyus, 2008, *Pengantar Ilmu Kriptografi, Teori, Analisis dan Implementasi*, Andi Offset, Yogyakarta.

[6] Efrandi, 2014, Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher”.

[7] Nurwanti, E. K, 2008, Analisis Kriptografi Menggunakan Agoritma Vigenere Cipher Dengan Metode Operasi Cipher Block Chaining (CBC).

[8] Religia, 2015 , *Implementasi Algotitma Affine Cipher dan Vigenere Cipher ntuk Keamanan Login.*

[9] Rinaldi Munir, 2006, *Kriptografi Informatika*, Jakarta

[10] Soesilo Wijono, dkk. 2007, *Pemprograman GUI Swing Java*, Andi Offset, Yogyakarta.