KOMBINASI VIGENERE CIPHER DAN PERMUTASI CIPHER DENGAN MODIFIKASI KEY DINAMIS PADA KRIPTOGRAFI BERBASIS TEKS

[1] Erfan Bahtiar (1110651009), [2] Agung Nilogiri, S.T, M.Kom
Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember
Email : superbachtiar@gmail.com

ABSTRAK

Menjaga kerahasiaan suatu pesan teks menjadi sangat diperlukan untuk mengantisipasi terjadinya penyadapan informasi. Vigenere cipher merupakan salah satu jenis algoritma klasik yang populer dan sering digunakan sebagai metode penyembunyian pesan (kriptografi). Cara kerja vigenere cipher adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya. Kelemahan vigenere cipher yaitu diulangnya key yang sama terus menerus sehingga menimbulkan cipherteks yang sama untuk potongan plainteks yang mana posisinya merupakan kelipatan dari panjang key sehingga plainteks tersebut akan selalu mendapatkan potongan key yang sama untuk enkripsinya dan hasil yang sama pula untuk dekripsinya. Namun untuk meminimalisir kelemahan tersebut dapat dilakukan beberapa modifikasi pada vigener cipher itu sendiri, salah satunya adalah menggabungkan vigenere cipher dan permutasi cipher dengan memodifikasi *key*-nya menjadi dinamis.

Kata kunci : *Vigenere cipher, kriptografi, enkripsi, dekripsi, plainteks, cipherteks, key, permutasi cipher.*

I. Pendahuluan

Dengan semakin pesatnya perkembangan ilmu pengetahuan dan teknologi, sistem multiuser sudah sangat memungkinkan dimana suatu informasi dapat dibagikan kepada komputer atau user lain dalam suatu jaringan komputer ataupun jaringan yang lebih luas lagi yaitu internet. Hal itu menyebabkan tidak menutup kemungkinan ada pihak ketiga yang ingin merubah atau mengambil informasi tersebut. Informasi penting dan bersifat rahasia harus dijaga dari pihak-pihak yang tidak bertanggung jawab baik terhadap pemalsuan, pencurian maupun pengubahan data secara illegal.

Untuk mengatasi permasalahan di atas, salah satu solusi yang dapat diambil adalah dengan cara penyandian atau kriptografi. Dengan cara ini sebuah informasi akan disandikan berdasarkan metode tertentu sehingga orang yang tidak berkepentingan dan tidak memiliki hak akses akan mengalami kesulitan untuk melakukan hal-hal yang tidak diinginkan.

Ada dua teknik kriptografi klasik yaitu teknik subtitusi dan teknik transposisi. Salah satu teknik subtitusi yaitu algoritma vigenere cipher. Vigenere cipher pertama kali dipopulerkan oleh diplomat (sekaligus seorang kriptologis) Prancis, Blaise de Vigenere pada abad 16. Namun pada zaman sekarang ini teknik kriptografi

klasik khususnya vigenere cipher tidak dapat menyaingi metode-metode baru yang lebih baik, karena kesederhanaannya. Oleh karena itu, maka muncul suatu ide untuk membangun sistem keamanan menggunakan metode vigenere cipher yang digabungkan dengan permutasi cipher dengan memodifikasi key-nya menjadi dinamis pada setiap blok pesan yang sudah dibagi perkata.

Kriptografi mempunyai dua bagian yang penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dari penyandian pesan asli menjadi pesan yang tidak dapat diartikan seperti aslinya. Untuk dekripsi merupakan proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali. Pesan asli biasanya disebut plaintext, sedangkan pesan yang sudah disandikan disebut ciphertext.

II. Tinjauan Pustaka

A. Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dan tanda tangan digital dan keaslian pesan dengan sidik jari digital (Dony Ariyus, 2005).

B. Tujuan Kriptografi

1. Kerahasiaan (confidentiality)

Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2. Integritas data (data integrity)

Adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman

3. Otentikasi (authentication)

Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi (*user autehentication*).

4. Nirpenyangkalan (non-repudiation)

Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

C. Serangan Terhadap Kriptografi

Serangan terhadap kriptografi dapat dikelompokkan dengan beberapa cara:

1. Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu :

a. Serangan pasif (*passive attack*)

Pada serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang

menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuannaya adalah untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain :

1) *Wiretapping*
2) *Electromagnetic eavesdropping*
3) *Acoustic eavesdropping*

b. Serangan aktif (*active attack*)

Pada jenis serangan ini, penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya. Misalnya penyerang mengubah aliran pesan seperti menghapus sebagian cipherteks , mengubah cipherteks, menyisipkan potongan cipherteks palsu, me-replay pesan lama, mengubah informasi yang tersimpan, dan sebagainya.

2. Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, maka serangan dapat dikelompokkan menjadi lima jenis, yaitu:
   a. *Ciphertext-only attack*
   b. *Known*-plaintext *attack*
   c. *Chosen-plaintext attack*
   d. *Chosen-cipertext attack*
   e. *Chosen-text attack*
3. Berdasarkan teknik yang digunakan dalam menemukan kunci, maka serangan dapat dibagi menjadi empat, yaitu:
   a. *Exhaustive attack* atau *brute force attack*
   b. *Analytical attack*
   c. *Related-key attack*
   d. *Rubber-hose cryptanalysis*

Ini mungkin jenis serangan yang paling ekstrim dan paling efektif. Penyerang mengancam, mengirim surat gelap, atau melakukan penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan.

D. Metode Vigenere Cipher

Vigenere cipher merupakan jenis cipher abjad majemuk yang paling sederhana. Vigenere cipher menerapkan metode substitusi poli alfabetik dan termasuk ke dalam kategori kunci simetris dimana kunci yang digunakan untuk proses enkripsi adalah sama dengan kunci yang digunakan untuk proses dekripsi.

Berikut adalah contoh penggunaan algoritma Vigenere cipher dalam enkripsi pesan dan kunci sebagai berikut :

Pesan : SAYA GANTENG SEKALI

Kunci : BENAR

Metode yang digunakan dalam enkripsi dengan menggunakan Vigenere cipher adalah menyusun kunci bersesuaian dengan plainteks yang ada di atasnya. Apabila telah sampai di akhir

kunci, ulangi kembali penyusunan kunci sampai seluruh plainteks telah memiliki karakter kunci masing-masing. Berikut adalah contoh pesan dan kunci yang telah diurutkan:

Pesan : SAYA GANTENG SEKALI
Kunci : BENA RBENARB ENARBE

Langkah selanjutnya adalah melakukan Caesar Cipher untuk tiap-tiap karakter tersebut dengan nilai pergeseran karakter ditentukan oleh karakter kunci untuk tiap karakternya. Dalam Vigenere cipher ini, karakter A menyatakan pergeseran 0, B=1, C=2, D=3, ... , dan Z=25.

Dari Caesar Cipher terhadap masing-masing karakter, didapat :

Pesan : SAYA GANTENG SEKALI
Kunci : BENA RBENARB ENARBE
Chiper: TELA XBRGEEH WRKRMM

Perhatikan karakter „A‟ memiliki beberapa karakter hasil enkripsi yaitu „E‟, ‟A‟, „B‟, dan „K‟. Inilah yang mmembuat Vigenere cipher merupakan cipher abjad majemuk. Untuk teknik dekripsinya, kita hanya tinggal membalikkan proses enkripsinya saja, yang tadinya memajukan karakter menjadi memundurkan karakter.

E. Permutasi Cipher

Ciphereteks diperoleh dengan mengubah posisi huruf di dalam plaintekls. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian huruf di dalam plainteks. Nama lain untuk metode ini adalah transposisi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Contoh plaintext : “NETWORK SECURITY”

Teknik meng-enkripsi pesan plainteks tersebut dengan menulis secara horizontal dengan lebar kolom tetap, misal selebar 5 karakter (*kunci k = 5*)

N	E	T	W	O
R	K	S	E	C
U	R	I	T	Y

Maka cipherteksnya dibaca secara vertikal menjadi:

“NRUEKRTSIWETOCY”

Untuk mendekripsi pesan, perlu membagi panjang cipherteks dengan kunci. Pada contoh ini, kita membagi 30 dengan 5 untuk mendapatkan 5. Algoritma dekripsi identik dengan algoritma enkripsi. Jadi, untuk contoh ini dapat dituliskan cipherteks dalam baris-baris selebar 5 karakter menjadi:

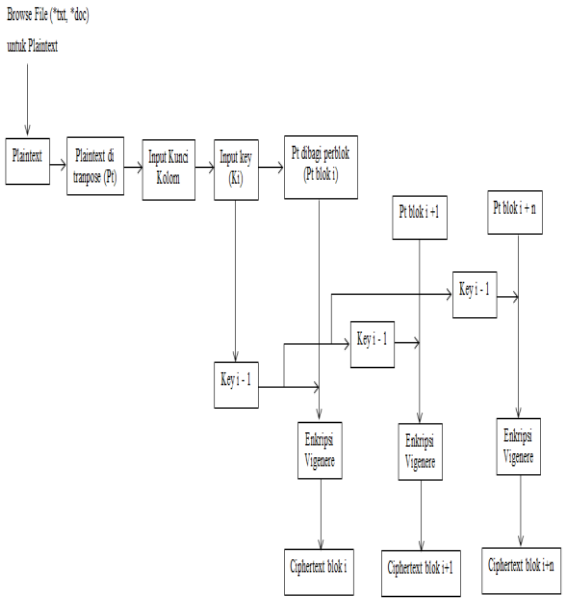
N	R	U
E	K	R
T	S	I
W	E	T
O	C	Y

Dengan membaca setiap kolom akan memperoleh plaintext asli yaitu:

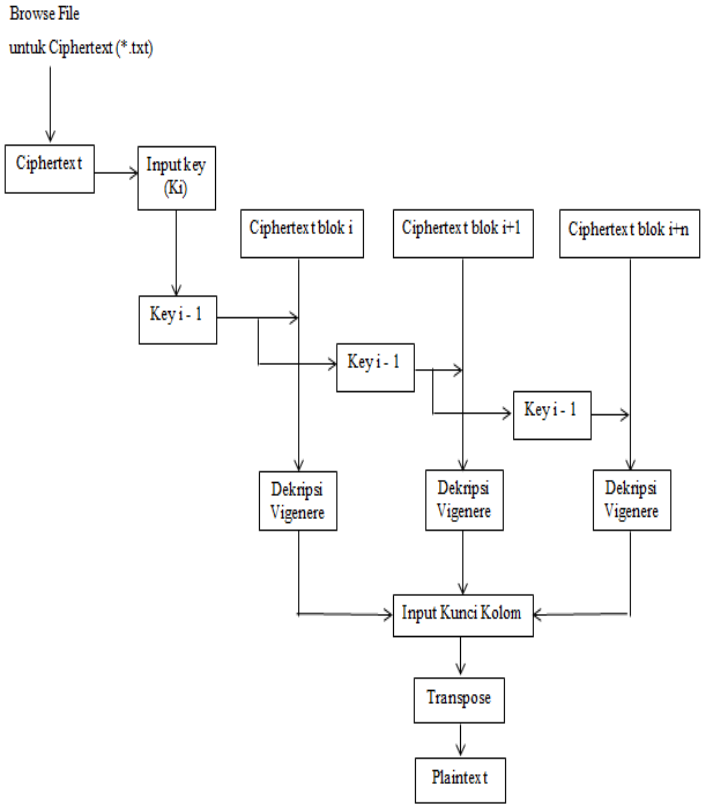
"NETWORK SECURITY"

III. Metode Penelitian

A. Blok Diagram



Gambar 3.1. Blok Diagram Proses Enkripsi File Text



Gambar 3.2. Blok Diagram Proses Dekripsi File Text

Keterangan :

Proses Enkripsi :

1. Memilih file text dengan mengklik menu 'Browse file' untuk dienkripsi.
2. Sebelum dienkripsi, teks asli (plaintext) terlebih dahulu di-*transpose*.
3. Masukkan kunci kolom.
4. Masukkan key (Ki) dengan panjang tidak boleh melebihi panjang plaintext.
5. Plaintext yang sudah di-*transpose* (Pt) kemudian dipecah menjadi blok-blok dengan panjang blok

adalah panjang key yang digunakan.

6. Setiap pemrosesan Pt blok i, akan memiliki key Ki-1 (key dinamis) yang dihasilkan dari blok key yang sebelumnya.
   Key i (Ki) = Ki blok 1 = Ki – 1;
   Ki blok 2 = Ki blok 1 – 1;
   Ki blok n = Ki blok n – 1;
7. Selanjutnya Pt blok i akan di enkripsi menggunakan vigenere cipher dengan key Ki-1 untuk membentuk ciphertext blok i (Ci).

Proses Dekripsi :

1. Memilih file text dengan mengklik menu ‘Browse file’ untuk didekripsi.
2. Masukkan key (Ki)
3. Ciphertext yang sudah dipecah perblok, selanjutnya akan didekripsi dengan key dinamis
4. Ciphertext blok i (Ci) didekripsi menggunakan vigenere cipher.
5. Masukkan kunci kolom
6. Hasil dari dekripsi tersebut di-*transpose* untuk membentuk file asli atau Plaintext (Pi).

B. Vigenere Cipher dan Permutasi Cipher dengan Key Dinamis

Rumus enkripsi vigenere cipher :

$$C_i = (P_i + k) \bmod 94$$

Keterangan:

C_i = Ciphertext
P_i = Plaintext
k = Kunci
mod 94= Modulus 94

Perhitungan :

Sebagai contoh, untuk pesan file teks (*plaintext)* “**TEKNIK INFORMATIKA**” kemudian diberikan kunci “**MANA**”. Sebelum menghitung *ciphertext, plaintext* di-*transpose* menggunanakan metode permutasi cipher.

Plaintext : TEKNIK INFORMATIKA

Kunci : MANA

Di-Permutasi : kunci kolom 5

T	E	K	N	I
K		I	N	F
O	R	M	A	T
I	K	A		

Hasil Permutasi : TKOIE RKKIMANNAIFT

Masukkan Key : MANA

Dipecah perblok, panjang blok = panjang key :

TKOI~E RK~KIMA~NNAI~FT

Key Dinamis (Key i -1) : LZMZ~KYLY~JXKX~IWJW~HV~

Cipherteks : **"'|%~pY &~u#xy~w'k"~n,~**

Keterangan : Tanda (~) merupakan tanda yang digunaka yang satu dengan yang selanjutnya.

Untuk proses dekripsi, langkah awal adalah men-generete ciphertext (Ci) tiap blok menggunakan metode vigenere

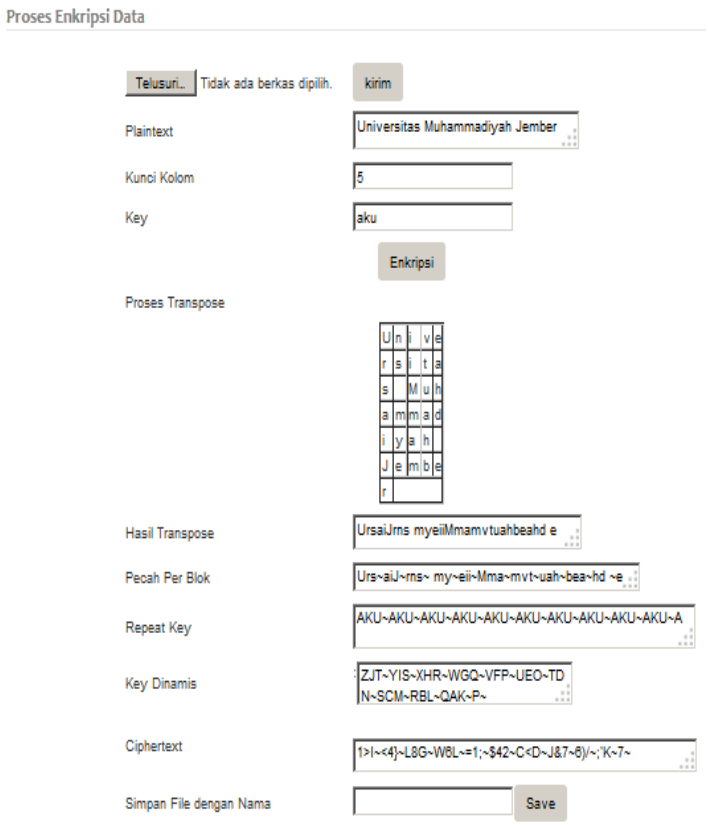
cipher dengan masing-masing key (Ki) blok yang berbeda. Hasil generete dari vigene cipher tersebut akan berupa plaintext (Pi) yang acak, untuk mendapatkan plaintext aslinya maka harus dilakukan transpose dengan kunci kolom yang sama diakhir metode.

IV. Implementasi dan Pengujian

Pada bagian ini akan dijelaskan tentang pengujian aplikasi untuk memastikan fungsi dari aplikasi yang telah dibuat. Untuk lingkup pengujian menggunakan file teks dokumen (*.txt dan *.doc) sebagai plaintext kemudian menghasilkan ciphertext juga dalam bentuk file text document.

A. Pengujian meng-*enkripsi* teks

Masuk ke aplikasi Kriptografi Teks Viper Dinamis (localhost/skripsi), kemudian klik menu *Enkripsi*.



Gambar 4.1 Langkah pengujian enkripsi teks

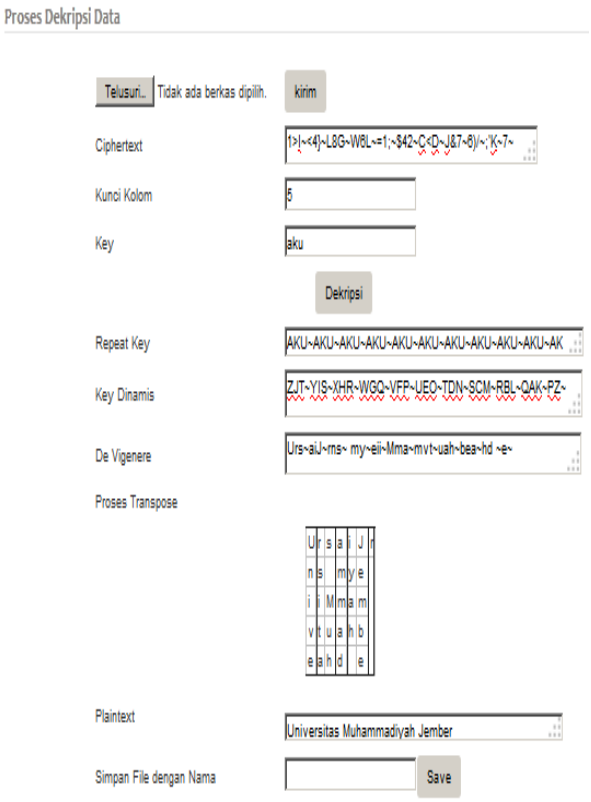
Keterangan proses *Enkripsi* :

Memilih *file text* dengan melakukan klik pada menu 'Telusuri' untuk dienkripsi. Sebelum dienkripsi, teks asli (*plaintext*) ditranspose terlebih dengan memasukkan 'Kunci Kolom'. Langkah selanjutnya yaitu memasukkan kunci pada kolom 'Key. Selanjutnya klik menu 'Enkripsi' maka dilakukan proses enkripsi menjadi *ciphertext* (teks yang sudah diacak/tidak asli). Kemudian tulis nama file dengan ekstensinya (*.txt atau *.doc) dikolom 'Simpan File', proses ini dilakukan untuk menyimpan

file yang sudah dienkripsi. Langkah terakhir klik 'Save'.

B. Pengujian men-*dekripsi* teks

Masuk ke aplikasi Kriptografi teks Viper Dinamis (localhost/skripsi) dan pilih menu *Dekripsi*.



Gambar 4.6 Langkah pengujian dekripsi teks

Keterangan proses *Dekripsi* :

Untuk membuka kunci enkripsi maka harus dilakukan proses dekripsi. Langkah awal yang harus dilakukan yaitu pilih menu 'Dekripsi'. Pilih menu 'Telusuri' untuk memilih *cipher text* yang dienkripsi. Selanjutnya transpose dengan memasukkan kunci kolom dan key. Klik 'Dekripsi' maka *file text* akan dihasilkan teks asli (*plaintext*).

V. Kesimpulan dan Saran

A. Kesimpulan

Dari hasil pengujian dapat disimpulkan sebagai berikut :

1. Aplikasi Kriptografi Teks Viper Dinamis telah berhasil diimplementasikan.
2. Aplikasi kriptografi ini tidak mudah dipecahkan oleh kriptanalis karena dilakukan transpose dan dibagi perblok sebelum dilakukan proses enkripsi maupun dekripsi.

B. Saran

Diharapkan aplikasi kriptografi teks ini dapat dikembangkan ke depannya untuk memaksimalkan hasil enkripsi dan dekripsi dengan menambah jumlah karakter menjadi lebih banyak pada *plaintext* dan *key*-nya, sehingga memaksimalkan *user* untuk menjaga kerahasiaan file dalam jumlah karakter yang lebih banyak sesuai dengan keinginan. Selain itu, dengan banyaknya karakter kemungkinan besar pesan enkripsi tidak dapat lagi dipecahkan oleh kriptanalis.

DAFTAR PUSTAKA

Agus, Chandra., (2014), *Implementasi Kriptografi Teks Berbasis Modifield Caesar Cipher Menggunakan Visual Basic*. Universitas Muhammadiyah Jember, Jember.

Arjana, Putu H., (2012), *Implementasi Enkripsi Data Dengan Algoritma Vigenere Cipher*. STMIK Dharma Putra, Tangerang.

Dwiartara, Loka., (2010), *Menyelam & Menaklukan Samudra PHP*. http://www.ilmuwebsite.com, Diakses pada 13 Juli 2012

Kumalasari, Erna., (2008), *Analisis Kriptografi Menggunakan Algoritma Vigenere Cipher Dengan Mode Operasi Cipher Block Chaining (CBC).* IST AKPRIND, Yogyakarta.

Leonardo, Kevin., (2012), *Modifikasi Vigenere Cipher dengan Metode Penyisipan Kunci pada Plaintext.* Institut Teknologi Bandung, Bandung.

Munir, R., (2004), *Algoritma Kriptografi Klasik,* Informatika, Bandung.

Rizky, Fatardhi., (2011), *Modifikasi Vigenere Cipher dengan Menggunakan Caesar Cipher dan Enkripsi Berlanjut untuk Pembentukan Key-nya.* Institut Teknologi Bandung, Bandung.