IMPLEMENTASI TRIPLE TRANSPOSITION VIGENERE CHIPER PADA PENGIRIMAN DATA TEKS DALAM JARINGAN LAN

[1]Asaziduhu Gea, [2]Fati G. N. Larosa, [3]Abraham Sembiring
[1,2,3]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Methodist Indonesia
[1]gea.asaziduhu@gmail.com, [2] fatignlarosa@gmail.com, [3]abrahamsembiring2@gmail.com

DOI: https://doi.org/10.46880/jmika.Vol3No1.pp7-13

ABSTRAK

Keamanan data menjadi sebuah hal yang tidak bisa dipisahkan pada pengolahan data menjadi informasi saat ini, terlebih pada prose pengiriman data tersebut didalam jaringan. Berbagai metode di gunakan untuk mengamankan data seperti menggunakan metode enkrispsi data. *Triple transposition vigenere chiper* adalah metode *enkripsi* dengan cara mengulang teknik *vigènere chiper* yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya. Proses yang terjadi pada *Triple Transposition Vigènere Chiper* terbagi menjadi dua bagian. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan vigenere yang disimbolkan dengan E serta kunci untuk melakukan vigenere K. Dengan metodeTriple Transposotion Vigenere Chipher pada jaringan LAN, mengamankan pesan yang benar-benar aman dan efektif untuk mencegah terjadinya penyadapan pesan. Dimana nantinya pertukaran kunci yang dilakukan adalah dengan mengenkripsi setiap subsequence yang dipartisi dari plain text sesuai metode *Vigenere Cipher* dengan algoritma kriptografi kunci simetris yang dapat saling berbeda, di mana jumlah subsequence yang dihasilkan adalah sebanyak algoritma kriptografi kunci simetris yang digunakan.Sehingga dengan metode seperti ini pengiriman data dalam jaringan tidak hanya nyaman tapi juga nyaman.

Kata Kunci: Keamanan Data, Triple Transposition Vigènere Chiper, Jaringan LAN, Kriptografi.

PENDAHULUAN

Teknologi pada saat ini berkembang sangat pesat, Salah satu teknologi yang cepat berkembang adalah jaringan komputer (*network*) dalam skala kecil *Local Area Network* (LAN) maupun skala luas yaitu *internet*. Dengan adanya jaringan pada komputer maka sangat dimungkinkan untuk terjadinya komunikasi antara satu komputer dengan komputer yang lainnya dalam waktu yang bersamaan secara cepat dan efisien. Untuk melakukan pengamanan dalam pengiriman data dibutuhkan suatu cara, salah satunya adalah dengan melakukan enkripsi. Enkripsi adalah salah satu bagian dari algoritma kriptografi. Dengan enkripsi data tidak dapat terbaca karena teks asli atau *plaintext* telah diubah ke teks yang tak terbaca atau disebut *chipertext*. Dalam penelitian ini, metode untuk enkripsi data yang penulis gunakan adalah menggunakan Metode *Triple Transposition Vigenere Chipher*. Cipher transposisi adalah metode enkripsi dimana posisi yang dimiliki oleh unit plaintext dialihkan sesuai dengan sistem yang teratur, sehingga chipertext merupakan permutasi dari plaintext. Plainteks yang dirubah susunan hurufnya seperti ini merupakan cipherteksnya.

Rumusan Masalah

Berdasarkan latar belakang yang telah digambarkan di atas, maka menetapkan pokok permasalahan yaitu :

a. Bagaimana mengamankan pesan yang benar-benar aman dan efektif untuk mencegah terjadinya penyadapan pesan dengan Metode *Triple Transposotion Vigenere Cipher* pada jaringan LAN?
b. Bagaimana mengimplementasikan Metode *Triple Transposition Vigenere Chipher* dalam enkripsi data yang akan dikirim?

Batasan Masalah

Untuk menghindari penyimpangan pembahasan dari tujuan awal maka diperlukan batasan masalah penelitian ini adalah sebagai berikut:

a. Data yang dikirimkan*User* berbentuk file text (file berisi huruf saja).
b. Metode kriptografi yang digunakan adalah Metode *Triple Transposition Vigenere Chipher*.
c. Aplikasi dirancang dengan menggunakan Bahasa Pemrograman Java.
d. Konsep jaringan yang digunakan adalah LAN *(Local Area Network)*

Tujuan dan Manfaat Penelitian

Adapun Tujuan penelitian ini adalah Membuat sistem yang dapat dijadikan sebagai aplikasi yang dapat mengirimkan data pada jaringan LAN dengan menggunakan sistem kriptografi Metode *Triple Transposition Vigenere Chipher* dalam enkripsi data yang akan dikirim yang bermanfaat untuk membantu menjaga keamanan dan kerahasiaan data pada saat proses pengiriman.

LANDASAN TEORI

Keamanan Sistem

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kali kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan setelah tampilan, atau bahkan di urutan terakhirdalam hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali masalah keamanan tidak begitu diperdulikan bahkan ditiadakan (Dony Ariyus, 2006:1).

Ancaman Keamanan

Ancaman keamanan yang terjadi terhadap informasi / data adalah:

a. *Interruption :* merupakan suatu ancaman terhadap *avaibability,* informasi, data yang ada dalam sistem dirusak, dihapus, sehingga jika data informasi tersebut dibutuhkan tidak ada lagi.
b. *Interception :* Merupakan ancaman terhadap kerahasiaan (*secrecy)* informasi yang ada disadap atau orang yang tidak berhak mendapat akses ke komputer dimana informasi tersebut disimpan.
c. *Modifikasi :* Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan dirubah sesuai dengan keinginan orang tersebut.
d. *Fabrication :* Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru (memalsukan) suatu informasi yang ada sehingga orang yang menerima informasi tersebut berasal dari orang yang dikehendaki oleh sipenerima inforasi tersebut.

Kriptografi

Kriptografi adalah teknik untuk menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Kriptografi adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Rifki Sadikin 2012:9).

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu sebagai berikut :

1. Kerahasiaan
   layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas untuk membuka informasi yang telah disandikan.
2. Integritas data
   Berhubungan dengan penjagaan dari perubahan data secara tidak sah.
3. Autentikasi
   saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keasliannya, isi datanya, waktu pengiriman dan lain sebagainya.
4. Non-repudiasi
   Usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan /membuat.

Sebagai ilustrasi pengirim pesan di WhatsApp mengirimkan pesan "Apa Kabar?", pada saat pesan dikirimkan maka pesan tersebut akan dienkripsi secara otomatis menjadi "9XB80FFAH". Kode tersebut sangat tidak akan dimengerti oleh pihak ketiga yang menyadapnya. Tetapi sesampainya pesan ke penerima maka secara otomatis kode "9XB80FFAH" akan kembali didekripsikan menjadi pesan semula "Apa Kabar?". Dengan menggunakan teknik enkripsi end-to-end (Jamaluddin, dkk., 2016)

Triple Transposition Vigenere Chiper

Triple transposition vigenere chiper adalah metode enkripsi dengan cara mengulang teknik *vigènere chiper* yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya. *Triple transposition vigenere chiper* terbagi menjadi dua bagian yaitu metode transposisi dan metode substitusi. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan *vigenere* yang disimbolkan dengan S serta kunci untuk melakukan teknik *vigenere.* (Ali Akbar Lubis, 2015).

Jaringan Komputer

Jaringan komputer merupakan sekelompok komputer otonom yang saling berhubungan antara satu dengan yang lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan perangkat keras bersama seperti *printer, harddisk*, dan sebagainya. (Stefan Wongkar, 2015)
Berdasarkan ruang lingkup, jaringan komputer terdiri dari :

1. *Local Area Network (LAN)*
   Merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer.
2. *Metropolitan Area Network (MAN)*
   Pada dasarnya merupakan versi *LAN* yang berukuran lebih besar dan biasanya memakai teknologi yang sama dengan *LAN*.
3. *Wide Area Network (WAN)*
   Jaringan yang memiliki jarak yang radiusnya mencakup sebuah Negara dan benua.

Unified Modeling Language* (*UML)

Menurut Adi Nugroho (2010:6), *Unified Modeling Language* (*UML) adalah bahasa pemodelan untuk system atau perangkat lunak yang berparadigma "berorientasi objek". Pemodelan (Modeling) sesungguhnya digunakan untuk penyederhanaan permasalahan-permasalahan yang kompleks sedemikian rupa sehingga lebih mudah dipelajaran dan dipahami.*

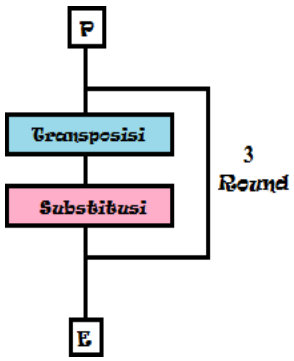
Java

Java adalah suatu teknologi di dunia software komputer selain merupakan suatu bahasa pemrograman, java juga merupakan suatu platform. Secara jelasnya java merupakan teknologi dimana

teknologi tersebut mencakup java sebagai bahasa pemrograman yang memiliki sintaks dan aturan pemrograman tersendiri, juga mencakup java sebagai platform dimana teknologi ini memiliki virtual machine dan library yang diperlukan untuk menulis dan menjalankan program yang ditulis dengan bahasa pemrograman java (Rickyanto 2003:2).

PERANCANGAN SISTEM

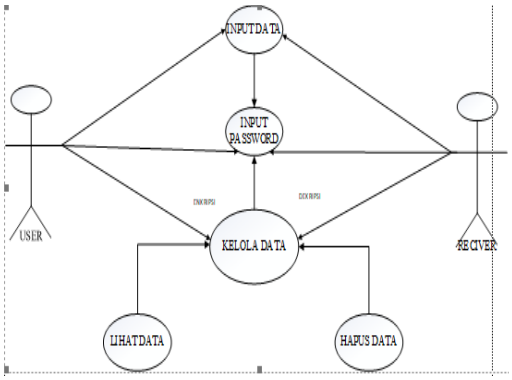
Penerapan Algoritma *Triple Transposition Vigenere Chiper*



Gambar 1. Proses *Triple Transposition Vigènere Chiper*

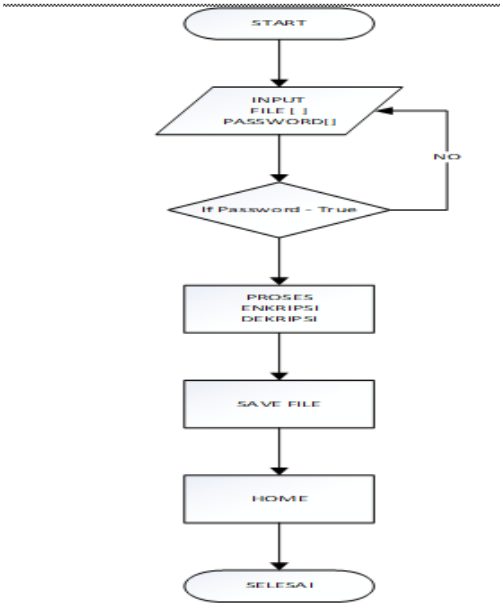
Pada metode *Triple Transposition Vigènere Chiper* ini, terlihat bahwa tergantungan hasil Chiperteks terhadap kunci sangat tinggi. Salah satu huruf saja, maka akan berakibat kesalahan yang Chiperteks. Setiap kunci harus didefinisikan dengan baik. Dengan begitu dapat dikatakan bahwa *Triple Transposition Vigènere Chiper* berpotensi untuk mengimbangi kekuatan *One-Time Pad*.

Triple Transposition Vigènere Chiper adalah metode enkripsi dengan cara mengulang teknik *Vigènere Chiper* yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya. Metode *Triple Transposition Vigènere Chiper* dapat digambarkan sebagai berikut:

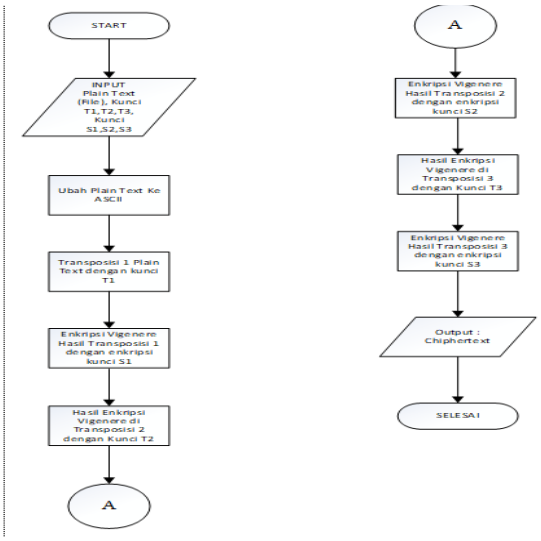


Gambar 2. *Use case* Diagram Pengaman data teks

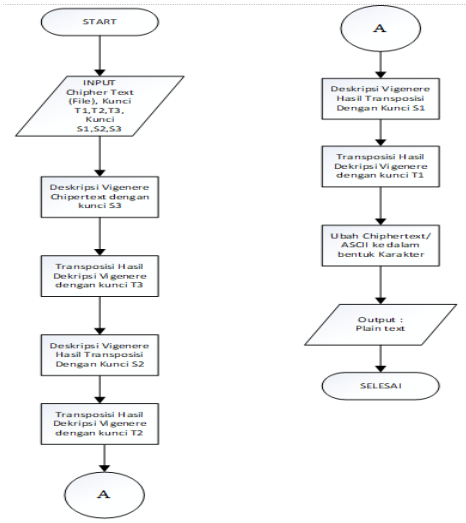
Penyusunan Diagram Alir *(flowchart)*



Gambar 3. *Flowchart* Sistem Yang Sedang Berjalan



Gambar 4. *Flowchart* Enkrpsi

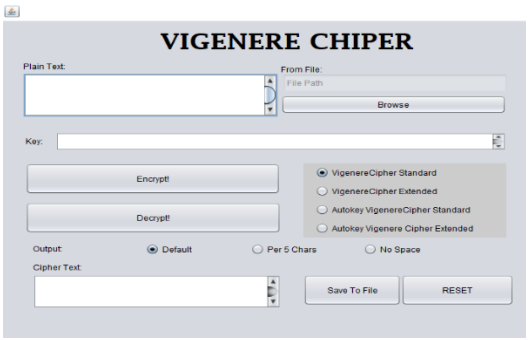


Gambar 5. *Flowchart* Dekripsi

IMPLEMENTASI SISTEM

Hasil Implementasi

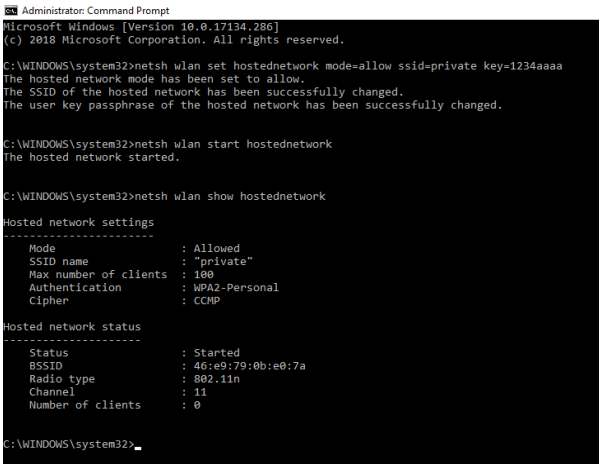
Berikut ini adalah tampilan implemetasi dari pengamanan data pada aplikasi pengiriman data menggunakan Triple Transposition Vigenere Chipher pada jaringan LAN.



Gambar 6. Tampilan menu utama

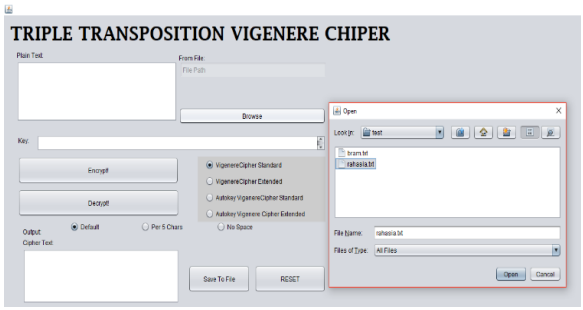
Implementasi Proses Pengiriman Data Dengan TTVC

Pada proses sistem ini, terlebih dahulu membuat jaringan LAN sebagai alat bantuan server untuk mengirim data ke client. Konfigurasi jaringan LAN menggunakan perintah cmd (Command Prompt). Berikut tampilan perintah untuk membuat jaringan LAN menggunakan perintah cmd (Command prompt).



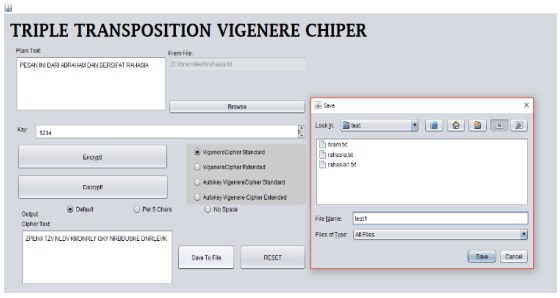
Gambar 7. Tampilan Membuat Jaringan LAN

Kemudian server mengambil file yaang mau dikim ke client menggunakan aplikasi Triple Transposisi Vigere Chiper Text. Berikut Tampilan pengambilan file menggunakan aplikasi Triple Transposisi Vigenere Chiper Text setelah file sharing diaktifkan.

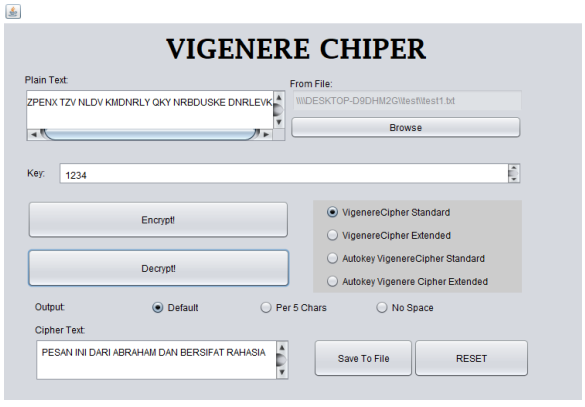


Gambar 8. Membuka File yang mau dikirim

Setelah file di input, maka plain text akan muncul. Dan server membuat kunci dengan kunci "1234". Kemudian server menyimpan file yang telah di *encrypt* ke file yang telah di sharing ke client. Berikut gambar dari pengiriman file yang telah di *encrypt* dan *decrypt.*



Gambar 9. Tampilan Menyimpan File Yang Telah di *Encrypt*.



Gambar 9. Tampilan Pengambilan File Yang Di *decrypt*

KESIMPULAN

Berdasarkan hasil perancangan dan pengujian yang dilakukan, maka diambil kesimpulan dan saran sebagai berikut:

1. Dengan metode*Triple Transposotion Vigenere Cipher* pada jaringan LAN, mengamankan pesan yang benar-benar aman dan efektif untuk mencegah terjadinya penyadapan pesan. Dimana nantinya pertukaran kuci yang dilakukan adalah dengan mengenkripsi setiap *subsequence* yang dipartisi dari *plain text* sesuai metode *Vigenere Cipher* dengan algoritma kriptografi kunci simetris yang dapat saling berbeda, di mana jumlah *subsequence* yang dihasilkan adalah sebanyak algoritma kriptografi kunci simetris yang digunakan.
2. Dengan sistem pengamanan file teks kombinasi algoritma kriptografi kunci public dalam kriptografi simetris dapat mengamankan pesan antar pengguna dari proses penyadapan. Dengan panjang karakter pesan yang disimpan menjadi dua kali lipat dari panjang yang asli.

DAFTAR PUSTAKA

Ariyus, D., (2006). *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu

Caroline, L.M. (2011). Metode Enkripsi baru Triple Transposition Vigènere Cipher. *Jurnal Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.*

Hermawan, J. (2005). *Analisa Desain & Pemrograman Berorientasi Obyek dengan UML dan Visual Basic.NET*. Yogyakarta: Penerbit Andi.

Jamaluddin, J., dkk. (2016). Konsep Pengamanan Pesan dengan Teknik End-to-End pada WhatsApp Messenger. *Jurnal STIPRO.* Vol. 9. No. 1.

Lubis, A.A., (2015). Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher, *Jurnal JSM STMIK Mikroskil.* Vol. 16 (2).

Nugroho, A.. 2010. *Rekayasa Perangkat Lunak Berbasis Objek dengan Metode USDP*. Yogyakarta: Penerbit Andi.

Rickyanto, I., 2003. *Dasar pemrograman Berorientasi Objek Dengan Java 2 (JDK 1.4)*. Yogyakarta: Penerbit Andi.

Sadikin, A.R. (2012). *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: Penerbit Andi.

Wongkar, S. (2015). Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan LAN, *Teknik Komputer*. Vol. IV(6), pp. 63-64.

Yatini, B.I., (2010). *Flowchart, Algoritma dan Pemrogaman Menggunakan Bahasa C++ Builder*. Yogyakarta : Penerbit Graha Ilmu.