IMPLEMENTASI VERNAM CIPHER UNTUK PENGAMANAN FILE TEKS

Jeita Parulian Pinem

STMIK Kristen Neumann Indonesia
Jl. Letjen Jamin Ginting KM. 10,5 Medan
Jeitapinem28@gmail.com

Program Studi Teknik Informatika

ABSTRAK

Salah satu proses pengamanan yang dapat diterapkan dalam proses penyimpanan file adalah dengan melakukan proses kriptografi. Proses kriptografi dilakukan dengan melakukan proses pengacakan data, sehingga file yang asli tidak mudah untuk dibaca oleh pihak yang tidak berkepentingan. . Metode Vernam Cipher mer upakanalgoritma berjenis symmetric key yaitu kunci yang digunakan untuk melakukan e nkripsi dan dekripsi yang menggunakan kunci yang sama. Dalam proses enkripsi, algoritma Vernam Cipher menggunakan cara stream cipher dimana cipher berasal dari hasil XOR an tara bit plaintext dan bit key. Dalam penelitian ini akan dibahas proses kriptografi terhadap suatu file teks. Proses kriptografi yang terdiri dari enkripsi dan dekripsi akan menggunakan metode Vernam Cipher.

***Kata Kunci** : Kriptografi, vernam cipher,Keamanan file.*

PENDAHULUAN

Kriptografi sudah mengalami pengembangan lumayan pesat, algoritma yang digunakan untuk perlindungan data semakin kompleks dan semakin sulit untuk dipecahkan, dan perkembangan cara berfikir Membuat manusia semakin bergantung kepada sebuah alat pengolahan data. Dan salah satu hal terpenting dalam komunikasi menggunakan komputer adalah untuk menjamin keamanan pesan, data, file, ataupun informasi dalam proses pertukaran data baik dalam jaringan komputer maupun melalui media.

Untuk mengamankan file data yang akan di simpan maupun yang akan dikirim. Maka dengan itu data atau file yang sudah disandikan atau dienkripsikan tidak akan mudah atau tidak akan dimengerti pihak lain tanpa melakukan dekripsi data.

Kriptografi dan enkripsi sangat dibutuhkan dalam pengamanan file. Dengan adanya kriptografi, data atau informasi yang dikirim dapat terhindar dari pembajakan, penghapusan, dan pensubstitusian yang dilakukan oleh user yang tidak berhak. Dalam hal ini, digunakan suatu metode yaitu autentikasi yang berkaitan dengan identifikasi/pengenalan kesatuan sistem maupun informasi itu sendiri.

Berikut ini beberapa penelitian tentang kriptografi yang berkaitan dengan Kriptografi Modern dan Algoritma *Vernam Cipher* :

1. Amanda Lilda Ramadayanti (2008) dengan judul penelitian Analisa Algoritma Vernam (OTP) menyatakan Algoritma Vernam atau One-timepad merupakan algoritma pengenkripsian data dan informasi yang relatif sederhana dan mudah digunakan namun cukup aman dalam menjamin kerahasiaan informasi atau data yang ingin dikirimkan oleh

pengirim pesan kepada penerima pesan tanpa dapat diketahui oleh pihak lain.

2. Sholeh dan Hamokwarong. (2011). Melakukan penelitian Aplikasi Kriptografi dengan Metode *Vernam Cipher* dan Metode Permutasi Biner. Jurnal Momentum Vol 7.
3. Aria, Rahajoeningroem (2011). Studi dan Implementasi Algoritma *RSA* untuk Pengamanan Data Transkip Akademik Mahasiswa.

Rumusan Masalah yang akan dibahas dalam penulisan skripsi ini adalah sebagai berikut :

1. Bagaimana merancang sebuah Aplikasi kriptografi untuk mengamankan file teks.
2. Bagaimana merancang aplikasi enkripsi file teks dengan *Vernam Cipher.*
3. Bagaimana menjelaskan proses te ks yang sudah dienkripsikan dan dikembalikan menjadi teks yang semula dengan melakukan dekripsi.

Adapun tujuan dari penulisan skripsi ini adalah sebagai berikut :

1. Menghasilkan sebuah kode yang tidak bisa dimengerti oleh pengguna informasi yang tidak berhak.
2. Membangun suatu program yang dapat menjaga keamanan dan menggunakan algoritma *Vernam Cipher.*
3. Menganalisa bagaimana cara kerja algoritma *Vernam Cipher* dalam kerahasiaan data.

Sejarah Kriptografi

Kriptografi memiliki sejarah yang panjang dan menarik, dimulai dari pekerjaan Feistel di IBM pada awal tahun 1970 sampai puncaknya pada tahun 1977 yang diadopsi oleh U.S *federal information Standard* untuk mengenkripsi informasi yang tidak terklasifikasi.

Perkembangan yang paling mencolok dalam sejarah kriptografi muncul di tahun 1976 ketika Diffie dan Hellman menerbitkan *New Direction in Cryptography*. Penelitian ini memperkenalk an konsep kunci public (*Public-Key)* yang revolusioner dan juga memberikan metode pertukaran kunci yang cerdas, keamanan berbasis *intracbility* pada masalah algoritma diskrit. Walaupun penulis tidak memiliki realisasi secara langsung dari skema enkripsi menggunakan *public-key* pada saat itu, namun ide tersebut sangat jelas dan mampu menarik minat komunitas kriptografi secara luas (Kromodimoeljo, S. 2009).

Metode *Vernam Cipher*

Metode *Vernam Cipher* merupakan sistem kerahasiaan yang sempurna di mana metode ini adalah *stream cipher* simetris di mana *plaintext* dikombinasikan dengan *key stream* (*pseudorandom*) yang sama panjang untuk menghasilkan *ciphertext* yang memungsikan *boolean* ekslusif. Algoritma *vernam cipher* diciptakan oleh Mayor J. Maugboune dan Gilbert Vernam pada Tahun 1917.

Pada algoritma *vernam cipher*, *plaintext* diubah kedalam ASCII. Nilai ASCII kemudian akan diubah kedalam barisan biner yang pada akhirnya akan dilakukan operasi XOR. Fungsi untuk melakukan operasi XOR antara *plaintext* dengan kunci dan fungsi untuk melakukan dekripsi adalah melakukan operasi XOR antar *cipher text* dengan kunci (Waruwu, T. S., Syahputra, I. E. & Lubis, A. H. 2014).

File Teks

File adalah kumpulan dari data dan informasi yang saling berhubungan dan juga tersimpan di dalam ruang penyimpanan sekunder. Definisi file dapat juga diartikan sebagai arsip atau data yang tersimpan di

dalam komputer. Secara konsep, file memiliki beberapa tipe, diantaranya adalah tipe data terdiri dari *character*, *numeric*, dan *binary*. Masing-masing file memiliki ekstensi yang berbeda sesuai dengan jenis filenya.

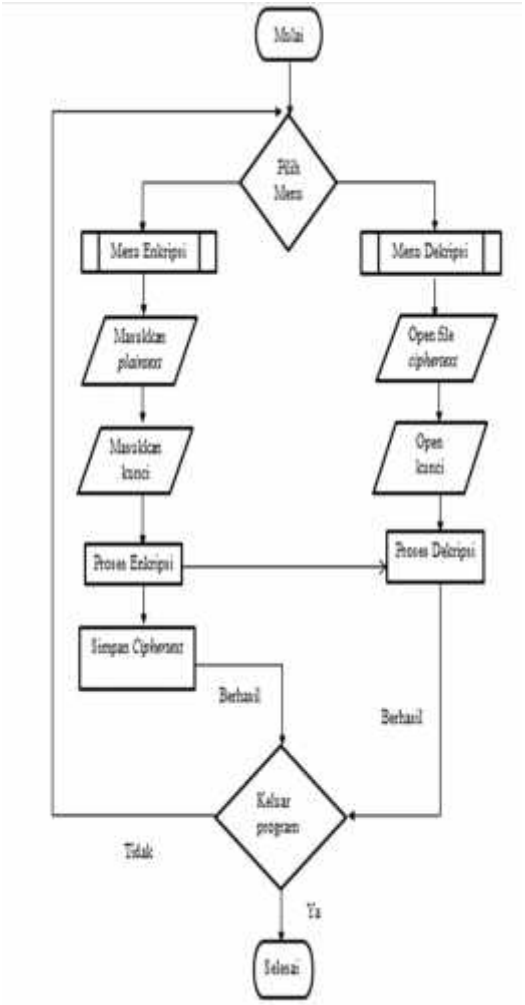
Sedangkan Teks adalah satuan lingual yang dimediakan secara tulis atau lisan dengan tata organisasi tertentu untuk mengungkapkan makna secara kontekstual. Untuk File teks merupakan file berisi data teks yang dapat disimpan dalam format teks biasa atau format teks kaya (Sitepu, N. B. 2014). Data yang berasal dari dokumen pengolah kata, angka yang digunakan dalam perhitungan, nama dan alamat dalam basis data merupakan contoh masukan d ata teks yang terdiri dari karakter, angka d an tanda baca. Untuk ekstensi file teks yang populer adalah: .TXT, .DOCX, .XML dan .SRT.

Metodologi Penelitian

Metodologi penelitian yang akan dilakukan dalam hal ini adalah Metode studi pustaka yaitu dengan membaca beberapa literatur-literatur dan referensi mengenai kriptografi yang diperoleh dari buku-buku dari berbagai jurnal, dan informasi yang ada di internet.

1. Analisis dan Design yaitu menganalisa kebutuhan program dan melakukan perancangan antarmuka dari aplikasi yang akan dibuat.
2. Pemrograman yaitu melakukan pengkodean terhadap rancangan-rancangan yang telah didefinisikan.
3. Implementasi yaitu mengevaluasi kemampuan program dalam mengubah data asli menjadi suatu runtutan data yang tidak bisa dimengerti oleh pengguna informasi yang tidak berhak.

Berikut ini merupakan *flowchart* sistem untuk enkripsi dan dekripsi file teks .



IMPLEMENTASI DAN HASIL

Setelah program aplikasi dirancang, maka tahap selanjutnya adalah tahap Hasil perancangan ini dilakukan dengan tujuan untuk mengetahui apakah berhasil atau tidak dan sesuai dengan yang dirancang. Aplikasi yang dihasilkan hanya dapat melakukan proses enkripsi dan dekripsi file teks.

Tampilan Menu Utama

Saat pertama kali aplikasi *Vernam Cipher* dijalankan, maka akan tampil *Form Menu* utama, terdapat empat menu yaitu Vernam, Help, About, dan Exit. Dimana pada menu Vernam kita akan melakukan proses enkripsi dan juga dekripsi. Untuk menu Help terdapat penjelasan sistem yang dirancang dan pemahamanya. Sedangkan menu About berisi profil pengguna progam.

Dan untuk menu Exit yaitu ketika kita ingin keluar dari aplikasi. Seperti gambar 1.

Gambar 1. Tampilan Menu Utama

Tampilan Form Vernam

Pada form ini user/pengguna diminta untuk mengetikkan teks yang akan dienkripsi ataupun di dekripsi dan juga *user*/pengguna diminta untuk memasukkan kunci agar dapat melakukan proses enkripsi dan juga dekripsi. Seperti gambar 2.

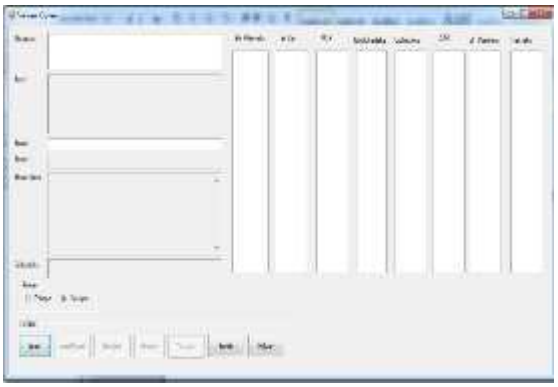
Gambar 2. Tampilan Aplikasi Vernam

Pada Form Vernam terdapat beberapa tombol yaitu :

1. Tombol “Load” berfungsi untuk melakukan panggilan file atau membuka file yang ingin di enkripsi maupun di dekripsi.
2. Tombol “Load Kunci” berfungsi untuk memanggil kunci yang sudah tersimpan dalam bentuk file, tombol ini akan muncul setelah melakukan load file untuk proses dekripsi.
3. Tombol “Enkripsi” berfungsi mengenkripsi teks yang mau dienkripsi setelah plainteks dan kunci di masukkan dan akan menghasilkan *Ciphertext.*
4. Tombol “Simpan” berfungsi untuk menyimpan hasil enkripsi plainteks dan kunci yang disebut *Ciphertext* kebentuk file, dan tombol ini akan muncul setelah proses enkripsi selesai.
5. Tombol “Dekripsi” berfungsi untuk mengeksekusi *Ciphertext* menjadi teks semula atau kembali ke plainteks, dan tombol ini akan muncul setelah proses enkripsi selesai.
6. Tombol “Bersih” berfungsi untuk menghapus semua tampilan baik itu plainteks, kunci, dan ciperteks di semua kolom ketika kita mau mengulang proses dari awal. Dan untuk
7. Tombol “Keluar” berfungsi ketika kita mau mengakhiri atau keluar dari aplikasi.

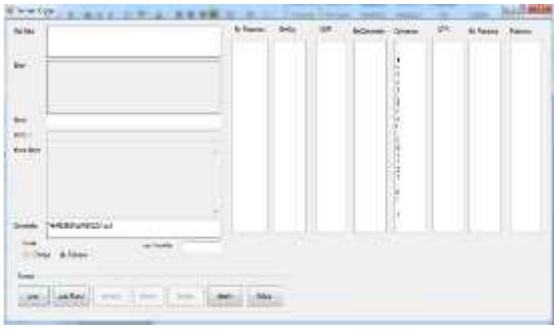
Proses Enkripsi

Setelah membuka form vernam *user/*pengguna diminta untuk mengetikkan teks yang akan dienkripsi. Teks yang dimaksud dapat berupa huruf,angka, dan simbol-simbol dan *user/*pengguna juga diminta untuk agar dapat melakukan proses enkripsi.Yang diinput juga dapat berupa huruf, angka, dan simbol-simbol. Pada saat proses enkripsi kita menyandikan teks dengan suatu kunci lalu dihasilkan *ciphertext*. Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis. Seperti gambar 3.



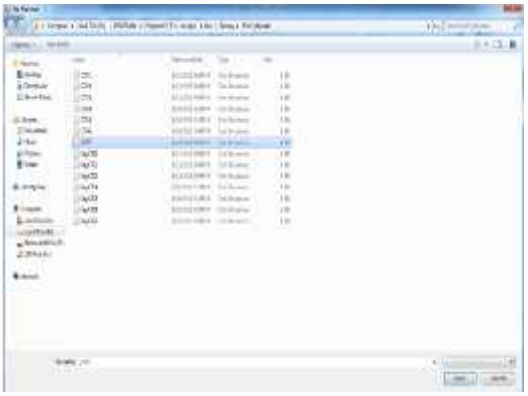
Gambar 3. Tampilan Vernam setelah didekripsi

Pada saat *user*/pengguna melakukan proses dekripsi maka *ciphertext* akan berubah menjadi pesan yang asli (*Plaintext*) yaitu (**17 Agustus #Merdeka73//.)**. Proses dekripsi juga dapat dilakukan dengan memanggil file yang sudah disimpan hasil dari enkripsi yang berisi *ciphertext* yang mana diawali kita harus menekan tombol "Load" dan kita akan diarahkan ke file yang mau kita open.



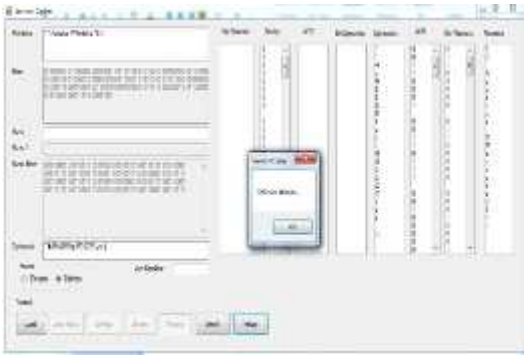
Gambar 4. Tampilan Vernam setelah membuka file teks yang terenkripsi

Setelah melakukan load file teks, maka isi file *ciphertext* itu akan muncul langsung pada kolom *ciphertext* pada aplikasi. Langkah selanjutnya yang kita lakukan adalah dengan melakukan load kunci, dengan cara yang sama yaitu dengan menekan tombol "Load Kunci" pada aplikasi kita akan dibawa ketempat folder file kunci yang tersimpan dan menekan open file akan terbuka. Akan tetapi meski kita melakukan Load Kunci, kunci tidak



Gambar 5. Tampilan File

akan lagi ditampilkan dalam bentuk teks melainkan dalam bentuk biner, meski begitu kita tetap dapat menjalankan proses dekripsi hanya dengan mengklik tombol dekripsi. Seperti gambar 6.



Gambar 7. Tampilan Vernam sesudah di dekripsi

Tampilan diatas menunjukkan proses Dekripsi file, yang mana *ciphertext* yaitu (" **vR$$EBFqt|RG52ZV - bx|-)** diubah kembali kedalam teks sebenarnya yang dinamakan *plaintext* (**17 Agustus #Merdeka73//.**).

KESIMPULAN

Dari hasil penelitian yang dilakukan terhadap aplikasi kriptografi enkripsi dan dekripsi file teks dengan menggunakan metode *Vernam Cipher*, dengan adanya

kesimpulan dan saran ini dapatlah suatu perbandingan yang akhirnya dapat memberikan perbaikan-perbaikan pada masa yang akan datang.

Adapun kesimpulan yang penulis peroleh adalah sebagai berikut :

1. Untuk menjamin kerahasiaan data serta menjamin keamanan kunci rahasia yang digunakan maka kunci yang degenerate harus benar-benar random atau acak.
2. Setiap satu spasi pada teks, akan terhitung satu karakter yang akan di Dekripsi maupun di Enkripsi.
3. Program ini merupakan sistem yang dibuat untuk membantu pengguna (user) dalam mengamankan *plaintext* file agar tidak diketahui oleh masyarakat umum, seperti file dokumen.
4. Teknik pengenkripsian ini relativ sederhana karena hanya menggunakan algoritma XOR dalam pembuatan sandinya.

DAFTAR PUSTAKA

[1] Ariyus, D. 2006. Pengertian Kriptografi Modern. Penerbit Informatika, Bandung.

[2] Chandra, R. & Noer, S. 2014. Implementasi Algoritma Enkripsi Kriptografi pada File. Jurnal Teknologi Volume : VII, Nomor: 2

[3] Daniel, A. M. & Sabatier, P. 1979. Pengertian Implementasi. Penerbit Pustaka Pelajar, Yogyakarta.

[4] Kromodimoeljo, S. 2009 Teori dan Aplikasi Kriptografi. SPK IT Consulting, Jakarta.

[5] Kurniawan, Y. 2004. Kriptografi Keamanan Internet dan Jaringan, Penerbit Informatika, Bandung.

[6] Madcoms, M. 2008. Microsoft Visual Basic. Penerbit C.V Andi Offset, Yogyakarta.

[7] Maugboune, J. M. & Vernam, G. 1917. Pengenalan Algoritma *Vernam Cipher*. *www.Cryptomuseum.com*, 11 Agustus 2012 (diakses11 Agustus 2012).

[8] Ramadayanti, A. L. 2008. Analisa Algoritma Vernam (OTP). Jurnal Teknik Electro majalah ilmiah unikom Vol 8, Universitas Komputer Indonesia.

[9] Rahajoeningroem, A. 2011. Studi dan Implementasi Algoritma *RSA* untuk Pengamanan Data Transkip Akademik Mahasiswa. Jurnal Teknik Electro majalah ilmiah unikom Vol 8, Universitas Komputer Indonesia.