

Kriptografi Dengan Metoda Substitusi Menggunakan Vb 6.0

TUGAS AKHIR

**Diajukan sebagai salah satu syarat
Untuk memperoleh gelar Ahli Madya**

Oleh

**Zainul Makmur
06 075 021**

**Program Studi Teknik Telekomunikasi
Jurusan Teknik Elektro**



**POLITEKNIK UNIVERSITAS ANDALAS PADANG
2010**

ABSTRAK

Kriptografi Dengan Metoda Substitusi Menggunakan Visual Basic 6.0

Oleh

Zainul Makmur
06075001

Keamanan dan kerahasiaan sebuah data atau informasi dalam komunikasi dan pertukaran informasi sangatlah penting. Seringkali data atau informasi yang penting, dalam komunikasi dan pertukaran informasi kadang tidak sampai kepada penerima atau tidak hanya diterima oleh penerima tetapi juga oleh pihak lain yang melakukan pembajakan atau penyadapan. Hal ini membuat data atau informasi tersebut menjadi tidak berguna lagi dan lebih parahnya lagi kadang data atau informasi tersebut oleh para pembajak digunakan untuk menjatuhkan pihak lain. Oleh karena itu kriptografi sangat dibutuhkan dalam menjaga kerahasiaan data atau informasi.

Algoritma kriptografi terdiri dari algoritma enkripsi (E) dan algoritma dekripsi (D). Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan metoda substitusi.

Key word: Kriptografi, metoda Substitusi, enkripsi, deskripsi

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam dunia sekarang ini, kemajuan teknologi di bidang komputer dan telekomunikasi berkembang sangat pesat. Seiring dengan perkembangan tersebut, maka memungkinkan dari berbagai lapisan masyarakat, termasuk para *cracker* dan penjahat lainnya dapat akses keberbagai komputer yang diinginkannya. Oleh karenanya kebutuhan akan keamanan kerahasiaan data atau informasi menjadi meningkat pula. Ini semua diperlukan untuk menghindari kejahatan terhadap komputer yang timbul sebagai akibat dari kemajuan teknologi tersebut. Terlebih kalau data tersebut terdistribusi dalam suatu jaringan komputer.

Ada berbagai jenis data yang perlu diamankan kerahasiaannya antara lain : data atau dokumen rahasia Negara, data strategis pengembangan usaha perusahaan swasta maupun pemerintah, data atau informasi hasil-hasil penelitian dan lain lain. Rusak atau hilangnya data hasil penelitian yang diperoleh dengan waktu dan biaya yang tinggi tentu saja sangat tidak diinginkan terlebih bila data tersebut merupakan data atau informasi pengembangan usaha.

Untuk menghindari terjadinya kejahatan terhadap komputer, maka diperlukan suatu keamanan yang baik, sehingga data yang terdapat pada komputer menjadi lebih aman. Salah satu cara yang paling baik adalah dengan menggunakan kriptografi. Terdapat berbagai macam algoritma dalam kriptografi

yang mampu memberikan jaminan keamanan dan kerahasiaan yang baik terhadap pesan. Salah satu algoritma yang mampu memberikan jaminan keamanan data adalah algoritma *substitusi*, untuk *enkripsi* data dalam berbagai aplikasi.

1.2 Tujuan

Adapun tujuan yang ingin dicapai dalam pembuatan tugas akhir ini adalah:

1. Dapat mengetahui konsep Kriptografi dan metoda yang digunakan dalam proses enkripsi - dekripsi.
2. Merancang suatu system yang dapat memberikan keamanan data dokumen yang dikirim.
3. Memberikan kenyamanan kerahasiaan data bagi para pengguna dalam berkomunikasi data.

1.3 Perumusan Masalah

Adapun permasalahan yang diangkat adalah sebagai berikut :

1. bagai mana menggunakan kriptografi dengan metoda substitusi.
2. Bagaimana pembuatan kriptografi dengan VB 6 dan *intervacanya*.
3. Bagaimana merubah suatu karakter menjadi karakter yang baru dengan alogaritma substitusi

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Kriptografi dengan menggunakan metoda substitusi yaitu merubah suatu karakter awal (plaintext) dengan karakter yang telah di enkripsi (ciphertext).
2. Pembuatan kriptografi metoda substitusi dapat menggunakan bahasa pemrograman Visual Basic 6 dimana fungsi-fungsi dari Visual basic 6 dapat merubah suatu karakter inputan menjadi suatu karakter baru.
3. Metoda kriptografi yang digunakan adalah metoda substitusi dimana suatu karakter awal (plaintext) digantikan dengan suatu karakter yang baru yang telah di enkripsi (ciphertext) dengan menggunakan key pada enkripsi " $\text{plaintext} \times 2 - 13$ " dan key pada deskripsi " $\text{ciphertex} / 2 + 6$ ".
4. Algoritma kriptografi ini merupakan algoritma asimetri dimana algoritma yang memakai kunci berbeda untuk proses enkripsi dan dekripsinya.
5. Kriptografi sangat berguna dalam keamanan data terutama dalam proses komunikasi data. Dimana suatu data yang di kirim pada suatu jaringan, akan aman walaupun data tersebut di sadap atau jatuh kepihak yang tidak bertanggung jawab karena data yang dikirim merupakan hasil enkripsi.

Daftar Pustaka

1. Situs Internet: ilmukomputer.com, yahoo.com, elektro.com, goggle.co.id
2. [Http://lecturer.ukdw.ac.id/budsus/jarkom/Week12.pdf](http://lecturer.ukdw.ac.id/budsus/jarkom/Week12.pdf).
3. [Http://www.vocal.com/AES_algorithm.pdf](http://www.vocal.com/AES_algorithm.pdf)
4. [Http://www.callio-id.com/bs7799/id,6](http://www.callio-id.com/bs7799/id,6)
5. Microsoft Encarta Library 2004 (Encryption).
6. [Http://www.agungnugroho.net](http://www.agungnugroho.net)