KEAMANAN FILE MENGGUNAKAN TEKNIK KRIPTOGRAFI SHIFT CIPHER

Eko Hari Rachmawanto[1], Christy Atika Sari [2]
[1,2]Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula 1 No 5-11 Semarang 50131 (024) 3569196
E-mail : rachmawanto@research.dinus.ac.id[1], atikasari@research.dinus.ac.id[2]

Abstrak

Dampak dari kemudahan pengaksesan informasi telah dirasakan oleh banyak pihak sebagai salah satu isu dalam keamanan data, khususnya file. Informasi sangat rentan untuk dimanipulasi oleh pihak yang tidak berkepentingan. Berdasarkan masalah tersebut, diperlukan teknik untuk mengamankan data. Teknik yang dikenal dapat digunakan untuk mengamankan data yaitu Kriptografi. Adapun algoritma kriptografi yang mudah untuk diterapkan namun mempunyai tingkat keamanan yang baik yaitu Shift Cipher. Shift Cipher dikenal lebih aman dibandingkan Caesar Cipher. Teknik ini menggunakan sisa bagi dari perhitungan yang dilakukan dan proses penyandian menggunakan operasi modulo 26. Dalam percobaan yang telah dilakukan pada sejumlah file dokumen, membuktikan bahwa Shift Cipher mempunyai kehandalan dalam mengamankan data. Hasil ekstraksi file telah berhasil dilakukan tanpa merusak file induk dan file pesan tanpa merubah isi dan ukuran file.

Kata Kunci : *Shift Cipher, Confidentiality, Kriptografi, File, Modulo.*

Abstract

The impact of the ease of access to information has been perceived by many as one of the issues in data security, in particular the file. Information is very vulnerable to manipulation by unauthorized parties. Based on these issues, the necessary techniques for securing data. Known techniques can be used to secure the data that is Cryptography. The cryptographic algorithms are easy to implement but has a good security level Shift Cipher. Shift Cipher known to be more secure than the Caesar Cipher. This technique uses for the remainder of the calculations performed and the process of encoding using modulo operation 26. In the experiments that have been performed on a number of files of documents, proving that the Shift Cipher has in securing the reliability of the data. The extracted files have been successfully carried out without damaging the master file and the message file without change the content and file size.

Keywords : *Shift Cipher, Confidentiality, Cryptography, File, Modulo.*

1. PENDAHULUAN

Adanya ketergantungan terhadap komputer dalam berbagai bidang membuat perpindahan informasi menjadi semakin cepat. Perpindahan informasi tersebut terkadang tidak diiringi oleh keamanan data yang sesuai. Pengamanan data menjadi sangat penting karena kemungkinan penggunaan file oleh orang lain yang tidak berwenang menjadi lebih besar. Berbagai teknik sering digunakan untuk mengamankan data, salah satunya yaitu kriptografi.

Di Indonesia, kriptografi dikenal sebagai teknik penyandian untuk menyandikan data serta informasi dari pihak-pihak yang sekiranya tidak berwenang. Data yang ada atau terkandung pada file tersebut dienkripsi menjadi beberapa simbol tertentu sehingga pihak berwenang saja yang

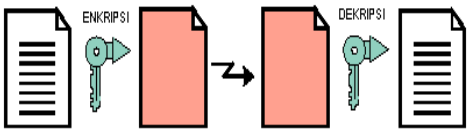
dapat mengetahui data/informasi hasil enkripsi [1]. Pengertian lain dari kriptografi dikenal sebagai ilmu untuk mempelajari cara penyandian data untuk memperoleh kerahasiaan, integritas dan autentikasi data [2]. Menurut era kemunculannya, kriptografi dapat dikasifikasikan menjadi 2 macam yaitu kriptografi klasik dan kriptografi modern. Terdaat bermacam jenis kriptografi klasik (konvensional) yang hingga saat ini telah dikembangakan. Kriptografi klasik mengguankan teknik cipher permutasi dan cipher transposisi, sehingga lebih cepat dibanding dengan kriptografi modern dan kunci yang digunakan merupakan kunci simetris, misalnya caesar cipher dan shift cipher [3]. Shift cipher merupakan salah satu bentuk kriptografi klasik/konvensional yang masih digunakan untuk mengamankan data. Shift cipher bekerja dengan menggeser plainteks sejauh yang diinginkan oleh pengguna, dengan maksimal pergeseran yaitu 26. Dalam penggunaannya, teknik shift cipher menggunakan model perhitungan modulo 26 dan kunci yang digunakan untuk proses enkripsi sama dengan proses dekripsi.

Dari keunggulan yang dimiliki, maka dalam makalah ini Shift Cipher dipilih sebagai teknik untuk mengamankan data, khususnya file. Adapun tujuan dari penelitian ini yaitu mengevaluasi performa algoritma shift cipher yang diimplementasikan dalam aplikasi pengamanan file melalui Visual Basic 6.0 dimana file tidak akan bida dibuka atau digunakan selain oleh pemilik file.

Beberapa penelitian mengenai keamanan file menyebutkan bahwa teknik kriptografi klasik unggul dalam mengamankan data. Menurut Syafa'at [4] dalam penelitiannya mengemukakan bahwa caesar cipher dan cipher subtitusi homofonik telah diujicoba menggunakan huruf dimana kedua teknik tersebut mempunyai kelemahan dan keunggulan masing-masing. Sedangkan Shift Vigenere Cipher [5] telah diimpleemntasikan dan terbukti juga unggul dalam mengamankan file teks.

2. METODE

Secara etimologi, kriptografi berasal dari bahasa Yunani yaitu "kriptos" dan "graphia". Kriptos dapat diartikan sebagai rahasia, sedangkan graphia dapat diartikan sebagai tulisan [3] merupakan ilmu yang digunakan untuk mempelajari tulisan rahasia dimana komunikasi dan data dapat dikodekan dan berfungsi mencegah orang yang tidak berwenang untuk memanipulasi informasi melalui sebuah teknik sehingga hanya pihak berwenang saja yang dapat mengetahui isi informasi tersebut [1].



Gambar 8. Konsep Penyandian Kriptografi

Berdasarkan kemunculannya, kriptografi dibedakan menjadi dua, yaitu kriptografi klasik dan kriptografi modern. Pada kriptografi klasik, proses enkripsi menggunakan perhitungan yang sederhana dan dapat dilakukan secara manual. Sedangkan pada kriptografi modern, proses enkripsi menggunakan perhitungan yang rumit dan melibatkan bilangan yang besar, sehingga diperlukan bantuan komputer [3]. Pada proses kriptografi, data yang dikenal dengan nama plainteks ditrasformasikan menjadi cipherteks yang tidak dikenali. Cipherteks

kemudian dikirim dan oleh penerima ditransformasikan menjadi plainteks kembali.

Kriptografi klasik dapat dijabarkan sebagai berikut [6]:

1. Subitusi Cipher, dikategorikan menjadi 2 yaitu *monoalphabetic*, setiap huruf pesan disubstitusi oleh satu huruf kunci *polyalphabetic*, setiap huruf pesan disubstitusi oleh beberapa huruf kunci dengan pola tertentu.
2. Transposisi Cipher, merupakan metode enkripsi dengan memindahkan posisi tiap-tiap huruf pesan dengan pola tertentu, misalnya *Blocking Cipher* dan Permutasi.

Sedangkan contoh dari kriptografi klasik yang lain yaitu antara lain *vigenere cipher, autokey cipher, reverse cipher, zig-zag cipher,* segitiga cipher, super enkripsi, mesin enigma, *rail fence cipher, nihilist cipher.*

Terdapat beberapa tuntutan yang terkait dengan isu mengenai keamanan data yaitu [7]:

a. Confidentiality
   Informasi hanya dapat diakses oleh pihak berwenang, yaitu pengguna atau pengirim dan penerima.
b. Authentication
   Baik pengirim maupun penerima mengetahui dengan jelas bahwa pesan yang dikirim betul-betuk berasal dari pengirim yang seharusnya.
c. Integrity
   Jaminan bahwa pesan yang dikirim sampai ke penerima tanpa ada bagian informasi yang dimanipulasi.
d. Nonrepudiation
   Pengirim atau penerima tidak dapat mengingkari bahwa keduanya telah mengirimkan atau menerima informasi.
e. Access Control
   Membatasi sumber informasi untuk orang lain yang ditunjuk/berwenang.
f. Availability
   Pada saat diperlukan, informasi dapat dengan mudah tersedia untuk pihak yang berwenang terhadap infomasi tersebut.

Shift cipher digunakan sejak jaman dahulu, tepaatnya saat pemerintahan Romawi Julius Caesar. Teknik ini merupkakan salah satu subtitusi cipher. Shift cipher yang merupakan generalisasi dari Caesar cipher, tidak membatasi pergeseran kunci sebanyak tiga huruf saja. Shift cipher menggunakan 26 kunci pergeseran sehingga lebih aman dibanding Caesar Cipher [8]. Teknik ini menggunakan sisa bagi dari perhitungan yang dilakukan [9]. Proses penyandian menggunakan operasi modulo 26. Plainteks disimbolkan dengan "P" sedangkan cipherteks disimbolkan dengan "C" dimana kunci disimbolkan dengan "K", sehingga didapatkan rumus enkripsi:

$$C = E(P) = (P+K) \bmod (26) \quad (1)$$

Sedangkan rumus enkripsi adalah sebagai berikut:

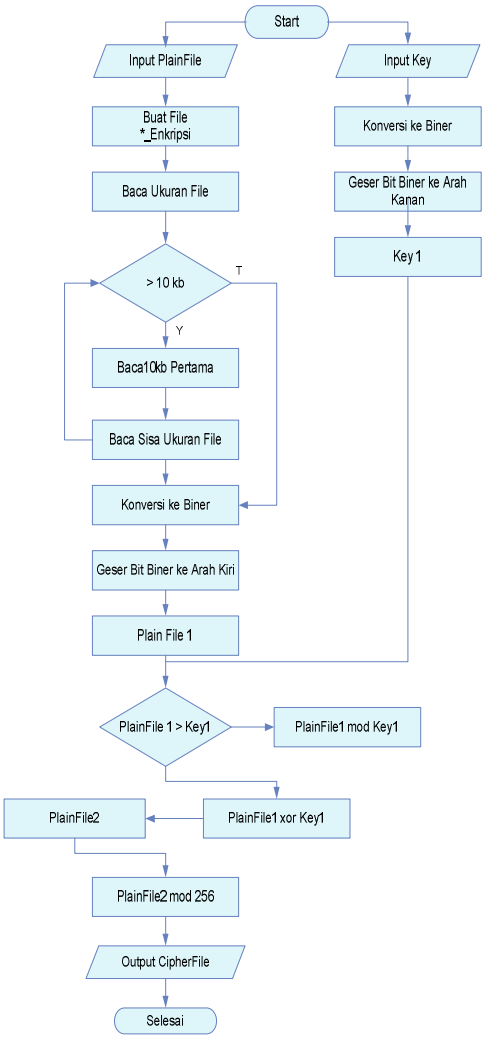
$$P = D(C) = (C–K) \bmod (26) \quad (2)$$

Dalam proses penyandian, tambahkan huruf yang akan disandikan dengan kunci sehingga akan diperoleh huruf sesuai alphabet sandi, sedangkan untuk mendekripsi dapat digunakan cara sebaliknya. Berikut ini merupakan contoh penggunaan shift cipher. Plainteks : "UDINUS", bentuk plainteks yaitu 21 4 9 14 21 19, apabila kunci yang digunakan yaitu 5 maka cipherteks menjadi 25 9 13 19 26 24 sehingga apabila ditransformasikan dalam huruf menjadi Z I N R Z W.

3. HASIL DAN PEMBAHASAN

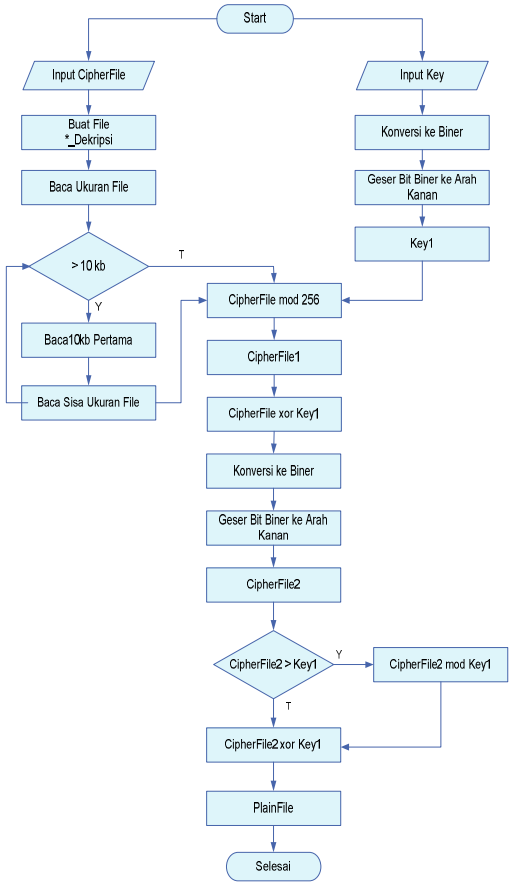
Aplikasi keamanan password ini dibuat dengan bahasa pemrograman Visual Basic 6.0. dalam beberapa percobaan yang dilakukan dengan format file dokumen antara lain txt, doc, dan docx dapat dilihat pada gambar-gambar berikut.

Di bawah ini merupakan flowchart penelitian yang digunakan.



Gambar 2. Flowchart Proses Penyisipan File menggunakan algoritma Shift Cipher

Sedangkan proses ektraksi file dapat dilihat pada Gambar 3 berikut ini.



Gambar 3. Flowchart Proses Ekstraksi File menggunakan algoritma Blowfish

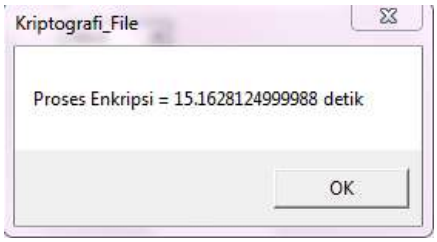
Berikut ini merupakan tampilan hasil percobaan enkripsi dan dekripsi menggunakan file .doc.

Gambar 4. Tampilan Awal Aplikasi Pengamanan Data

Gambar 4 merupakan tampilan awal dari aplikasi pengamanan data. Adapun format file yang dapat diolah oleh aplikasi ini antara lain dokumen berformat .doc, .docx, .pdf, .txt, dan .xls.

Gambar 5. Proses Input PlainFile dan Key

Pada Gambar 5 dapat dilihat proses enkripsi file dimulai dengan menginputkan plainfile (file asli), kunci yang digunakan dan ekstensi file. Kunci yang digunakan pada proses ini dapat berupa Character (huruf dan angka), sedangkan ekstensi file yang digunakan merupakan file dokumen seperti pada penjelasan Gambar 4 diatas.

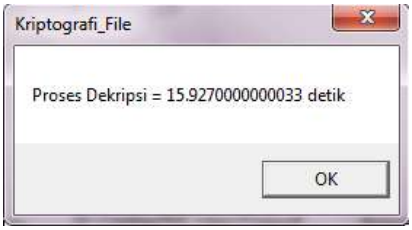


Gambar 6. Lama Proses Berjalan pada Proses Enkripsi

Proses enkripsi file telah selsesai dilakukan ditandai dengan munculnya tampilan informasi seperti pada Gambar 6 diatas yang mendeskripsikan lamanya waktu tempuh aplikasi untuk melakukan proses enkripsi.

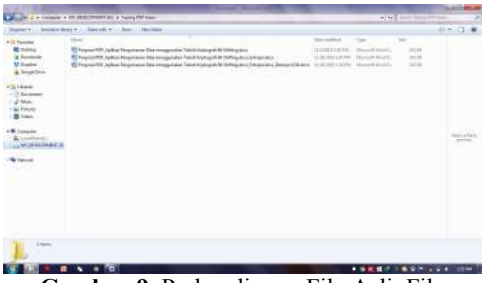
Gambar 7. Input Cipher File, Kunci dan Ekstensi File

Setelah proses enkripsi selesai, maka perlu dilakukan evaluasi apakah proses enkripsi tersebut telah berhasil untuk dilakukan. Salah satu carany yaitu melakukan proses dekripsi file. Proses ini dimulai dengan memasukkan file enkripsi, kunci dan ekstensi file. Dalam hal ini, kunci yang digunakan untuk proses dekripsi harus sama dengan kunci pada proses enkripsi. Demikian juga dengan ekstensi file, harus sama antara proses enkripsi dan dekripsi.



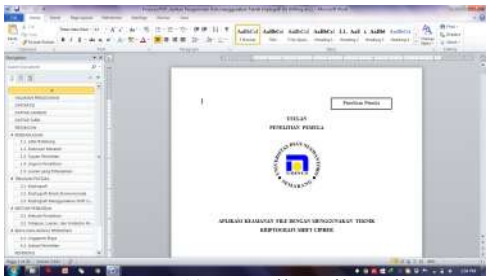
Gambar 8. Lama Proses Berjalan pada Proses Dekripsi

Proses dekripsi file telah selsesai dilakukan ditandai dengan munculnya tampilan informasi seperti pada Gambar 8 diatas yang mendeskripsikan lamanya waktu tempuh aplikasi untuk melakukan proses dekripsi.

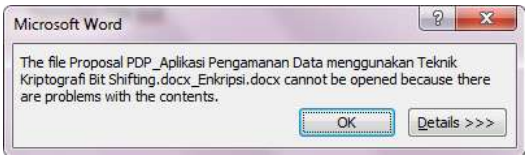


Gambar 9. Perbandingan File Asli, File Enkripsi dan File Dekripsi

Gambar 9 merupakan tampilan File asli, file hasil enkripsi dan file hasil dekripsi. Tampilan diatas menunjukkan bahwa ukuran file asli, file enkripsi maupun file dekripsi masih tetap dalam ukuran yang sama. Hal ini membuktikan bahwa proses enkripsi dan dekripsi berhasil dan orang lain tidak dapat mengetahui bahwa file asli tersebut telah diamankan melalui teknik kriptografi.

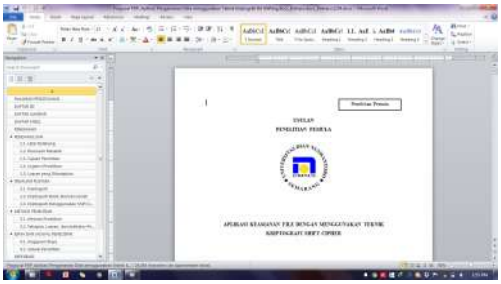


Gambar 10. Tampilan File Asli



Gambar 11. Bukti File Telah Berhasil Dienkripsi

Gambar 11 merupakan informasi bahwa file yang terenkripsi tidak dapat dibuka. Hal ini menjadi acuan bahwa proses enkripsi berhasil. File hasil enkripsi ini kemudian digunakan sebagai file inputan dalam proses dekripsi.



Gambar 12. File Hasil Dekripsi

Gambar 12 merupakan file hasil proses dekripsi dari file pada Gambar 11 apabila file hasil dekprisi ini dapat dibuka atau dibaca dan tampilan sesuai dengan file asli atau plainteks maka proses dekripsi dapat dikatakan berhasil.

4. KESIMPULAN

Penelitian ini sangat diperlukan untuk mengatasi permasalahan keamanan data yaitu Confidentiality dimana data maupun informasi hanya diakses oleh pihak yang berwenang melalui teknik kriptografi dengan mengimplementasikan salah satu algoritma kriptografi klasik yaitu shift cipher. Sehingga dapat disimpulkan bahwa semua masalah keamanan yang berkaitan dengan komputer, khususnya file, tidak dapat dipisahkan dari kriptografi. Dari hasil percobaan dengan

menggunakan file .docx, file hasil proses enkripsi tidak mengalami perubahan baik isi maupun ukuran file. Proses ekstraksi berjalan dengan sempurna dan menghasilkan file hasil dekripsi yang sama dengan file dekripsi. Dari percobaan yang telah dilakukan, terbukti bahwa shift cipher handal untuk mengamankan file dokumen.

DAFTAR PUSTAKA

[1] Kurniawan, Y. (2004). Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika.

[2] Wikipedia. (2015, Agustus 5). kriptografi. Retrieved Oktober 3, 2015, from wikipedia: https://id.wikipedia.org/wiki/kriptografi.

[3] Munir, R. (2006). Kriptografi. Bandung: Informatika.

[4] Syafa'at, A. (2009). Perbandingan Kriptografi Subtitusi Homofonik dan Poligram dengan Vaesar Cipher.

[5] Dikson, A. (2007). Rancangan Algoritma Shift Vigenere Cipher.

[6] Stallings, W. (n.d.). Kriptografi. Retrieved Oktober 6, 2015, from William Stallings: http://williamstallings. com/ Extras/ Security –Notes / lectures /classical.html.

[7] Stallings, W. (2006). Cryptography and Network Security, Principles and Practices. London: Pearson Education.

[8] National Sience Foundation. (2008). Kriptografi. Retrieved Oktober 3, 2015, from math.cornell: http://www.math.cornell.edu/~mec/Summer2008/lundell/lecture1.html.

[9] *Cyptography*. (2009). Retrieved Sepetember 5, 2015, from khanacademy: https:// www.khanacademy.org/computing/computer-science/cyrptography.