IMPLEMENTASI ALGORITMA AES 128 DAN RC4 UNTUK PENGAMANAN EMAIL PADA PT. DINAMIKA HYDRO ENGINEERING

Ahmad Galih Pramudito[1)], Dewi Kusumaningsih[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : ahmadgalihpramudito@gmail.com[1)], dewi.kusumaningsih@budiluhur.ac.id[2)]

ABSTRAK

PT. Dinamika Hydro Engineering adalah perusahaan yang bergerak dibidang Hydraulic. Perusahaan ini melayani pembuatan System Hydraulic, dan semua informasi proses negosiasi mulai dari pembuatan desain, persetujuan biaya, dan serah terima barang dikirim menggunakan email. Berdasarkan hal tersebut, PT Dinamika Hydro Engineering membutuhkan suatu metode untuk menjaga kerahasiaan email yang mengandung data atau informasi yang bersifat rahasia. Salah satu cara yang dapat digunakan untuk menganggulangi hal tersebut adalah dengan menggunakan teknik kriptografi. Kriptografi adalah sebuah teknik menyamarkan suatu pesan yang mudah dibaca (plaintext) menjadi suatu pesan yang sulit dibaca atau dipahami (ciphertext). Tujuan dari penulisan laporan tugas akhir ini adalah membuat aplikasi kriptografi email yang dapat melakukan penyandian terhadap suatu pesan, data dan informasi yang dikirim atau diterima oleh PT Dinamika Hydro Engineering. Perancangan aplikasi pada penulisan laporan tugas akhir ini menggunakan metode pengembangan SLD(System Development Life Cycle). SLDC merupakan metode klasik yang digunakan untuk mengembangkan, memelihara dan menggunakan sistem informasi. Algoritma yang digunakan untuk pembuatan aplikasi kriptografi email ini adalah algoritma AES 128 dan RC4. Berdasarkan implementasi dan pengujian aplikasi, menghasilkan aplikasi yang mudah untuk digunakan, dan dapat disimpulkan bahwa pesan yang dikirim dan diterima melalui aplikasi ini terjamin keamanannya karena pesan yang dikirim sudah melalui proses enkripsi dan pesan tidak dapat terbaca jika tidak menggunakan aplikasi ini.

Kata kunci : AES 128, RC4, Kriptografi, Email

1. PENDAHULUAN

1.1. Latar Belakang

PT Dinamika Hydro Engineering adalah perusahaan yang bergerak dibidang *Hydraulic*. Perusahaan ini melayani pembuatan *system hydraulic*, dan semua informasi proses negosiasi mulai dari membuat desain, persetujuan biaya, dan serah terima barang dikirim menggunakan *email*. Berdasarkan hal tersebut, PT Dinamika Hydro Engineering membutuhkan suatu metode untuk menjaga kerahasiaan *email* yang mengandung data atau informasi yang bersifat rahasia. Salah satu cara yang dapat digunakan untuk menanggulangi hal tersebut adalah dengan menggunakan teknik kriptografi. Kriptografi adalah sebuah teknik menyamarkan suatu pesan yang mudah dibaca (*plaintext*) menjadi suatu pesan yang sulit dibaca atau dipahami (*chipertext*).

Berdasarkan uraian diatas penulis bermaksud untuk membuat suatu aplikasi untuk mengamankan isi pesan yang akan dikirim menggunakan media *email* untuk membantu mengatasi masalah keamanan data dan informasi pada PT Dinamika Hydro Engineering sehingga hanya orang yang bersangkutan yang dapat mengetahui isi dari pada informasi tersebut.

1.2. Masalah

perumusan masalah dalam menyelesaikan penulisan laporan Tugas Akhir ini adalah "Bagaimana cara mengamankan informasi atau pesan yang akan dikirim atau diterima oleh PT. Dinamika Hydro Engineering supaya terjamin keamanannya?".

1.3. Tujuan

Tujuan dari penulisan laporan Tugas Akhir adalah membuat aplikasi kriptografi *email* berbasis web yang dapat melakukan penyandian (Enkripsi dan Dekripsi) terhadap informasi atau pesan yang dikirim atau diterima oleh PT. Dinamika Hydro Engineering dengan mengkombinasikan algoritma AES-128 dan RC4 sehingga informasi atau pesan yang sifatnya

rahasia akan terjamin keamanannya dan diharapkan aplikasi yang dibuat dapat dimengerti dan digunakan oleh pengguna.

1.4. Batasan Masalah

Dalam penulisan laporan Tugas Akhir ini penulis memfokuskan masalah yang ada agar tidak menyimpang pada pokok bahasan, pembatasan masalah ini diantaranya sebagai berikut:

a. Metode yang digunakan dalam aplikasi ini adalah RC4 dan AES-128.
b. Data yang dienkripsi dan didekripsi adalah data berbentuk teks (isi pesan) dan *file* lampiran berformat *.jpg, *.png, *.txt, *.pdf, *.doc, *.docx, *.xls, *.xlsx, *.ppt, dan *.pptx.
c. Total ukuran *file* maksimal 15 MB.
d. Aplikasi dibuat dengan berbasis *Web*.
e. Bahasa pemograman yang digunakan adalah *PHP*.

2. LANDASAN TEORI

2.1. Sejarah Kriptografi

Kriptografi telah dikenal kurang lebih pada tahun 2000 sebelum masehi oleh bangsa Mesir. Berbentuk tulisan *heiroglyphic* pada monumen. Bangsa *Mesopotania* telah menggunakan kriptografi pada tahun 1500 sebelum masehi, selanjutnya dikenal juga oleh bangsa Yahudi dan bangsa Yunani[1].

Pada perkembangannya aplikasi kriptografi dimanfaatkan secara intensif untuk keperluan pengiriman data secara rahasia pada saat manusia berperang. Implementasi berupa alat atau mesin rotor yang dapat berfungsi sebagai penghasil *ciphertext* dan untuk mengembalikannya ke dalam bentuk *plaintext*. Contoh mesin jenis ini yang terkenal pada perang dunia II adalah *Enigma*, digunakan oleh pihak tentara Jerman untuk menyandikan informasi pada saat dikirimkan[2].

.

2.2. Definisi Kriptografi

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah *plaintext*. Kemudian setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini disebut sebagai *chipertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut enkripsi (*encryption*), dan proses pengembalian dari *ciphertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*)[3].

Kekuatan algoritma yang digunakan untuk proses enkripsi dan dekripsi berhubungan erat dengan penggunaan persamaan matematika. Semakin banyak dan rumit perhitungan dari persamaan matematika yang digunakan maka data sandi semakin aman[4]. Kerahasiaan kunci adalah bagaimana cara kunci tersebut disimpan dan didistribusikan kepada pihak yang berhak menerima data, karena kunci ini akan digunakan untuk melakukan dekripsi. Semakin rapih kunci disimpan dan didistribusikan maka data sandi semakin aman[2].

2.3. Algoritma AES

Algoritma AES terdiri dari urutan data sebesar 128 *bit*. Urutan data yang sudah terbentuk dalam satu kelompok 128 *bit* tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *ciphertext*. *Cipher key* dari AES terdiri dari *key* dengan panjang 128 *bit*, 192 *bit*, atau 256 *bit*. Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma AES ini. Tabel 1 dibawah ini yang akan memperlihatkan jumlah *round*/putaran (Nr) yang harus diimplementasikan pada masing-masing panjang kunci[5].

Tabel 1. Tabel Perbandingan Jumlah *Round* dan *Key*

	Jumlah *Key* (Nk)	Ukuran *Block* (Nb)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2.3.1. Ekspansi kunci

Penyandian AES membutuhkan kunci ronde untuk setiap ronde transformasi kunci ronde ini di bangkitkan (diekspansi) dari kunci AES. Pada bagian ini di bahas bagaimana kunci ronde di bangkitkan oleh kunci AES. Kunci AES 128 bit atau 4 *word* menghasilkan sebuah larik sebanyak 44 *word* yang menjadi kunci[6].

2.3.2. Enkripsi AES

Blok-blok data masukan dan kunci dioperasikan dalam bentuk array. Setiap anggota array sebelum menghasilkan keluaran ciphertext dinamakan dengan state. Setiap state akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu,

AddRoundKey, SubBytes, ShiftRows, dan MixColumns [7].

2.3.3. Dekripsi AES

Transformasi byte yang digunakan pada invers cipher pada proses dekripsi AES adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey[7].

2.4. Algoritma RC4

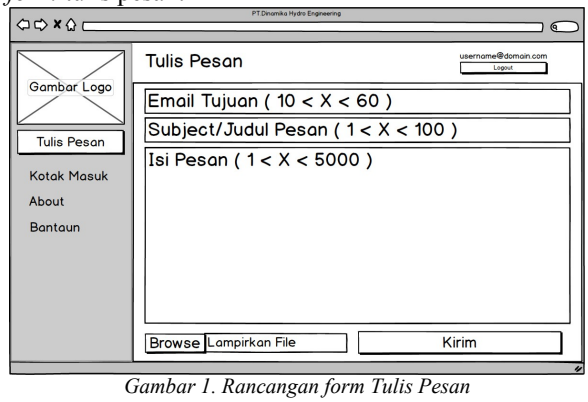
Rivest Code (RC4) merupakan salah satu jenis algoritma yang mempunyai sebuah S-*Box* S0, S1, …,S255 yang berisi permutasi dari bilangan 0 sampai 255[8]. Pada algoritma enkripsi ini akan membangkitkan *pseudo random byte* dari *key* yang akan dikenakan operasi XOR terhadap *plaintext* untuk menghasilkan *ciphertext*.

Secara garis besar algoritma dari metode RC4 *stream cipher* ini terbagi menjadi dua bagian, yaitu *key-scheduling algorithm* (KSA) dan *pseudo-random generation algorithm* (PRGA)[9].

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Rancangan Form Tulis Pesan

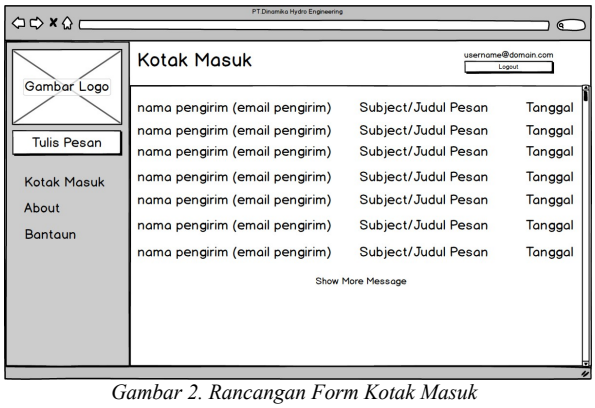
Rancangan layar *form* tulis pesan ini berfungsi untuk mengirim pesan ke alamat lain. Disini pengguna harus memasukkan alamat tujuan, judul pesan(*subject*), isi pesan, dan lampiran(jika dibutuhkan). Berikut adalah tampilan rancangan layar *form* tulis pesan:



Gambar 1. Rancangan form Tulis Pesan

3.2. Rancangan Form Kotak Masuk

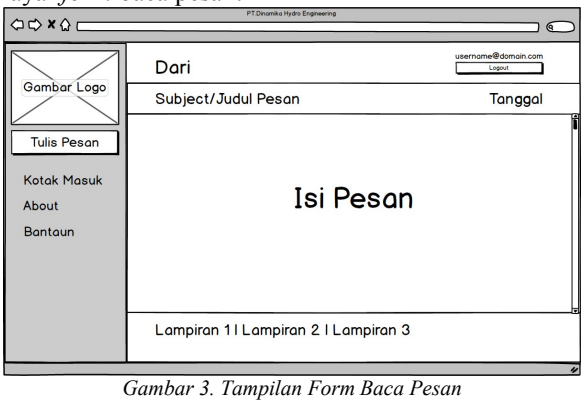
Disini pengguna dapat melihat semua pesan yang masuk ke *email* pengguna. berikut adalah tampilan rancangan layar *form* kotak masuk:



Gambar 2. Rancangan Form Kotak Masuk

3.3. Rancangan Form Baca Pesan

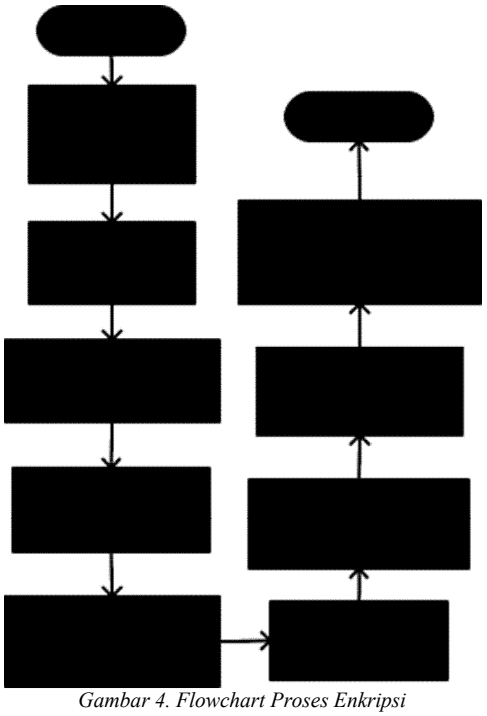
Rancangan layar *form* baca pesan ini berfungsi untuk menampilkan keseluruhan isi pesan mulai dari alamat *email* pengirim, *subject* pesan, tanggal pesan, dan isi pesan. Berikut adalah tampilan rancangan layar *form* baca pesan:



Gambar 3. Tampilan Form Baca Pesan

3.4. Flowchart Proses Enkripsi

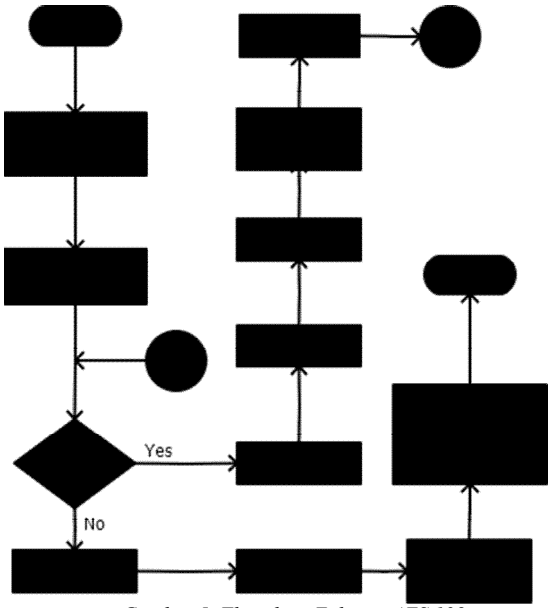
Flowchart dan Algoritma dibawah akan menjelaskan alur proses yang terjadi pada proses enkripsi



Gambar 4. Flowchart Proses Enkripsi

3.5. Flowchart Enkripsi AES 128

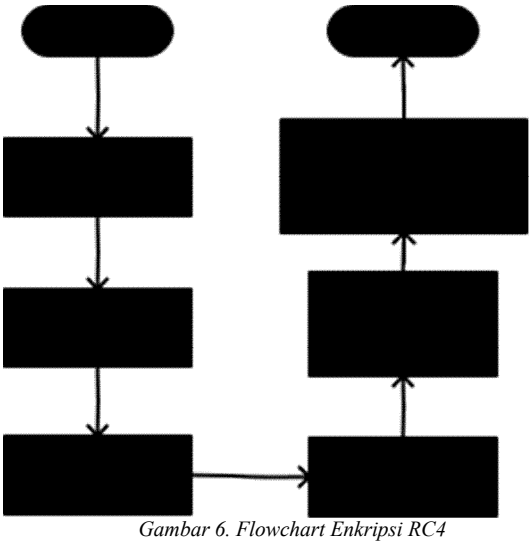
Flowchart dan Algoritma dibawah akan menjelaskan alur proses yang terjadi pada enkripsi AES 128:



Gambar 5. Flowchart Enkripsi AES 128

3.6. Flowchart Enkripsi RC4

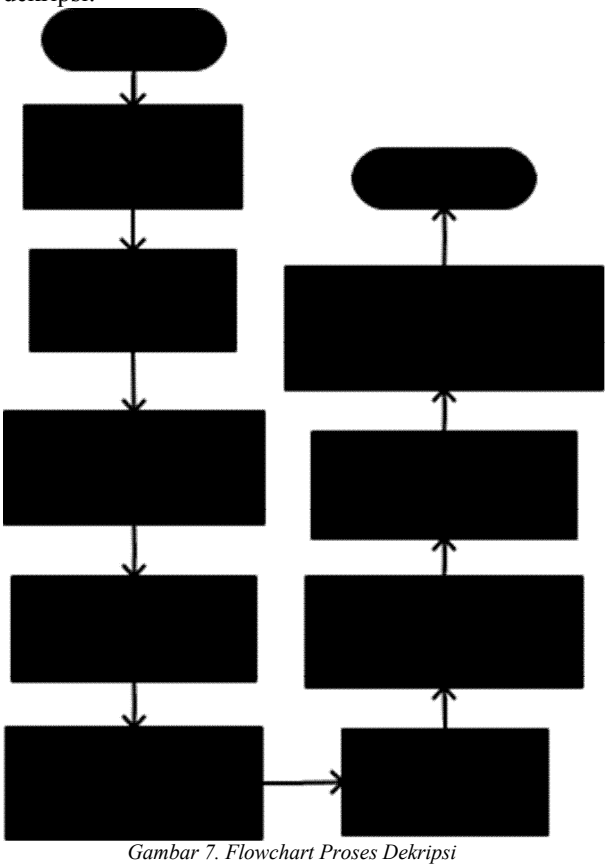
Flowchart dan Algoritma dibawah akan menjelaskan alur proses yang terjadi pada enkripsi RC4:



Gambar 6. Flowchart Enkripsi RC4

3.7. Flowchart Proses Dekripsi

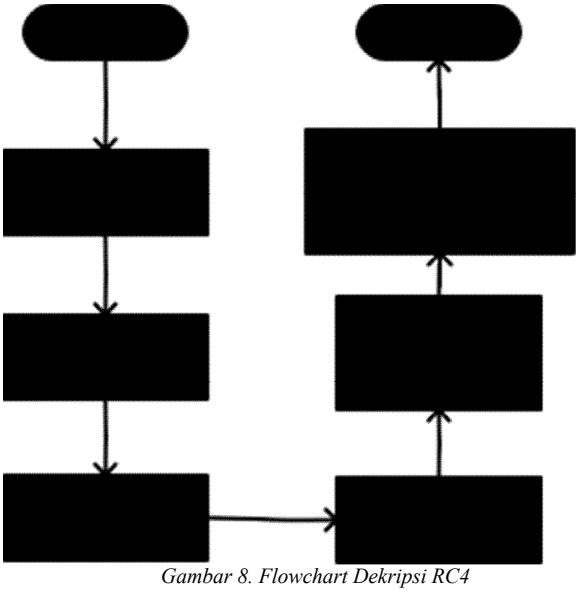
Flowchart dan Algoritma dibawah akan menjelaskan alur proses yang terjadi pada proses dekripsi:



Gambar 7. Flowchart Proses Dekripsi

3.8. Flowchart Dekripsi RC4

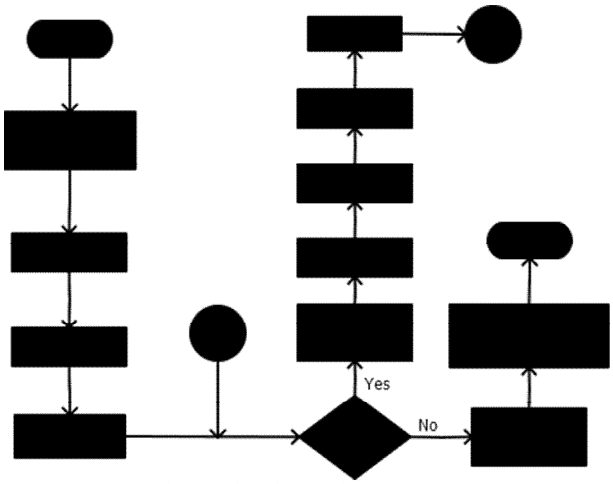
Flowchart dan Algoritma dibawah akan menjelaskan alur proses yang terjadi pada dekripsi RC4:



Gambar 8. Flowchart Dekripsi RC4

3.9. Flowchart Dekripsi AES 128

Flowchart dan Algoritma dibawah akan menjelaskan alur proses yang terjadi pada dekripsi AES 128:



Gambar 9. Flowchart Dekripsi AES 128

4. HASIL DAN PEMBAHASAN

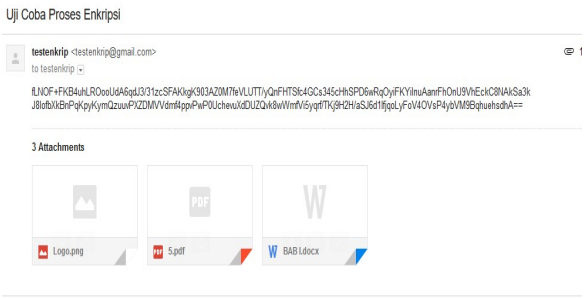
4.1. Uji Coba Proses Enkripsi

Uji coba proses enkripsi merupakan pengujian untuk merubah *plaintext* menjadi *ciphertext*. Gambar dibawah ini menampilkan pesan dan file lampiran sebelum dan sesudah dikirim dan dienkripsi.

Berikut ini adalah tampilan pesan sebelum dikirim dan dienkripsi menggunakan aplikasi kriptografi.

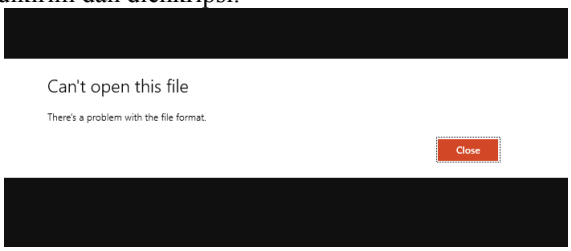
Gambar 10. Tampilan Pesan Sebelum Dienkripsi

Berikut ini adalah tampilan pesan sesudah dikirim dan dienkripsi.



Gambar 11. Tampilan Pesan Setelah Dienkripsi

Berikut ini adalah tampilan lampiran sesudah dikirim dan dienkripsi.

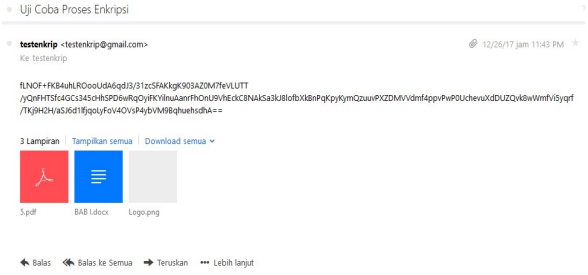


Gambar 12. Tampilan File Lampiran Setelah Dienkripsi

4.2. Uji Coba Proses Dekripsi

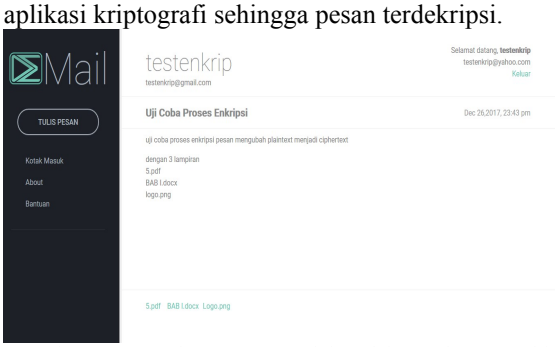
Uji coba proses dekripsi merupakan pengujian untuk merubah *ciphertext* menjadi *plaintext*.

Berikut ini adalah tampilan pesan jika tidak menggunakan aplikasi kriptografi sehingga pesan tidak terdekripsi.



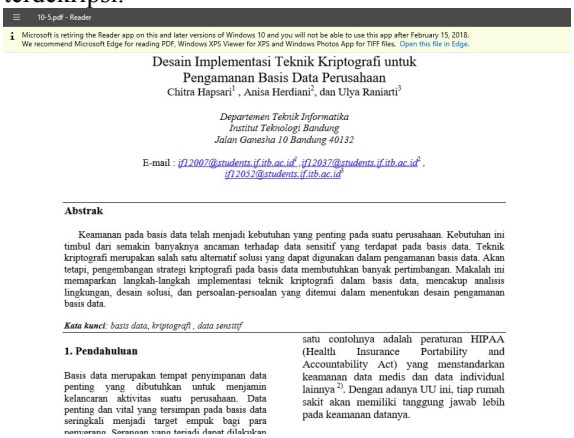
Gambar 13. Tampilan Pesan

Berikut ini adalah tampilan pesan menggunakan aplikasi kriptografi sehingga pesan terdekripsi.



Gambar 14. Tampilan Pesan Sesudah Didekripsi dengan Aplikasi

Berikut ini adalah tampilan lampiran yang telah terdekripsi.


10-5.pdf - Reader

Microsoft is retiring the Reader app on this and later versions of Windows 10 and you will not be able to use this app after February 15, 2018. We recommend Microsoft Edge for reading PDF, Windows XPS Viewer for XPS and Windows Photos App for TIFF files. Open this file in Edge.

Desain Implementasi Teknik Kriptografi untuk Pengamanan Basis Data Perusahaan

Chitra Hapsari[1] , Anisa Herdiani[2], dan Ulya Raniarti[3]

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if12007@students.if.itb.ac.id[1] , if12037@students.if.itb.ac.id[2] , if12052@students.if.itb.ac.id[3]

Abstrak

Keamanan pada basis data telah menjadi kebutuhan yang penting pada suatu perusahaan. Kebutuhan ini timbul dari semakin banyaknya ancaman terhadap data sensitif yang terdapat pada basis data. Teknik kriptografi merupakan salah satu alternatif solusi yang dapat digunakan dalam pengamanan basis data. Akan tetapi, pengembangan strategi kriptografi pada basis data membutuhkan banyak pertimbangan. Makalah ini memaparkan langkah-langkah implementasi teknik kriptografi dalam basis data, mencakup analisis lingkungan, desain solusi, dan persoalan-persoalan yang ditemui dalam menentukan desain pengamanan basis data.

***Kata kunci**: basis data, kriptografi , data sensitif*

1. Pendahuluan

Basis data merupakan tempat penyimpanan data penting yang dibutuhkan untuk menjamin kelancaran aktivitas suatu perusahaan. Data penting dan vital yang tersimpan pada basis data seringkali menjadi target empuk bagi para penyerang. Serangan yang terjadi dapat dilakukan satu contoluya adalah peraturan HIPAA (Health Insurance Portability and Accountability Act) yang menstandarkan keamanan data medis dan data individual lainnya [2]. Dengan adanya UU ini, tiap rumah sakit akan memiliki tanggung jawab lebih pada keamanan datanya.

Gambar 15. Tampilan File Lampiran Sesudah Didekripsi Dengan Aplikasi

4.3. Hasil Uji Coba Proses Enkripsi

Dalam tabel ini akan membahas mengenai perbandingan hasil enkripsi dan dekripsi.

Tabel 2. Tabel Hasil Uji Coba Proses Enkripsi isi Pesan

No	Plaintext	Kunci	Ciphertext
1	uji coba proses enkripsi pesan mengubah plaintext menjadi ciphertext dengan 3 lampiran 5.pdf BAB I.docx logo.png	Uji Coba Proses Enkripsi	fLNOF+FKB4uhLROooUdA6qdJ3/31zcSFAKkgK903AZ0M7feVLUTT/yQnFHTSfc4GCs345cHhSPD6wRqOyiFKYilnuAanrFhOnU9VhEckC8NAkSa3kJ8lofbXkBnPqKpyKymQzuuvPXZDMVVdmf4ppvPwP0UchevuXdDUZQvk8wWmfVi5yqrf/TKj9H2H/aSJ6d1lfjqoLyFoV4OVsP4ybVM9BqhuehsdhA==
2	Jangan mudah putus asa, Tugas Akhir harus selesai.	Tetap semangat	aO69CXoBlNPp4vc4+M2YTgPuR/GY83PQjMlw0K8zzmEap2IpnO3B+HM+aUQolx1PfSo3nJ
	Semangat!!		ZnxCtCwnfrAdZNQpRw1g3/Z2/J51026i9kWh9M
3	1411500331 Ahmad Galih Pramudito Fakultas Teknologi Informasi, Teknik Informatika	Ahmad Galih Pramudito	mwmanpis9qkJgfd9cDginappavGBjpTlFF7grtU5lSWehyNs9F1P4KaqJr5wyco46ecUC1vDzbSkmw0A4Dqdh5ZBZAeXBAXoNl4+/TJ8Vl70dTeDg5NNxd0x3EiSz5QIW986

Tabel 3. Tabel Hasil Uji Coba Proses Enkripsi File Lampiran

No	Nama	Ukuran	Waktu
1	5.pdf, BAB I.docx, Logo.png	120 kb	7.71 sec
2	PDF.pdf, Word.docx	148 kb	5.4 sec
3	Edited.xlxs	140 kb	8.01 sec

4.4. Hasil Uji Coba Proses Dekripsi

Tabel 4. Tabel Hasil Uji Coba Proses Dekripsi Isi Pesan

No	Ciphertext	Kunci	Plaintext
1	fLNOF+FKB4uhLROooUdA6qdJ3/31zcSFAKkgK903AZ0M7feVLUTT/yQnFHTSfc4GCs345cHhSPD6wRqOyiFKYilnuAanrFhOnU9VhEckC8NAkSa3kJ8lofbXkBnPqKpyKymQzuuvPXZDMVVdmf4ppvPwP0UchevuXdDUZQvk8wWmfVi5yqrf/TKj9H2H/aSJ6d1lfjqoLyFoV4OVsP4ybVM9BqhuehsdhA==	Uji Coba Proses Enkripsi	uji coba proses enkripsi pesan mengubah plaintext menjadi ciphertext dengan 3 lampiran 5.pdf BAB I.docx logo.png
2	aO69CXoBlNPp4vc4+M2YTgPuR/GY83PQjMlw0K8zzmEap2IpnO3B+HM+aUQolx1PfSo3nJZnxCtCwnfrAdZNQpRw1g3/Z2/J51026i9kWh9M	Tetap semangat	Jangan mudah putus asa, Tugas Akhir harus selesai. Semangat!!
3	mwmanpis9qkJgfd9cDginappavGBjpTlFF7grtU5lSWehyNs9F1P4KaqJr5wyco46ecUC1vDzbSkmw0A4Dqdh5ZBZAeXBAXoNl4+/TJ8Vl70dTeDg5NNxd0x3EiSz5QIW986	Ahmad Galih Pramudito	1411500331 Ahmad Galih Pramudito Fakultas Teknologi Informasi, Teknik Informatika

No	Ciphertext	Kunci	Plaintext
1	fLNOF+FKB4uhLROooUdA6qdJ3/31zcSFAKkgK903AZ0M7feVLUTT/yQnFHTSfc4GCs345cHhSPD6wRqOyiFKYilnuAanrFhOnU9VhEckC8NAkSa3kJ8lofbXkBnPqKpyKymQzuuvPXZDMVVdmf4ppvPwP0UchevuXdDUZQvk8wWmfVi5yqrf/TKj9H2H/aSJ6d1lfjqoLyFoV4OVsP4ybVM9BqhuehsdhA==	Uji Coba Proses Enkripsi	uji coba proses enkripsi pesan mengubah plaintext menjadi ciphertext dengan 3 lampiran 5.pdf BAB I.docx logo.png
2	aO69CXoBlNPp4vc4+M2YTgPuR/GY83PQjMlw0K8zzmEap2IpnO3B+HM+aUQolx1PfSo3nJZnxCtCwnfrAdZNQpRw1g3/Z2/J51026i9kWh9M	Tetap semangat	Jangan mudah putus asa, Tugas Akhir harus selesai. Semangat!!
3	mwmanpis9qkJgfd9cDginappavGBjpTlFF7grtU5lSWehyNs9F1P4KaqJr5wyco46ecUC1vDzbSkmw0A4Dqdh5ZBZAeXBAXoNl4+/TJ8Vl70dTeDg5NNxd0x3EiSz5QIW986	Ahmad Galih Pramudito	1411500331 Ahmad Galih Pramudito Fakultas Teknologi Informasi, Teknik Informatika

Tabel 5. Tabel Hasil Uji Coba Proses Dekripsi File

No	Ciphertext	Kunci	Plaintext
1	fLNOF+FKB4uhLROooUdA6qdJ3/31zcSFAKkgK903AZ0M7feVLUTT/yQnFHTSfc4GCs345cHhSPD6wRqOyiFKYilnuAanrFhOnU9VhEckC8NAkSa3kJ8lofbXkBnPqKpyKymQzuuvPXZDMVVdmf4ppvPwP0UchevuXdDUZQvk8wWmfVi5yqrf/TKj9H2H/aSJ6d1lfjqoLyFoV4OVsP4ybVM9BqhuehsdhA==	Uji Coba Proses Enkripsi	uji coba proses enkripsi pesan mengubah plaintext menjadi ciphertext dengan 3 lampiran 5.pdf BAB I.docx logo.png
2	aO69CXoBlNPp4vc4+M2YTgPuR/GY83PQjMlw0K8zzmEap2IpnO3B+HM+aUQolx1PfSo3nJZnxCtCwnfrAdZNQpRw1g3/Z2/J51026i9kWh9M	Tetap semangat	Jangan mudah putus asa, Tugas Akhir harus selesai. Semangat!!
3	mwmanpis9qkJgfd9cDginappavGBjpTlFF7grtU5lSWehyNs9F1P4KaqJr5wyco46ecUC1vDzbSkmw0A4Dqdh5ZBZAeXBAXoNl4+/TJ8Vl70dTeDg5NNxd0x3EiSz5QIW986	Ahmad Galih Pramudito	1411500331 Ahmad Galih Pramudito Fakultas Teknologi Informasi, Teknik Informatika

5. KESIMPULAN

Setelah melewati tahap perancangan, penerapan/implementasi, dan pengujian pada aplikasi ini maka dapat disimpulkan bahwa:

a. Dengan adanya aplikasi ini, proses mengirim atau menerima *email* lebih aman.
b. Pesan tidak dapat terbaca jika tidak menggunakan aplikasi kriptografi.
c. Pesan yang didekripsi akan kembali seperti semula tanpa ada perubahan sedikitpun.
d. Kecepatan proses enkripsi dan dekripsi berbading lurus dengan ukuran pesan dan file lampiran, semakin besar ukuran pesan dan file lampiran maka proses enkripsi dan dekripsinya akan semakin lama.

Adapun saran yang mungkin diperlukan agar aplikasi ini dapat berjalan lebih baik lagi antara lain:

a. Perlu adanya pengembangan pada algoritma untuk mengenkripsi dan mendekripsikan pesan sehingga keamanannya lebih terjamin.
b. Perlu adanya penambahan fitur seperti *forward email*, *reply email*, *folder trash*, dan *folder sent*.

DAFTAR PUSTAKA

[1] Stallings W., 1999, *Cryptography and Network Security Principles and Practice Second edition*. Prentice Hall, New Jersey, USA

[2] Hartono, B. (2004) 'Ruang Lingkup Kriptografi Untuk Mengamankan Data', *Jurnal Dinamika Informatika*, 9(2), pp. 1–8.

[3] Pabokory, F. N., Astuti, I. F. and Kridalaksana, A. H. (2015) 'Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard', *Jurnal Informatika Mulawarman*, 10(1), pp. 20–31.

[4] Alfred J.M., Paul C.O., and Scott A.V, 1997, *Handbook of Applied Cryptography*. CRC Press LLC, Florida, USA.

[5] Yuniati, V., Indriyanta, G. and C, A. R. (2009) 'Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jensis File', *Journal Informatika*, 5(1), pp. 22–31.

[6] Tulloh, A. R., Permanasari, Y. and Harahap, E. (2016) 'Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption sebagai agensi departemen perdagangan AS menetapkan sebuah standard kriptografi Standard (AES)', *Prosiding Matematika*, 2(2460–6464), pp. 118–125.

[7] Rahmawati, R. and Rahardjo, D. (2016) 'Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi grafi AES 128 BIT pada SMK PGRI 15 Jakarta', *Jurnal teknik Informatika dan Sistem Informasi*, 2(April), pp. 67–74.

[8] Fauzan, M., Purnomo, E., Priyono, W. A., Sari, S. N. and Wulandari, A. (2012) 'Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi Voice over Internet Protocol(VoIP)', *Jurnal EECCIS*, 6(2), pp. 183–188.

[9] Sutiono, A. P. (2011) 'Algoritma RC4 sebagai Perkembangan Metode Kriptografi', *Bandung: Institut Teknologi Bandung*.