IMPLEMENTASI KRIPTOGRAFI PADA FILE ATTACHMENT EMAIL MENGGUNAKAN ALGORITMA RIJNDAEL

Bakir[1], Hozairi[2]
[1] Program Studi Sistem Informasi, Universits Islam Madura, Pamekasan, Indonesia
[2] Program Studi Teknik Informatika, Universits Islam Madura, Pamekasan, Indonesia
bakir.madura@gmail.com, dr.hozairi@gmail.com

ABSTRAK

E-mail adalah media yang sering digunakan untuk mengirim pesan baik berupa informasi, laporan, pemberitahuan maupun berkas-berkas penting terutama melalui Attachcmen di e-mail. Dibalik manfaat tersebut terdapat bahaya yang tidak disadari oleh pengguna e-mail, yaitu penyadapan, ditambah dengan adanya *hacker* dan *cracker* yang mampu menembus keamanan suatu server e-mail sehingga dapat menyusup ke akun e-mail. Penerapan *kriptografi* merupakan sebuah solusi yang ditawarkan untuk mengatasi permasalahan mengenai keamanan data baik berupa teks maupun file, algoritma *kriptografi* cukup banyak diminati dan berkembang dengan pesat salah satunya adalah metode *Rijndael*. Rijndael adalah salah satu algoritma yang mempunyai kinerja sangat baik yang mampu bekerja dari berbagai sudut padang baik dari segi keamanan, kesederhanaan struktur dan fleksibilitas sehingga *Rijndael* terpilih sebagai pemenang dalam pemilihan Algoritma AES *(Advance Encryption Standart)* untuk menggantikan Algoritma DES *(Data Encryption Standart)*. Enkripsi e-mail menggunakan Algoritma Rijndael terbukti dapat menjaga kerahasiaan suatu data baik berupa teks maupun file, file yang terenkripsi tidak dapat terbaca kecuali mengetahui kunci untuk mendeskripsinya. Algoritma enkripsi rijndael terbukti dapat mempertahankan kerahasiaan file attachment pada email, file tidak akan terbaca kecuali dengan mendeskripsi nya terlebih dahulu menggunakan aplikasi ini..

Keyword : *e-mail, enkripsi, kriptografi, rijndael*

1. PENDAHULUAN

E-mail merupakan aplikasi yang ada pada awal terbentuknya sebuah internet digunakan untuk mengirimkan suatu pesan yang sangat cepat dan efisien. Seiring berjalannya waktu, e-mail menjadi sebuah aplikasi yang sering digunakan untuk mengirim pesan maupun berkas-berkas penting melalui attachcmen e-mail. Namun ada beberapa yang harus diwaspadai yang belum tentu kita ketahui bahwa e-mail sering terjadi penyadapan, merubah dan menjadikan e-mail itu tidak asli lagi dan hal ini sering terjadi di kalangan beberapa instansi di indonesia.

12 September 2014, Sebuah situs milik Rusia telah membeberkan ribuan bahkan jutaan kata sandi (*password*) kemudian pada tahun berikutnya 2015 komputer pribadi milik Presiden Amerika Serikat yaitu Barack Obama telah diserang hacker dan email rahasia milik Presiden Barack Obama dirsebar ke publik. Dengan demikian keamanan menjadi salah satu aspek yang sangat penting dalam penggunakan e-mail untuk mencegah jatuhnya data ke pihak-pihak lain yang tidak berkepentingan dan menjadi salah satu upaya pengamanan file attachment e-mail dari beberapa kejadian tersebut dapat dilakukan adalah metode kriptografi.

Keamanan menjadi suatu aspek yang sangat penting pada e-mail untuk mencegah jatuhnya data ke pihak-pihak lain yang tidak bertanggung jawab sehingga data tersebut disalah gunakan. Kemudian salah satu upaya pengamanan file attachment email yang dapat dilakukan adalah kriptografi.

Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, Saat ini terdapat berbagai algoritma penyandian dalam ilmu kriptografi, namun dalam hal ini penulis memilih Rijndael yang merupakan algoritma simetri yang hanya menggunakan satu kunci dalam proses enkripsi dan deskripsi file.

Sistem aplikasi yang dibangun untuk mengamankan e-mail yang akan dikirim oleh pengguna ke pengguna lainnya menggunakan algoritma rijndael untuk menjaga keamanan dan kerahasiaan suatu data baik berupa teks maupun file pada email.

2. TINJAUAN PUSTAKA

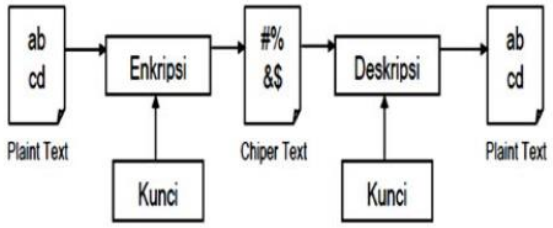
2.1. Kriptografi

Tercatat dalam sejarah bahwa kriptografi dipergunakan secara terbatas oleh bangsa kairo mesir pada empat ribu (4000) tahun lalu. Kriptografi berasal dari dua kata yaitu crypto dan graphy didalam sudut bahasa Crypto adalah rahasia (*secret*) sedangkan graphydapat bermakna tulisan (*write*) dengan ini kata Kriptografi (*Cryptography*) mempunyai arti adalah suatu ilmu seni untuk mengamankan pesan digital baik berupa tek maupun file hal ini dilakukan oleh Cryptographer. (Sadikin, 2012).

Orang yang telah melakukan sebuah enkripsi terhadap suatu pesan digital maka disebut Cryptographer. Kemudian yang melakukan sebuah pesan yang tidak dikunci dengan kata sandi disebut sebagai plaintext sedangkan pesan yang telah

dikunci dengan kata sandi maka hal tersebut merupakan sebuah algoritma kriptografi disebut sebagai chiphertext.

Proses untuk mengubah plaintext ke chipertext disebut encryption atau encipherment dan proses tersebut dapat mengubah chipertext ke plaintext disebut decryption atau decipherment. secara sederhana proses tersebut digambarkan pada gambar 1.



Gambar 1. *Proses Enkripsi dan Deskripsi*

Berdasarkan gambar diatas adalah proses engkripsi dan deskripsi untuk mengkonversikan plain text ke cipher text begitu juga proses sebaliknya dimana sebuah proses sistem tersebut dapat terdiri dari algoritma tertentu tergantung pada situasi dan kondisi sehingga sistem tersebut sesuai keinginan.

Algoritma kriptografi disebut juga cipher merupakan persamaan dari matematik yang akan digunakan dalam proses enkripsi dan deskripsi dimana semua proses tersebut diatur oleh satu atau lebih kunci kriptografi yg menjadin kunci tersebut secara umum dapat digunakan untuk memproses enkripsi dan dekripsi pada sebuah pesan digital yang tidak perlu identikpada sistem yang digunakan.

Kemudian proses enkripsi dan deskripsi secara matematis diterangkan sebagaimana berikut :

EK (M) = C
DK (C) = M

Keterangan :
EK : Enkripsi.
DK : Deskripsi.
M : Message.
C : Cipher.

Secara umum algoritma yang dapat digunakan untuk mengkriptografikan oleh orang yang ahli dan berpengalaman dalam bidang sebuah keamanan sistem data dan mungkin pernah membuka sebuah algoritma kriptografi tanpa sebuah bantua. (Sadikin, 2012).

Tujuan dari adanya enkripsi merupakan untuk meningkatkan sebuah keamanan sistem data tetapi juga berfungsi untuk melindungi data agar data tersebut tidak dapat dibaca oleh orang-orang yang tidak berhak serta mencegah agar orang-orang yang tidak bertanggung jawab atas penyalah gunaan data.

Adapun tujuannya dari sebuah sistem kriptografi yang akan dibangun adalah :
1. Confidentiality
2. Message Integrity
3. Non-repudiation
4. Authentication

2.2. Email dan Attachment Email

E-mail merupakan singkatan dari kata Electronic dan Mail sedangkan dalam bahasa indonesianya merupakan surat elektronik. email mempunyai fungsi sebagai sarana untuk mengirim surat atau pesan digital yang menggunakan jasa jaringan intenet dengan email kita membutukan beberapa menit untuk mengirim pesan kita sampai pada tujuanny.

E-mail mulai dipakai pada tahun 1960-an diamana pada saat itu juga internet belum terbentuk dengan baik seperti sekarang dan hanyalah berupa kumpulan (*mainframe*). Sedangkan pada tahun 1980-an, e-mail sudah bisa dinikmati secara umum sampai saat ini banyak perusahaan pos di berbagai negara menurun labanya disebabkan masyarakat sudah beralih pada email dan tidak memakai jasa pos kembali.

Attachment meruapakann fasilitas yang tersedia pada suatu situs yang memberikan fasilitas email sehingga dapat mengirimkan dokumen baik berupa tulisan, musik, gambar dan video serta data lainnya kemudian diupload menggunakan fasilitas email.

Dengan adanya attachment pada email sangat memudahkan kita kalau misalnya mau bertukar informasi atau mau mengirim data dokumen penting dengan jarak jauh sehingga kita membutuhkan biaya yang lebih mahal dan waktu yang lebih lama.

e-mail bukan hanya untuk mengirim pesan digital maupun berkas akan tetapi dapat dimanfaatkan berupa apapun yang berhubungan dengan internet seperti mendaftar facebook, twitter, blogger dan lain-lainnya yang pasti memerlukan e-mail utuk mendaftar dan validasi pengguna.

Keamanan data e-mail tidaklah terjamin keamannya dan apapun selalu ada risiko yang harus kita tempuh karena emial sifatnya terbuka untuk umum, bahkan semua isinya juga dapat dibaca oleh orang lain hal ini yang menyebabkan email keamanannya juga kurang menjamin karena harus melewati banyak server atau dari hosting ke hosting lainnya sebelum sampai di tujuan.

2.3. Algoritma Rijndael

Rijndael tahun 1972-1974 National Bureau of Standards (sekarang dikenal dengan nama National Institute of Standards and Technology, NIST) telah menerbitkan sebuah permintaan kepada masyarakat untuk pembuatan standar enkripsi. Pada saat itu adalah DES (Data Encryption Standard), yang banyak digunakan di dunia yang diminta untuk menyederhanakan. DES (Data Encryption Standard)

merupakan sebuat algoritma cryptography simetris dengan panjang key 56 bit dan blok data 64 bit.

Dengan semakin majunya teknologi para cryptografer merasakan bahwa panjang kunci yang digunakan untuk DES terlalu pendek untuk menjada keamanan data sehingga algoritma DES yang digunakan pada saat itu tidak dianggap tidak memenuhi syarat.

Untuk mengatasi hal itu, akhirnya muncul triple DES yang akhirnya NIST mengadakan kompetisi untuk standar cryptography dengan varian terbaru, yang dinamakan AES (Advanced Encryption Standard). (Sianturi, 2013).

Persyaratan AES (Advanced Encryption Standard) adalah sebagai berikut :

1. Algoritma harus dipublikasikan secara umum.
2. Algoritma harus simetris block cipher.
3. Algoritma harus cepat dan tepat.
4. Algoritma harus terdiri dari data 128 bit.
5. Algoritma harus fleksibel 128-256 bit.

Dari hasil seleksi yang dilakukan oleh NIST, akhirnya NIST memilih 5 finalis AES, yaitu : Mars (IBM Amerika), RC6 (RSA Corp, Amerika), Rijndael (Belgia), Serpent (Israel, Norwegia dan Inggris), dan Twofish (Counterpane Amerika). Kompetisi ini yang akhirnya dimenangkan oleh Rijndael dan secara resmi diumumkan oleh NIST pada tahun 2001. Sejak saat itu Algoritma Rijndael berkembang dan sering disebut juga dengan AES. (Sadikin, 2012).

Rijndael diambil dari nama pembuatnya Dr. Vincent Rijmen dan Dr. Joan Daemen. Rijndael terpilih sebagai pemenang algoritma yang paling aman dan memiliki keseimbangan dalam berbagai paltform software dan hardware.

2.4. Representasi Data

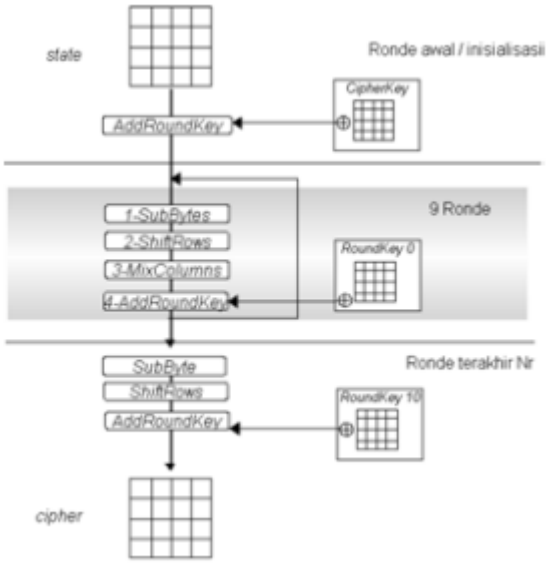
Proses Input output dari sebuah algoritma Rijndael terdiri dari data 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok tersebut juga disebut sebagai blok data dan plaintext yang nantinya akan dienkripsi menjadi ciphertext. Cipher key dari Rijndael terdiri dari key dengan panjang 128-256 bit.

Urutan bit diberi dari nomor urut dari 0 sampai dengan n-1 dimana n adalah nomor urutan. Urutan data 8 bit secara berurutan disebut sebagai byte dimana byte ini adalah unit dasar dari operasi yang akan dilakukan pada blok data.

Operasi algoritma Rijndael dapat dilakukan pada suatu state, sedangkan dimana state sendiri merupakan suatu array byte dua dimensi yang akan diproses. Setiap state pasti jumlah baris yang tetap yaitu 4 (empat) baris, sedangkan jumlah kolom tergantung dari besarnya blok data. Untuk baris pada state mempunyai indeks nomor baris (row) (r) dimana $0 \leq r < 4$, sedangkan kolom (colums) mempunyai indeks nomor kolom (c) dimana $0 \leq c <$ Nb. Nb sendiri adalah besarnya blok data dibagi 32.

2.5. Algoritma Engkripsi Rijndael

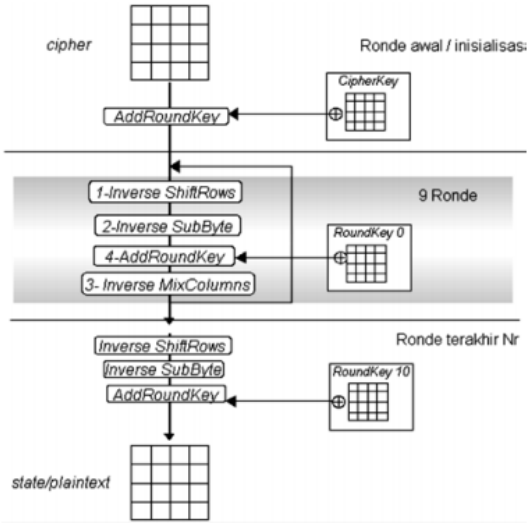
Proses enkripsi pada sebuah algoritma Rijndael terdiri dari empat jenis transformasi bytes diantara SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input telah dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr.



Gambar 2. Proses Enkripsi

2.6. Algoritma Diskripsi Rijndael

Transformasi cipher dapat diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse kemudian cipher dapat mudah dipahami untuk algoritma Rijndael. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.



Gambar 3. Proses Diskripsi

3. METODE PENELITIAN

3.1. Pengumpulan Data

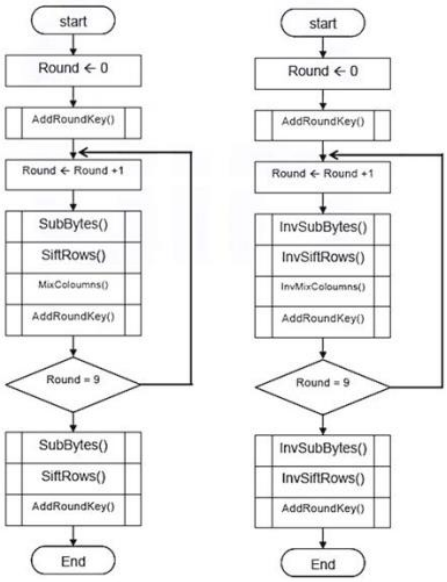
Pada tahap awal dalam penelitian ini adalah pengumpulan data yang akan digunakan diantara media cetak maupun melalui situs-situs berita online dengan melakukan pengamatan dan mencari informasi seputar permasalahan yang berkaitan dengan keamanan e-mail, hal ini bertujuan untuk memperoleh dan penjelasan mengenai data dan informasi yang dibutuhkan serta dengan mempelajari beberapa referensi yang ada, buku, jurnal dan ebook yang berkaitan dengan objek penelitian.

Adapun metode pengumpulan data yang digunakan dalam penelitian ini adalah dengan menggunakan studi pustaka dan observasi. Studi pustaka digunakan dengan membaca dan mempelajari referensi yang ada, buku-buku, ebook, serta mencari referensi tambahan dari internet. Document yang temasuk didalamnya yaitu penelitian-penelitian terdahulu, buku, artikel dan jurnal yang berkaitan dengan objek penelitian.

Observasi adalah proses mengumpulkan data dengan melakukan pengamatan dan mencari informasi seputar permasalahan yang berkaitan dengan keamanan e-mail, hal ini bertujuan untuk memperoleh kebenaran dan penjelasan mengenai data-data dan informasi yang dibutuhkan dan melakukan pengujian.

3.2. Perancangan Sistem

Pada tahapan ini dilakukan dilakukan perancangan sistem dan aplikasi ini menggunakan metode enkripsi Rijndael. Pada proses enkripsi, file dienkripsi menggunakan metode Rijndael dengan sebuah kunci yang nantinya kunci tersebut digunakan untuk deskripsi file.

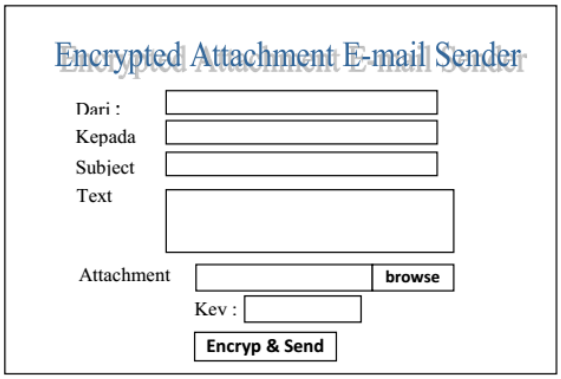


Gambar 4. Flowchart Algoritma *Rijndael*

Pada proses deskripsi, file terenkripsi terlebih dahulu di download ke komputer dan dengan menggunakan aplikasi ini pada bagian deskripsi, file tersebut dapat dkembalikan ke file asli dengan menggunak kunci yang di gunakan pada proses enkripsi sebelumnya.

3.3. Perancangan User Interface

Perancangan Interface memberikan fasilitas komonikasi antara pemakai (user) dengan sistem memberikan berbagai fasilitas informasi dan berbagai keterangan yang bertujuan untuk membantu penelusuran masalah sampai ditemukan solusi.



Gambar 5. Rancangan User Interface

Rancangan yang akan dibangun akan diimplementasikan dalam bentuk soucecode dalam bahasa visual basic kemudian dilakukan pengujian terhadap aplikasi yang telah dibuat, pada pengujian terhadap aplikasi ini dilakukan dengan pengujian *black-box* yaitu suatu pengajuan yang berfokus pada persyaratan fungsional perangkat lunak dan Berdasarkan hasil pengujian selanjutnya akan diambil kesimpulan mengenai kinerja program, kinerja algoritma dan hasil enkripsi attachment serta hasil deskripsi file attachment.

3.4. Implentasi dan Pengujian Sistem

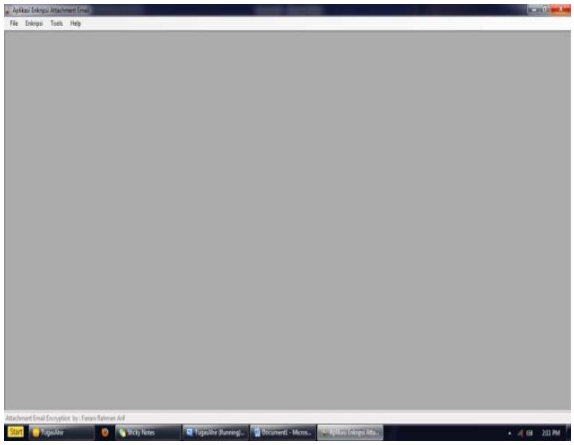
Setelah rancangan yang akan dibangun selesai maka akan selanjutnya diimplementasikan dalam bentuk *soucecode* dengan menggunakan bahasa pemrograman visual basic.

Kemudian pada tahapan berikutnya dilakukan pengujian terhadap aplikasi yang telah dibuat, pada pengujian terhadap aplikasi ini akan menggunakan pengujian *black-box* yaitu suatu pengajuan yang berfokus pada persyaratan fungsional perangkat lunak. Berdasarkan hasil pengujian selanjutnya akan diambil beberapa kesimpulan mengenai kinerja aplikasi ini dan kinerja algoritma serta hasil enkripsi attachment dan hasil deskripsi file attachment.

4. HASIL PENELITIAN

4.1. Simulasi

Proses simulasi dengan menjalankan program secara bertahap, simulasi dilakukan dengan beberapa tahap dan kriteria, yaitu uji coba program, uji coba server email dan Uji coba Enkripsi File. Pada aplikasi menu dan kode program selesai dibuat, maka program dieksekusi sehingga hasilnya seperti pada gambar 6.



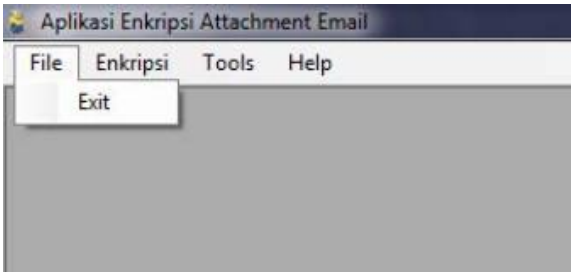
Gambar 6. Tampilan Menu Utama

4.2. Pengujian Sistem

Pada saat aplikasi dijalankan, aplikasi akan mengecek adanya koneksi internet, jika tidak terdapat jaringan, aplikasi ini akan memberikan pemberitahuan bahwa tidak ada koneksi. Hal ini bertujuan untuk memberikan peringatan awal sebelum melakukan pengiriman email.

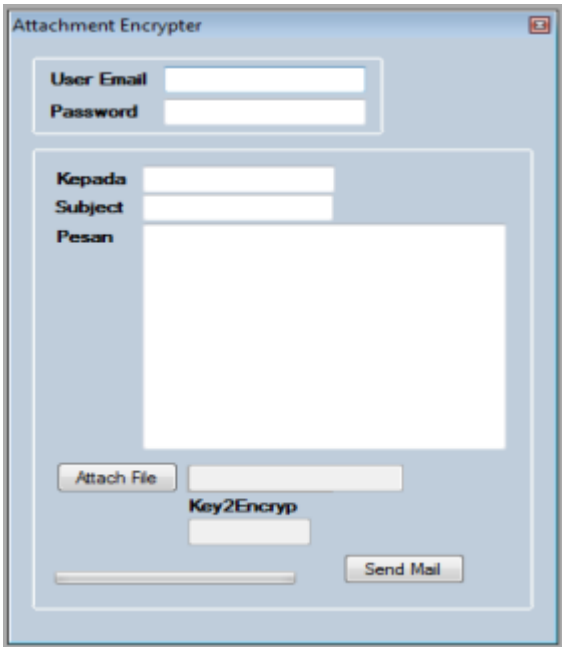
Gambar 7. Pesan Error Koneksi Internet

Setelah dapat dipastikan koneksi internet tersambung maka terdapat beberapa sub menu dari aplikasi ini seperti terlihat pada Gambar 7, menu enkripsi memiliki sub menu attachment enkripter, enkripsi file dan deskripsi file. Menu tools merupakan menu tambahan pada aplikasi ini, berisi email browser dan email sender (tanpa enkripsi). Terahir menu help, berisi sub menu tentang pengertian kriptografi dan algoritma rijndael.



Gambar 8. Menu Pada Aplikasi

Selanjutnya dalah menu Enkripsi pada menu ini berfungsi untuk mengkripsi file attachment email sebagaimana yang terdapat pada Gambar 9.



Gambar 9. Form Attachment Enkripter

Pada Gambar 8 menjelaskan menu form utama dalam aplikasi ini, karena tujuan penelitian ini terdapat pada form ini, yaitu mengenkripsi file *attachment* email. Terdapat dua bagian pada form *attachment enkripter*, yaitu bagian email account dan isi email. Email account yaitu tempat pengguna memasukkan account email beserta password nya untuk kemudian digunakan dalam proses login pada email server nya. Isi email terdiri dari email tujuan, judul, isi dan attachment. Pada bagian attachment ditambahkan code menggunakan algoritma *rijndael* untuk mengenkripsi file attachment sebelum dikirim ke server email menuju alamat yang dituju.

Pada form *Attachment Enkripter* menggunakan dua jenis pemprograman, yaitu email sender dan enkripsi file. Dengan mengaktifkan attachment, code untuk enkripsi akan aktif dan meminta key(sandi) untuk mengenkripsi file attachment. Setelah penggunamenekan tombol send, kedua program ini akan bergantian bekerja dan file attachment terenkripsi akan dikirim ke alamat email tujuan nya kemudian dilanjutkan proses pengiriman email yang

dienkripsi menggunakan aplikasi seperti pada Gambar 10.

Gambar 10. Proses Pengisian Form Attachment Enkripter

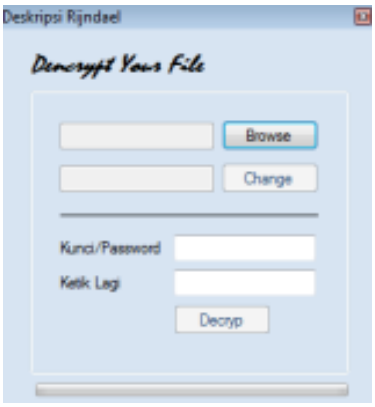
Selanjutnya pengguna mengisikan data berupa username dan password account email mereka, kemudian aplikasi akan menentukan email tersebut akan dikirim menggunakan server sesuai teks belakang dari username nya.

Gambar 11. Pesan pengiriman berhasil

Selanjutnya, file terenkripsi akan ditambahkan ke attachment e-mail kemudian dikirim ke alamat tujuan nya dan attachment pada e-mail tersebut terenkripsi sesuai harapan, terbukti dengan berubahnya ekstensi file yang dikirim menjadi .fra dan file ini dapat didownload untuk kemudian di deskripsi menggunakan aplikasi ini pada bagian deskripsi file. File yang di enkripsi setelah di download akan seperti gambar dibawah ini.

Gambar 12. File Terenkripsi Berekstensi *.fra

Pada Form deskripsi file adalah form yang sangat penting pada aplikasi ini, karena pada tanpa form deskripsi, file yang dienkripsi tidak akan dapat dikembalikan seperti semula. Pada form ini pengguna diminta memasukkan file yang akan di deskripsi dan memasukkan kata sandi sesuai dengan pada saat di enkripsi, file terenkripsi tidak dapat dikembalikan. bahkan ada beberapa kasus kesalahan penggunaan kata sandi akan membuat file tersebut menjadi tidak dapat dikembalikan ke file asli.



Gambar 13. Deskripsi File

Berdasarkan hasil uji coba aplikasi ini semua file yang di uji coba berhasil di *enkripsi* dengan baik dan terkirim ke email tujuan, serta file terenkripsi tidak bertambah ukurannya sebagaimana tabel 1.

Tabel 1. Hasil Pengujian

Nama File	Ukuran File	Nama File	Ukuran File
ilmu komp_aes.pdf	785 KB	ilmu komp_aes_pdf.fra	785 KB
Keamanan Komputer-02.pptx	4.27 MB	Keamanan Komputer-02_pptx.fra	4.27 MB
Keamanan Informasi.docx	1.10 MB	Keamanan Informasi_docx.fra	1.10 MB
SISTEM DIGITAL tugas.xls	188 KB	SISTEM DIGITAL tugas_xls.fra	188 KB
config.txt	85.6 KB	config_txt.fra	85.6 KB
logo uim.jpg	14.2 KB	logo uim_jpg.fra	14.2 KB
The Last Naruto the Movie (2014).MP4	337 MB	The Last Naruto the Movie (2014)_MP4.fra	337 MB
Burger Islan.rar	32.7 MB	Burger Island_rar.fra	32.7 MB
smadav1025.exe	1.24 MB	smadav1025_exe.fra	1.24 MB

Berdasarkan hasil pengujian yang dilakukan secara *blackbox* mandiri, maka dapat disimpulkan bahwa aplikasi berjalan dengan baik pada pc/laptop. Uji coba server email berjalan dengan baik dan Proses Enkripsi maupun Deskripsi tidak ada error yang terjadi ketika program dijalankan dan file

terenkripsi berhasil kembali ke bentuk semula tanpa merusak file asli. Penelitian ini telah berhasil menerapkan enkripsi data untuk meningkatkan keamanan data tersebut, penelitian ini bisa dikembangkan untuk meningkatkan keamanan data yang bersifat rahasia khususnya data intelijen atau data rahasia sebuah perusahaan.

5. KESIMPULAN

Berdasarkan hasil uji coba aplikasi pada pembahasan yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

1. Berdasarkan hasil pengujian, algoritma *rijndael* mampu melakukan *enkrpsi* terhadap file doc, docx, xls, xlsx, ppt, pptx pdf, jpg dan txt dengan ukuran file berkisar antara 1KB-25MB secara baik, terbukti file *attachment* tidak dapat dibaca tanpa kunci yang benar dan algoritma yang sama, meskipun type file nya diketahui dan dikembalikan ke bentuk file semula.
2. Proses *Enkripsi* dan *Deskripsi* berjalan sesuai tujuan dan target, file yang di *enkripsi* tidak dapat dibaca dan file hasil *deskripsi* berhasil kembali seperti semula.
3. Pengiriman Email, baik attachment yang terenkripsi maupun yang attachment tanpa enkripsi dapat berjalan dengan baik, teks maupun file terkirim sempurna ke email tujuan.

DAFTAR PUSTAKA

Arius, D. (2006). Pengantar Ilmu Kriptografi. Yogyakarta: AndiPublisher.

Justian, O. E. (2012). Aplikasi Pembelajaran Kriptografi Klasik Dengan Visual basic.Net. 49-55.

Komputer, W. (2009). Membangun Aplikasi Toko dengan Visual Basic 2008. Yogyakarta: AndiPublisher.

Kurniawan, W. (2007). Jaringan Komputer. Yogyakarta: AndiPublisher.

Zakaria, Andri. "Securing E-Mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices", Faculty of Information Technology, University of Budi Luhur, Jakarta, 2012.

Sadikin, R. (2012). Kriptografi Untuk Keamanan Jaringan. Yogyakarta: AndiPublisher.

Alvin Susanto.___. Penerapan Teori Chaos di Dalam Kriptografi. Jurnal Teknik Informatika

Sianturi, F. A. (2013). Perancangan Aplikasi Pengamanan Data Dengan Kiptografi Advanced Encryption Standart (AES). Pelita Informatika Budi Darma, 42-46.

Dwi Lestari dan Zaki Riyanto.(2012). Suatu Algoritma Kriptografi Stream Cipher Berdasarkan Fungsi Chaos. Prosiding,Seminar Nasional. Yogyakarta : FMIPA UNY.

Menezes, Oorchshot,& Vanstone. (1996).Handbook of Applied Cryptography. Florida: CRC Press.

Dimas Ridwan W.(2014).Aplikasi Aljabar Min-Plus untuk Mengamankan Informasi Rahasia. Skripsi. Yogyakarta : Universitas Negeri Yogyakarta.

Caroline, Maureen Linda. “Perbandingan Algoritma Kriptografi Kunci Publik RSA, Rabin dan ElGamal”. Program Studi Teknik Informatika Institut Teknologi Bandung, Bandung, 2011.

Sarwoko. “Implementasi Kriptografi Algoritma DES dan RSA dalam Penyandian Data”. Program Studi Sistem Informasi Universitas Ahmad Dahlan, Yogyakarta, 2009.

Wahyuni, Ana. “Aplikasi Kripotgrafi untuk Pengamanan E-Dokumen dengan Metode Hybrid : Biometrik Tanda Tangan dan DSA (Digital Signature Algorithm)”. Program Studi Magister Sistem Informasi Universitas Diponegoro, Semarang, 2011.

Yulius, Afdal. "Rancang Bangun Aplikasi Enkripsi File Menggunakan Algoritma Rijndael", Jurusan Teknik Informatika Universitas Islam Negara Malang, Malang, 2008.