Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake

Fifit Alfiah[1]*, Rio Sudarji[2]†, Dzakwan Taqiyyuddin Al Fatah [1]‡

[1,3]Universitas Raharja, Jl. Jenderal Sudirman No.40, Cikokol, Kec. Tangerang, Kota Tangerang, Banten 15117

[2]Universitas Budi Luhur, Jl. Ciledug Raya, RT.10/RW.2, Petukangan Utara, Kec. Pesanggrahan, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12260

Abstrak

Kemajuan teknologi saat ini telah berpengaruh pada hampir semua aspek kehidupan manusia, yang dapat memudahkan untuk melakukan pertukaran data secara cepat, tak terkecuali dalam hal berkomunikasi. Namun dalam melakukan pertukaran data tersebut masih sangat kurang disadari. Salah satu dampak negatifnya yaitu adanya pencurian data. Oleh karena itu aspek keamanan dalam pertukaran informasi dan penyimpanan data sangatlah penting. Terutama pada bidang retail otomotif, dimana banyak data yang penting dan bersifat rahasia seperti data identitas customer, dan laporan keuangan. Karena begitu pentingnya data tersebut, maka dibutuhkan suatu metode yang dapat menjaga kerahasiaan data dan metode yang dimaksud adalah kriptografi. Algoritma yang digunakan adalah algoritma ElGamal. Algoritma ini merupakan bagian dari algoritma asimetris, proses enkripsi dan dekripsi masing-masing memiliki kunci yang berbeda. Tujuan dari penelitian ini untuk menemukan cara mengimplementasikan algoritma kriptografi ElGamal ke dalam bentuk aplikasi yang nyata serta menghasilkan aplikasi pengamanan data berbasis desktop yang mudah dimengerti dan digunakan oleh user. Penelitian ini menggunakan metode Pengumpulan data dan Pengembangan. Hasil dari penelitian ini akan diimplementasikan dalam sebuah program aplikasi menggunakan Bahasa pemrograman berbasis java desktop memberikan kemudahan untuk semua orang yang ingin mengamankan file penting. Pada aplikasi ini user harus membuat public key sebelum proses enkripsi dan private key sebelum proses dekripsi pada file.

Keywords: Kriptografi, Asimetris, ElGamal, Enkripsi, Dekripsi

*E-mail: fifitalfiah@raharja.info

†E-mail: 1411500893@student.budiluhur.ac.id

‡E-mail: dzakwan@raharja.info

1. Pendahuluan

Perkembangan teknologi computer saat ini telah mengalami tahapan kemajuan yang sangat pesat dan sudah menjadi suatu kebutuhan. Semakin tinggi tingkat teknologi komputer, semakin tinggi ancaman yang mengancam keamanan pengguna komputer. Salah satu dampak negatif dalam perkembangan teknologi adalah adanya pencurian data maka aspek yang di takuti oleh para pengguna jaringan komunikasi. Dengan adanya pencu- rian data maka aspek keamanan data dalam pertukaran informasi serta penyimpanan data sangatlah penting. Karena suatu komunikasi data jarak jauh, belum tentu aman dari pencurian sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri.

PT. Wahana Indo Trada Nissan Jatake merupakan perusahaan yang bergerak dibidang retail otomotif, pelayanan purna jual yang terletak di Jl. Gatot Subroto KM. 8, Jatake Tangerangdan terbentuk pada tanggal 1 Agustus 1931.Sebagai perusahaan yang bergerak dibidang retail otomotif, PT. Wahana Indo Trada Nissan Jatake selalu berkomunikasi melalui e-mail ke sesama anggota dengan divisi terkait, untuk memberikan informasi persoalan-persoalan pelayanan yang telah diberikan terhadap kliennya. Keamanan data, khususnya untuk dokumen teks bagi perusahaan yang mengasumsikan bahwa dokumen tersebut bernilai rahasia Ikomang and Triandini (2014). PT. Wahana Indo Trada Nissan Jatake ingin berinovasi dalam menerapkan teknologi terkini untuk mengamankan data informasi/pesan yang akan dikirimkan melalui e-mail.

Salah satu cara yang dapat digunakan dalam mengamankan pengiriman informasi, yaitu dengan menyembunyikan informasi pada media lain maupun dengan menyandikan informasi menjadi kode-kode yang tidak dengan mudah dimengerti oleh orang-orang yang tidak berkepentingan Anshori and Aribowo (2014). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan akan dikirim dari suatu tempat ke tempat yang lain Rahman (2019). Begitu pentingnya kriptografi, saat berbicara tentang keamanan computer orang tidak bisa memisahkannya dengan kriptografi Anadia et al. (2012). Enkripsi adalah proses pengamanan suatu file dengan membuat file tersebut tidak dapat dibaca tanpa bantuan alat khusus. Sedangkan dekripsi adalah cara yang dapat digunakan untuk membaca file yang telah dienkripsi agar kembali dapat dibaca ke bentuk semula.

2. Kerangka Teoritis

2.1. Algoritma Generate Key

Algoritma Elgamal merupakan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan dua buah bilangan acak (random) g dan x, dengan syarat bahwa nilai g dan x lebih kecil dari p yang memenuhi persamaan. (Tamam, M. T., Dwiono, W., & Hartanto, T, 2010).

$$Y = g \hat{} x \bmod p$$

Dari persamaan tersebut nilai y, g, dan p merupakan pasangan kunci public, sedangkan x, p merupakan pasangan kunci pribadi. Besaran-besaran digunakan dalam algoritma kriptografi Elgamal adalah:

1) P adalah bilangan prima dengan syarat P > 255

2) G adalah bilangan acak, dengan syarat G < P
3) X adalah bilangan acak, dengan syarat X < P
4) Y adalah hasil perhitungan dari Y = G ^ x mod P
5) Lalu dihasilkan public key = y g p, dan private key = p x

2.2. Algoritma Proses Enkripsi

Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (chipertext). Pada proses ini digunakan public key (p,g,y). Langkah-langkah dalam mendekripsi pesan adalah sebagai berikut. (Elys C.Y, n.d.).

$$a = g \hat{} k \bmod p$$
$$b = y \hat{} k.m \bmod p$$

1) Potong plaintext menjadi blok-blok m1, m2. . . .
2) Ubah nilai blok pesan ke dalam nilai ASCII
3) Pilih bilangan acak k, dengan syarat $1 \leq k \leq p-2$. Nilai k digunakan untuk menghitung nilai a dan b.
4) Setiap blok m dienkripsi dengan rumus sebagai berikut:

Nilai a (Gamma) = g ^ k mod p

Nilai b (Delta) = y ^ k.m mod p

5) Susun ciphertext dengan urutan
a1,b1,a2,b2,……,aN,bN

2.3. Algoritma Proses Dekripsi

Proses Dekripsi Merupakan proses mengubah pesan rahasia (ciphertext) menjadi pesan asli (plaintext). Proses dekripsi menggunakan kunci pribadi x dan p untuk mendekripsi a dan b menjadi plaintext (m) dengan persamaan:

$$m = b \, . \, a \hat{} (p-1-x) \bmod p$$

1) Penentuan nilai Gama dan Delta. Nilai Gamma(a) diperoleh dari chipertext dengan urutan ganjil, sedangkan Delta(b) diperoleh urutan genap.
2) Hitung plaintext m dengan persamaan rumus tersebut.
3) Ubah nilai m yang didapat ke dalam nilai ASCII
4) Susun plaintext dengan urutan m1, m2,. ...,mN.

3. Literature

1. Penelitian ini dilakukan oleh Whilda Chaq (2013), yang berjudul "Perbandingan Al- goritma Kunci Nirsimetris ElGamal dan RSA Pada Citra Berwarna". Pada Makalah ini peneliti akan membandingkan dua buah algoritma kriptografi kunci nirsimetris RSA dan ElGamal. Alasan pemilihan kedua algoritma tersebut Karena RSA merupakan algoritma kriptografi kunci publik yang paling popular hingga saat ini dan ElGamal yang dini- lai memiliki keunikan dalam mengenkripsi sebuah plaintext menjadi 2 buah ciphertext. Perbandingan duah buah algoritma ini akan diujikan pada citra berwarna sehingga hasil enkripsi maupun dekripsi dapat dilihat secara visual.

2. Penelitian ini dilakukan oleh Faqihuddin Al-Anshori, dkk (2014) yang berjudul "Implementasi Algoritma Kriptografi Kunci Publik ElGamal Untuk Proses Enkripsi dan Dekripsi Guna Pengamanan File Data". Subyek dalam penelitian ini adalah bagaimana mengamankan sebuah file data. Metode yang digunakan adalah kriptografi ElGamal,

metode ini merupakan bagian dari kriptografi asimetris.

3. Penelitian ini dilakukan oleh I Komang Rinartha Yasa Negara, dkk (2014) yang berjudul "Analisis dan Implementasi Gabungan Kriptografi ElGamal dan Stenografi Frame Dengan Menggunakan Kunci Citra Digital". Pada penelitian ini dikembangkan sebuah algoritma kriptografi dan steganografi yang merupakan gabungan dari kriptografi ElGamal dan steganografi Frame.

4. Penelitian ini dilakukan oleh Anadia Zelvina, dkk (2012) yang berjudul "Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal untuk Mahasiswa" Pada penulisan artikel ilmiah ini akan dijelaskan cara-cara mengamankan data menggunakan algoritma ElGamal

5. Penelitian ini dilakukan oleh Purwadi, dkk (2014) yang berjudul "Aplikasi Kriptografi Asimetris Dengan Metode Diffie-Hellman dan Algoritma ElGamal Untuk Keamanan Teks". Hasil penelitian ini menjelaskan; Pertama, Diperlukan instalasi aplikasi untuk setiap perangkat yang akan digunakan untuk melakukan enkripsi dan dekripsi, Kedua, Aplikasi yang dibangun dapat menerapkan metode pertukaran kunci Diffie Hellman dan menghasilkan kunci baru.

4. Metodologi Penelitian

4.1. Metode Pengembangan

Metode pengembangan yang digunakan dalam mengembangkan aplikasi ini adalah metode prototipe dan metode pengumpulan data yang meliputi: Metode pengumpulan data yang digunakan adalah : a. Metode Observasi, b. Metode Wawancara atau Interview, c. Metode Studi Pustaka.

4.2. Metode Pengembangan

Model prototipe yang akan digunakan :

1) Pengumpulan kebutuhanssss
2) Membangun prototipe
3) Evaluasi prototipe
4) Mengkodekan sistem
5) Menguji sistem
6) Evaluasi sistem
7) Menggunakan sistem

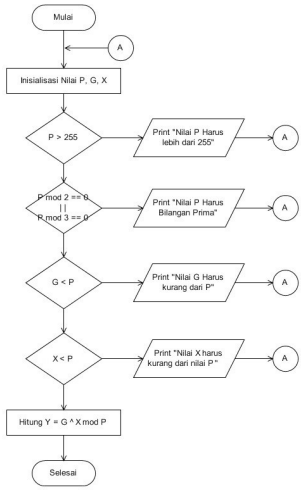
5. Hasil Dan Pembahasan

Flowchart Program

Berikut ini adalah flowchart enkripsi dan dekripsi yang digunakan untuk menelusuri proses enkrip dan dekrip pada aplikasi pengamanan data ini.

5.1. Flowchart Algoritma Proses Generate Key

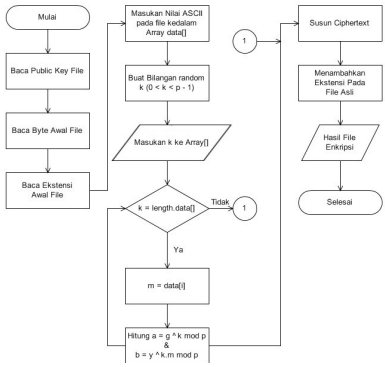
F*lowchart* ini menjelaskan alur proses algoritma pada *generate key*, dimana nilai P harus bilangan prima dan nilai G harus lebih kecil dari pada nilai P dan nilai X juga harus lebih kecil dari pada nilai P, setelah itu simpan kunci *public* dan kunci *private* ke tempat penyimpanan. Gambar 1 *flowchart* dari *Form* Algoritma Proses *Generate Key.*



GAMBAR 1: FlowchartAlgoritma Proses Generate Key

5.2. Flowchart Algoritma Proses Enkripsi

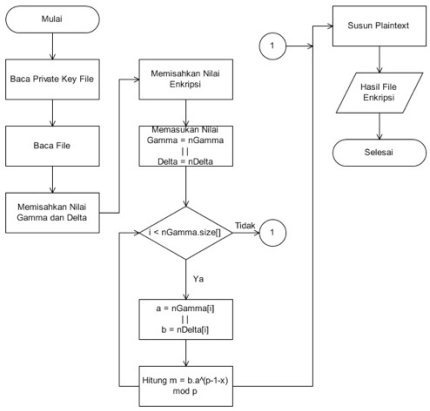
Flowchart ini menjelaskan alur proses dari file asli yang dikelola dengan menggunakan algoritma ElGamal dan dienkripsi hingga menjadi file acak. Gambar 2 flowchart dari Form Algoritma Proses Enkripsi.



GAMBAR 2: Flowchart Algoritma Proses Enkripsi

5.3. Flowchart Algoritma Proses Dekripsi

Flowchart ini menjelaskan alur proses dari file yang sudah terenkripsi menjadi file asli dengan menggunakan algoritma ElGamal.



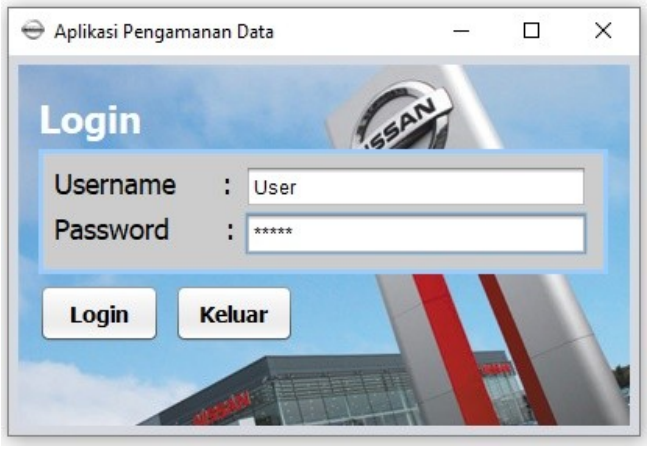
GAMBAR 2: *Flowchart* Algoritma Proses Dekripsi

5.4. Tampilan Layar

Pada bagian ini akan menjelaskan mengenai proses tampilan layar aplikasi mulai dari pertama sampai selesai. Berikut ini akan diberikan penjelasan dari gambar mengenai tampilan-tampilan yang ada pada aplikasi pengaman data yang dibuat ini.

Tampilan Layar Form Login

Berikut ini adalam tampilan layar formlogin dimana user harus memasukan username dan password terlebih dahulu agar dapat menggunakan aplikasi ini. Pada menu ini dapat dilihat gambar 4 berikut ini.



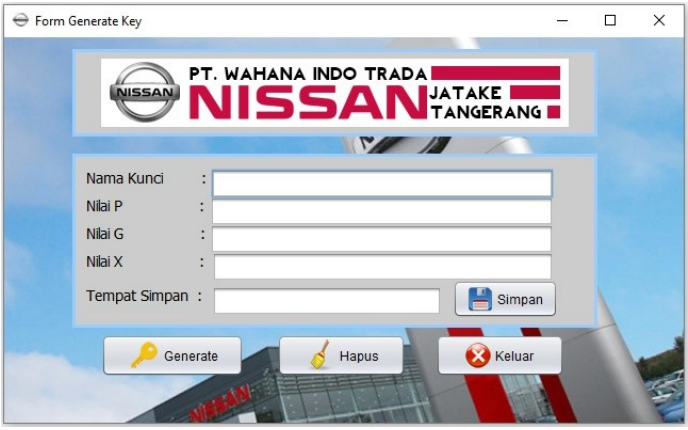
GAMBAR 4: Tampilan Form Login

Jika user tidak memasukan username dan password atau pun kosong, maka akan muncul message box seperti gambar 5 berikut ini.

GAMBAR 5: Tampilan Layar Message box Username dan Password Kosong

Tampilan Layar Form Generate Key

Berikut ini adalah form generate key terdapat nama kunci untuk memberikan nama pada kunci yang akan dibuat, berikutnya user diminta mengimput nilai P, G, dan X. Dimana nilai P harus diatas 255 (prima), nilai G juga harus kurang dari nilai P, dan nilai X harus kurang dari nilai P-2. Pada menu ini dapat dilihat pada gambar berikut ini.

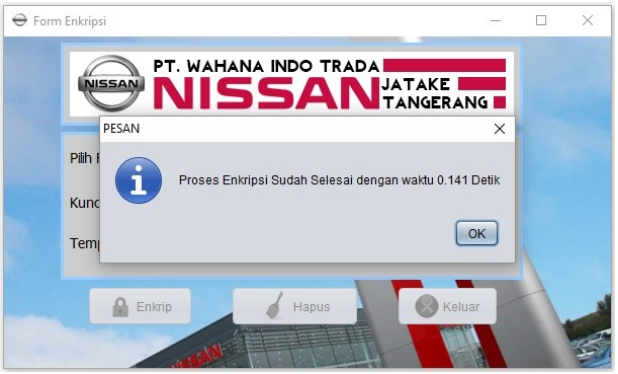


GAMBAR 6: Tampilan Layar Form Generate Key

Proses input harus terisi semua pada form Enkripsi. Dapat dilihat pada gambar 7 berikut ini.

GAMBAR 7: Tampilan Layar Form Enkripsi Terisi Semua

Selanjutnya proses enkripsi sudah selesai maka akan muncul message box. Dapat dilihat pada gambar 8 berikut ini.



GAMBAR 8: Tampilan Layar Message box Enkripsi Selesai

Setelah proses input terisi semua pada form dekripsi. Dapat dilihat pada gambar 9 berikut ini.

GAMBAR 9: Tampilan Layar Form Dekripsi Terisi Semua

Setelah proses pada form dekripsi selesai akan muncul message box. Dapat dilihat pada gambar 9 berikut ini.

GAMBAR 10: Tampilan Layar Message box Dekripsi Selesai

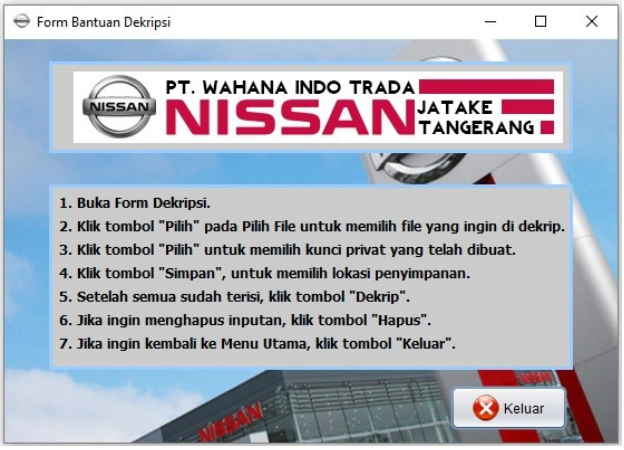
Tampilan LayarForm Bantuan Enkripsi

Selanjutnya form bantuan enkripsi yang menampilkan bagaimana cara proses file yang ada pada di form enkripsi. Dapat dilihat pada gambar 11 berikut ini.

GAMBAR 11: Tampilkan Layar Form Bantuan Enkripsi

Tampilan LayarForm Bantuan Dekripsi

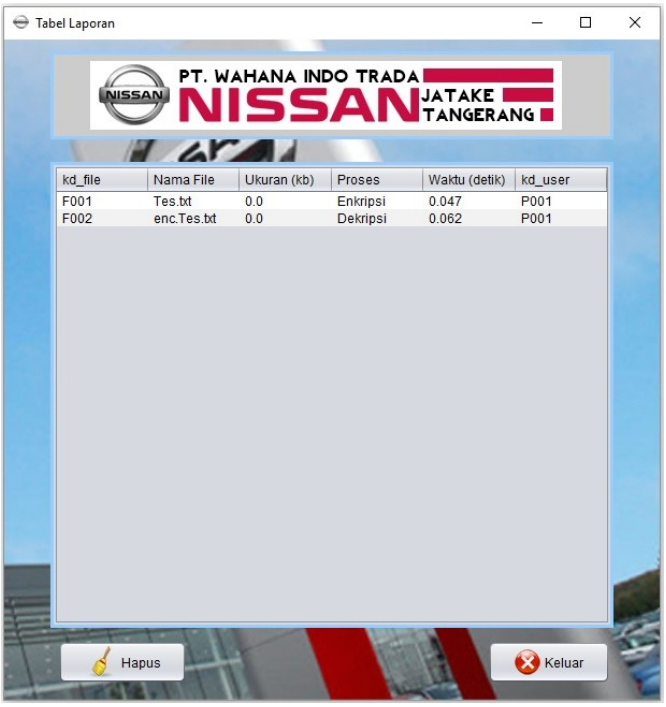
Selanjutnya form bantuan dekripsi yang menampilkan bagaimana cara proses file yang ada pada di form dekripsi. Dapat dilihat pada gambar 12 berikut ini.



GAMBAR 12: Tampilan Layar Form Bantuan Dekripsi

Tampilan Layar Form Laporan

Selanjutnya form Laporan disini menampilkan riwayat data yang pernah dilakukan dekripsi maupun enkripsi yang tersimpan pada database.



GAMBAR 13: Tampilan Form Laporan

Berikut ini adalah hasil perbandingan antara file yang asli dengan file yang belum di enkripsi dengan menggunakan aplikasi ini. Dengan kebutuhan yang sudah terpenuhi baik software maupun hardware maka akan dilakukan uji coba.

5.5. Proses Dari File Asli Ke Enkripsi

Berikut ini adalah hasil perbandingan antara file yang asli yang belum di enkripsi dengan menggunakan aplikasi ini. Dengan kebutuhan yang sudah terpenuhi dengan baik software maupun hardware maka akan dilakukan uji coba. Dapat dilihat file .pdf yang asli dan yang sudah di enkripsi pada Gambar 14 berikut ini.

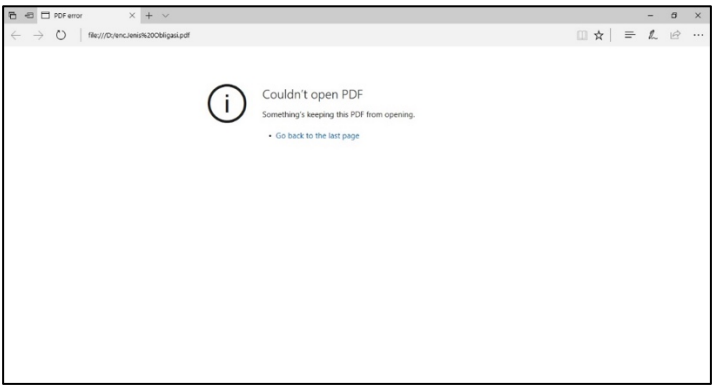
GAMBAR 14: Tampilan File Asli sebelum di Enkripsi

Diatas merupakan file asli yang belum dienkripsi dan gambar dibawah ini adalah file yang sudah terenkripsi.

GAMBAR 15: Perbandingan Gambar File Asli .pdf dengan yang sudah di enkripsi

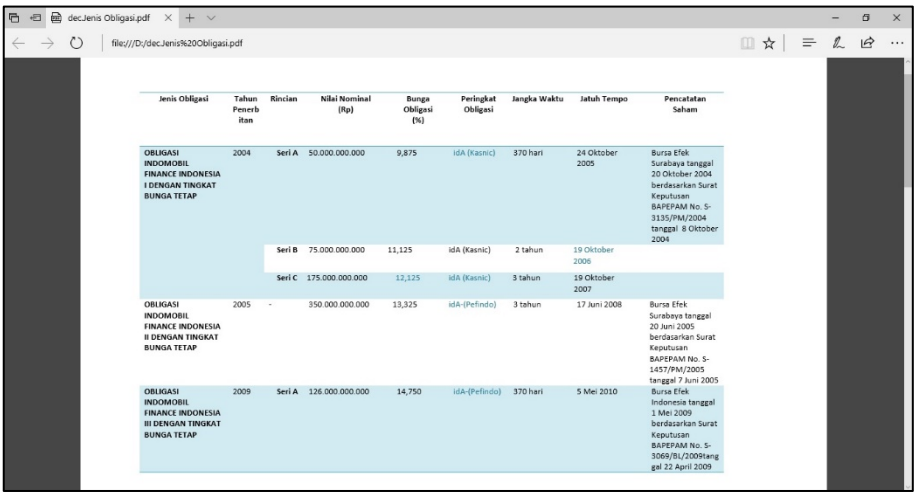
5.6. Proses Dari File Enkripsi ke File Dekripsi

Merupakan proses pengembalian file yang sudah di enkripsi menjadi file dekripsi dan user bisa memilih form dekripsi lalu memilih file yang berformat *.pdf. Dapat dilihat file .doc yang sudah terenkripsi dan yang sudah di dekirpsi dapat dilihat pada gambar berikutini.



GAMBAR 16: File hasil Enkripsi

Diatas merupakan file yang sudah terenkripsi sedangkan file dibawah ini merupakan file yang sudah di dekripsi menjadi file asli kembali.



GAMBAR 17: Perbandingan Gambar File Enkripsi .doc dengan yang sudah di Dekripsi
Diatas merupakan file yang sudah terenkripsi sedangkan file dibawah ini merupakan file yang sudah di dekripsi menjadi file asli kembali.

6. Kesimpulan

Kesimpulan yang diperoleh setelah melewati tahap perancangan, pembuatan, serangkaian

Analisa dan uji coba program aplikasi kriptografi ini, maka dapat disimpulkan sebagai berikut. Aplikasi ini sangat bermanfaat untuk mengamankan file dokumen agar isinya tidak dapat diketahui, dicuri atau ditiru oleh orang lain yang tidak berhak. Waktu proses enkripsi dan dekripsi tergantung ukuran file yang diinput, semakin besar ukuran file maka akan semakin lama proses enkripsi dan dekripsinya. Ukuran file yang dapat dienkripsi dibatasi kurang dari 1MB

User harus membuat public key dan private key terlebih dahulu untuk melakukan enkripsi dan dekripsi. Sebelum file dikirim melalui e-mail data harus dienkripsi terlebih dahulu agar tidak dapat terlihat isi dari file yang akan dikirim dan file sulit untuk dibaca atau diubah jika terjadi pencurian oleh pihak yang tidak bertanggung jawab. File yang telah dienkripsi harus dilakukannya proses deskripsi menggunakan private key yang telah dibuat saat proses generate key sebelumnya agar file dapat berubah menjadi file asli semula.

Daftar Pustaka

[1] IKomang, R.Y.N., dan Evi Triandini, 2014. *"Analisis Dan Implementasi Gabungan Kriptografi ElGamal Menggunakan Kunci Citra Digital. Eksplora Informatika, 2(3), 141-150."*

[2] Anshori, F., dan Aribowo, E., 2014. *"Implementasi Algoritma Kriptografi Kunci Public ElGamal Untuk Proses Enkripsi Dan Dekripsi Guna Pengamanan Data.*" Jurnal Informatika, 1(1), 56-62.

[3] Abdul Rahman., 2019. *"Perancangan Aplikasi Pengamanan File Pada Memory Card Handphone Menggunakan Algoritma Kunci Asimetris Elgamal."* Vol. 6, No. 5, Oktober 2019 ISSN 2407-389X (Media Cetak)

[4] Anadia, Z., Efendi, S., dan Dedy, A., 2012. *"Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa".* Jurnal Dunia Teknologi Informasi, 1(1), 56-62.

[5] Purwadi, Hendra, J., dan Ahmad, C., 2014. *"Aplikasi Kriptografi Asimetris Dengan Metode Diffie-Hellman Dan Algoritma ElGamal Untuk Keamanan Teks."* Jurnal SAINTIKOM, 3(13), 183-196.

[6] Chaq, W., 2013. "*Perbandingan Algoritma Kunci Nirsimetris ElGamal dan RSA pada Citra Berwarna"*, IF3058 Kriptografi Sem. II.

[7] Triase., 2015. *"Kriptografi Elgamal Menggunakan Metode Mersenne."* Jurnal ilmiah "INTEGRITAS" Vol.1 No. 4 Desember 2015

[8] Bella Ariska, Suroso, Jon Endri., 2018. *"Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher Dan Elgamal Pada Pengamanan Pesan Rahasia"* ITN Malang, 3 Pebruari 2018 ITN Malang, 3 Pebruari 2018

[9] Aisyatul Karima, L. Budi Handoko, Ari Saputro., 2017. *"Pemfaktoran Bilangan Prima pada Algoritme ElGamal untuk Keamanan Dokumen PDF"* UGM Jogja, Vol 6, No 3 (2017)

[10] Islamiyah., 2017. *"Algoritma Kriptografi Kunci Publik Elgamal Untuk Keamanan Pesan Sms (Short Message Service) Berbasis Android"* SEMANTIK 2017 ISSN:

2580-796x

[11] Buyung Solihin Hasugian., 2017. *"Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah"* No 53 (2017)

[12] David Iman Fauzan., 2019. *"Kriptografi Kunci Publik Kurva Eliptik Atas Lapangan Hingga Dan Implementasinya Menggunakan Bahasa Pemrograman Python Untuk Membuat Python Packages")"* Universitas Islam Negeri Sunan Kalijaga, Yogyakarta

[13] Nur Fajrin Maulana Yusuf., 2019. *"Pengiriman Pesan Dengan Algoritma Kriptografi Elgamal (Menggunakan Aplikasi Visual Basic)." Vol 1 No 2 (2019): Axiomath*

[15] Kentol Mas Sudrajat., 2019. *"Perancangan Aplikasi Pengamanan File Teks Menggunakan Algoritma El Gamal Dan Kompresi File Teks Menggunakan Algoritma Huffman."* Volume 18, Nomor 4, Oktober 2019 ISSN 2301-9425 (Media Cetak)

[16] Puspita sari, Fifi Safitri, Ajeng Listianingrum, Nurfika Sari, M. Arif Hasan., 2020. *"Enkripsi File Audio Mp3 Dan Wav Menggunakan Metode Kriptografi Rsa (Rivest Shamir Adleman) Dan Elgamal."* Jurnal Teknik Informatika 2020

[17] Wahyu Pramusinto, Nugroho Wizaksono, Ari Saputro., 2019. *"Aplikasi Pengamanan File Berbasis Web Dengan Metode Kriptografi Aes 192, Rc4 Dan Metode Kompresi Huffman."* Jurnal Teknik Informatika 2020

[18] Fachrur Rijal., 2019. *"Penerapan Sistem Enkripsi AES-128 Pada Aplikasi SMS Berbasis Android."* Universitas Jember, Jember

[19] Nasrudin, Agung Pratama, Ega Pratama, Ella Tri Wulandari., 2019. *"Implementasi Algoritma Elgamal Dan Kode Hill Untuk Keamanan Database."* Universitas Lancang Kuning, Pekanbaru

[20] Diah Anggraini, Safitri Juanita., 2018. *"Aplikasi E-Arsip Pengamanan Pesan Elektronik Berbasis Web dengan Mengimplementasikan Algoritma Kriptografi RSA dan Elgamal pada Klinik Dr. H. Hartono."* Jurnal TICOM Vol. 6 No.3 Mei 2018

[21] Tanjung, Muhammad Hakim., 2018. *"Perbandingan Kinerja Algoritma ElGamal dan Algoritma Multipower RSA Dalam Pengamanan File."* Universitas Sumatera Utara, Medan