Enkripsi Dan Dekripsi File Dokumen Dengan Metode Elgamal

Thabrani Rahim, Muhardi, Faisal
Universitas Dipa Makassar
Jl. Perintis Kemerdekaan Km. 9, 0411-587194
e-mail: thabranidp@gmail.com, muhardi@dipanegara.ac.id, ichslsbinurullah@gmail.com

Abstrak

Kriptografi penting dalam mengamankan file dokumen digital yang tidak boleh dilihat secara umum. Bukan tidak mungkin bagi siapa pun untuk melihat, merusak, mencuri atau menyalahgunakan data penting dari agensi atau perusahaan. Solusinya adalah dengan kriptografi atau metode keamanan data yang dapat menjaga kerahasiaan dan keaslian data atau informasi. Metode ini ditujukan untuk informasi file dokumen yang disimpan dalam komputer. Kriptografi mendukung aspek keamanan informasi, yaitu perlindungan kerahasiaan. Oleh karena itu kebutuhan untuk menjaga kerahasiaan data dan informasi adalah aplikasi cryptographic. Prosesnya berupa enkripsi dan dekripsi yang digunakan oleh pengguna untuk mengamankan data tanpa mengubah isi data. Aplikasi ini memiliki kunci 32 karakter tetapi dalam penggunaannya dibuat menjadi 2 kunci, yaitu kunci publik dan privat di mana kunci publik adalah kunci yang diisi oleh pengguna sesuai dengan keinginan, sedangkan kunci privat adalah kunci default yang dimasukkan oleh aplikasi secara acak untuk memenuhi panjang 32 karakter. Algoritma Elgamal di mana algoritma ini menggunakan prinsip dengan jumlah putaran berdasarkan kunci.

Kata kunci: *Kriptografi , Elgamal, Enkripsi, Dekripsi, Algoritma.*

Abstract

Cryptography is important in securing digital document files that should not be viewed in public. It is not impossible for anyone to view, tamper with, steal or misuse important data from agencies or companies. The solution is cryptography or data security methods that can maintain the confidentiality and authenticity of data or information. This method is intended for document file information stored in the computer. Cryptography supports aspects of information security, namely the protection of confidentiality. Therefore the need to maintain the confidentiality of data and information is a cryptographic application. The process is in the form of encryption and decryption that is used by users to secure data without changing the contents of the data. This application has a 32 character key but in its use it is made into 2 keys, namely the public and private keys where the public key is the key that the user fills in as desired, while the private key is the default key entered by the application randomly to meet the length of 32 characters. . Elgamal algorithm where this algorithm uses the principle of the number of rounds based on the key.

Keywords*: Cryptography, Elgamal, Encryption, Decryption, Algorithm.*

1. Pendahuluan

Keamanan merupakan salah satu aspek penting dalam dokumen digital baik yang bersifat data pribadi maupun data penting lainnya yang tersimpan dalam komputer. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi. Teknik ini berguna untuk membuat pesan, data, maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak dan mengetahui teknik dekripsinya. Teknik enkripsi dan dekripsi dikenal dan dipelajari dalam sistem kriptografi.

Kriptografi berasal dari bahasa Yunani yaitu, *cryptos* yang berarti rahasia dan *graphein* yang berarti tulisan. Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh sesorang yang tidak memiliki kunci dekripsi [1].

Secara umum ada dua tipe algoritma kriptografi berdasarkan kuncinya yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah algoritma yang memiliki kunci enkripsi dan dekripsi yang sama, sedangkan untuk algoritma asimetris terdiri atas dua buah kunci yaitu kunci publik untuk melakukan enkripsi sedangkan kunci pribadi untuk melakukan dekripsi. Dalam algoritma kunci asimetris, kunci yang didistribusikan adalah kunci publik yang tidak diperlukan kerahasiaanya sedangkan kunci pribadi tetap disimpan atau tidak didistribusikan. Setiap orang yang memiliki kunci publik dapat melakukan proses enkripsi tetapi hasil dari enkripsi tersebut hanya bisa dibaca oleh orang yang memiliki kunci pribadi [2].

Kajian terdahulu telah dilakukan oleh Yudi Wiharto dan Ari Irawan yang menghasilkan sebuah program aplikasi untuk enkripsi dan dekripsi file dokumen menggunakan Algoritma RSA dengan menggunakan Delphi 7. Aplikasi tersebut dapat digunakan untuk keamanan data file dokumen yang dapat digunakan oleh pemakai program baik secara umum maupun pribadi [3].

Kriptografi kunci publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Kotak surat yang diletakkan di depan rumah pemiliknya sehingga setiap orang dapat memasukkan surat ke dalam kotak tersebut, tetapi hanya pemilik kotak yang dapat membuka dan membaca surat yang ada di dalam kotak tersebut. Kriptografi kunci publik berkembang menjadi sebuah revolusi baru dalam sejarah kriptografi, tidak seperti pada kunci simetris yang hanya didasarkan pada subtitusi dan permutasi saja, akan tetapi kriptografi kunci publik didasarkan pada fungsi matematika seperti perpangkatan dan modulus. Konsep kriptografi kunci asimetris dapat dilihat pada Gambar 1.

Gambar 1. Kriptografi kunci asimetris

Algoritma kriptografi ElGamal menggunakan beberapa persamaan untuk melakukan proses *generate key*, proses enkripsi dan proses dekripsi [4].

2. Metode Penelitian

Untuk menyelesaikan penelitian ini diperlukan pengumpulan data yang berhubungan dengan masalah yang dibahas. Tujuannya sebagai sumber landasan pembahasan dan pembuatan rancangan sistem. Adapun metode penelitian yang digunakan dalam mengumpulkan data atau materi penulisan adalah dengan cara:

2.1. Pengamatan (observasi)
Pengamatan atau observasi merupakan salah satu teknik pengumpulan data/fakta yang cukup efektif untuk mempelajari suatu sistem. Pengamatan langsung ini dilakukan untuk mengetahui proses-proses yang sedang berjalan serta membuat keputusan yang menyangkut lingkungan fisiknya pada suatu kegiatan yang sedang berjalan.

2.2. Wawancara (*interview*)
Wawancara dilakukan untuk mendapatkan data dan informasi dalam bentuk tanya jawab kepada orang yang terlibat secara langsung yang merupakan obyek penelitian.

2.3. Studi Pustaka
Metode ini menggunakan dokumen sebagai sumber bacaan, baik buku-buku ilmiah maupun jurnal, terutama yang erat hubungannya dengan masalah yang di bahas dalam penelitian ini.

3. Hasil dan Pembahasan

3.1. Teori Terkait

Perangkat lunak adalah objek tertentu yang dapat dijalankan seperti kode sumber, kode objek atau sebuah program yang lengkap. Produk perangkat lunak memiliki pengertian perangkat lunak yang ditambahkan dengan semua item dan pelayanan pendukung yang secara keseluruhan dapat memenuhi kebutuhan pemakai. Produk perangkat lunak memiliki banyak bagian yang meliputi manual, referensi, tutorial, intruksi instalasi, data sampel, pelayanan pendidikan, pelayanan pendukung teknis dan sebagainya. Semua yang dihasilkan oleh proyek perangkat lunak adalah produk kerja (*work product*) [5].

Program merupakan ekspresi, pernyataan kombinasi yang disusun dan dirangkai menjadi satu kesatuan prosedur yang berupa urutan langkah untuk menyelesaikan masalah yang diimplementasikan dengan menggunakan bahasa pemrograman, sehingga dapat dieksekusi oleh komputer. Sedangkan Aplikasi adalah suatu penerapan, menyimpan sesuatu hal, data, permasalahan pekerjaan kedalam suatu sarana atau media yang digunakan untuk menerapkan atau mengimplementasikan hal atau permasalahan tersebut sehingga berubah menjadi suatu bentuk yang baru tanpa menghilangkan nilai - nilai dasar dari hal, data, permasalahan atau pekerjaan [6].

Kriptografi berasal dari kata kripto dan grafi. Kripto berarti menyembunyikan, dan grafik yaitu ilmu. Kriptografi (*cryptography*) adalah suatu ilmu yang mempelajari suatu sistem penyandian untuk menjamin kerahasiaan dan keamanan data. Orang yang melakukan disebut *Criptographer*. Kriptografi merupakan ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, dan integritas data serta autentifikasi data. Sistem kriptografi klasik umumnya menggunakan metode subtitusi atau transposisi dan telah digunakan jauh sebelum komputer ditemukan [7]. Terdapat beberapa komponen utama dalam sistem kriptografi. Secara umum, istilah kriptografi yang sering digunakan adalah:

1. Pesan
   Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya, pesan sering juga disebut dengan *plaintext* atau teks jelas (*cleartext*). *Plaintext* merupakan suatu pesan bermakna yang akan diproses menggunakan algoritma kriptografi.
2. *Ciphertext*
   Cipertext atau di sebut dengan *cryptosystem* merupakan pesan yang telah tersandi. Pesan dalam bentuk ciphertext tidak dapat dibaca karena berisi karakter-karekter yang tidak memiliki makna setelah melalui proses enkripsi.
3. Enkripsi
   Enkripsi merupakan proses penyandian plaintext menjadi *ciphertext* atau disebut sebagai *enciphering*. Enkripsi dilakukan dengan tujuan agar plaintext tersebut tidak dapat dibaca oleh pihak yang tidak memiliki otoritas (wewenang).
4. Dekripsi
   Dekripsi merupakan proses pengembalian ciphertext menjadi plaintext semula atau disebut *deciphering*. Dekripsi dilakukan ketika pesan telah sampai kepada pihak yang dituju.
5. Kunci (*key*).
   Kunci (*key*) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci dapat juga berupa string atau deretan bilangan. Keamanan suatu algoritma kriptografi biasanya tergantug kepada kerahasiaan penyebaran *key*.
6. Kriptosistem (*cryptosystem*)
   Cryptosystem adalah perangkat keras atau implementasi perangkat lunak kriptografi yang diperlukan atau mentranformasi sebuah pesan asli menjadi *ciphertext* atau juga sebaliknya.

Algoritma ElGamal merupakan algoritma kriptografi asimetris. Pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985 [8]. Seperti RSA (Rivest Shamir Adleman), algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok *plaintext* dan menghasilkan blok-blok *ciphertext* yang kemudian dilakukan proses enkripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan bisa dimengerti. Untuk membentuk sistem kriptografi ElGamal, dibutuhkan bilangan prima p. Untuk algoritma ElGamal maka secara secara umum dapat dijelaskan pada gambar dibawah ini, merupakan pseudo code ElGamal proses pembentukan kunci, enkripsi dan dekripsi ElGamal.

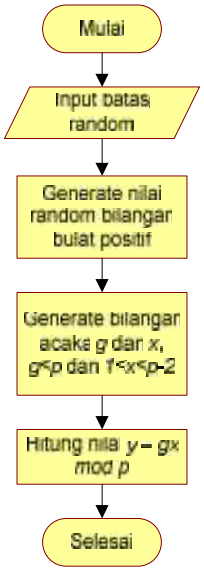
3.2. Algotima *Generate Key*

Algoritma ElGamal memerlukan 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.

$$y = g^x \bmod p \qquad (1)$$

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

1. Bilangan prima *p* bersifat tidak rahasia.
2. Bilangan acak *g* ($g < p$) bersifat tidak rahasia.
3. Bilangan acak *x* ($x < p$) bersifat rahasia.
4. Bilangan *y* bersifat tidak rahasia.
5. *m* (*plaintext*) bersifat rahasia merupakan pesan asli yang digunakan untuk data.
6. Sumber dalam proses enkripsi dan merupakan hasil pada proses dekripsi.
7. *a* dan *b* (*ciphertext*) bersifat tidak rahasia.



Gambar 2. Algoritma generate key

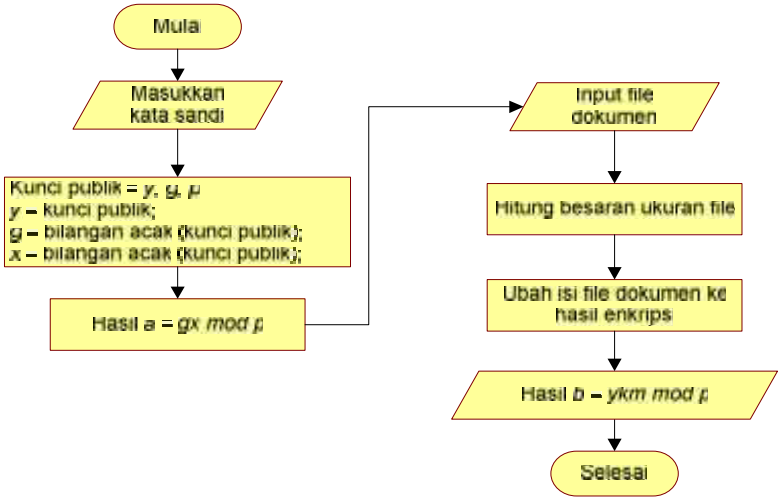
3.3. Algoritma Proses Enkripsi

Algoritma proses enkripsi dilakukan dengan memilih bilangan acak *k* yang berada dalam himpunan $1 \le k \le p\text{-}2$. Setiap blok plaintext *m* dienkripsi dengan persamaan:

$$a = gk \bmod p \qquad (2)$$

$$b = yk \bmod p \qquad (3)$$

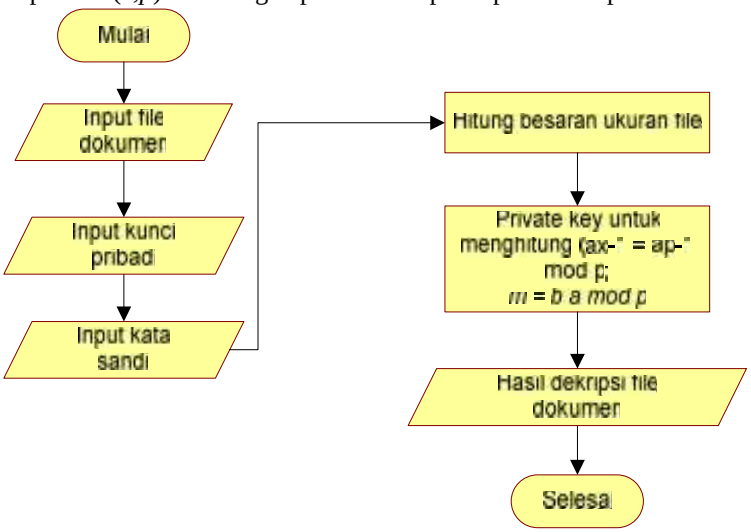
Rancangan proses enkripsi dapat dilihat pada Gambar 3.



Gambar 3. Algoritma proses enkripsi

3.4. Algoritma Proses Dekripsi

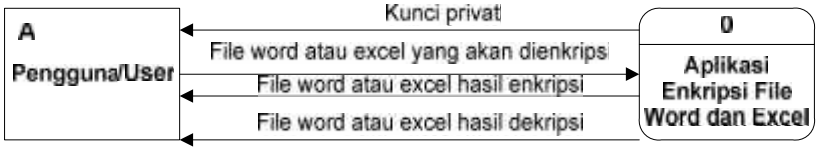
Proses dekripsi adalah proses untuk mengembalikan *ciphertext* kedalam bentuk *plaintext*, dengan menggunakan kunci pribadi (*x*,*p*). Rancangan proses dekripsi dapat dilihat pada Gambar 4.



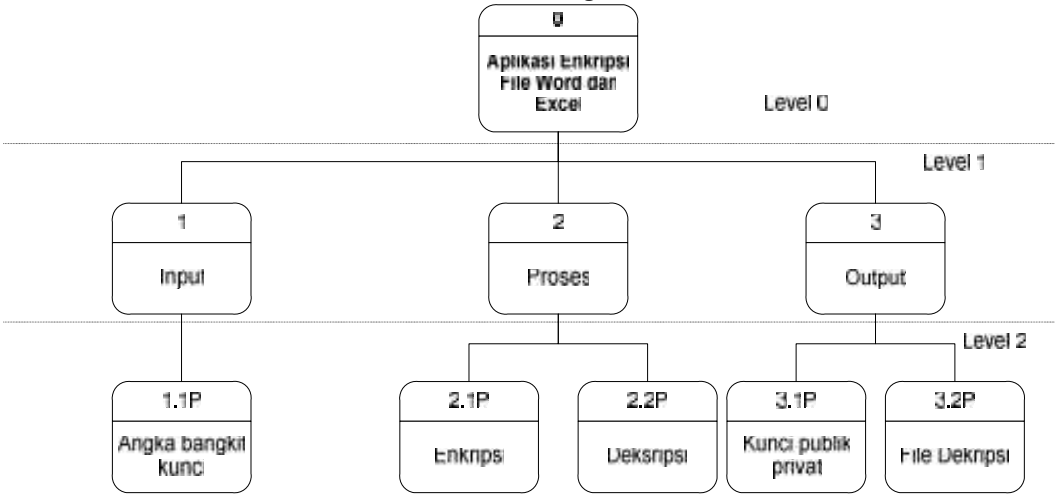
Gambar 4. Algoritma proses dekripsi

3.5. Diagram Sistem

Diagram sistem menggambarkan hubungan *input/output* antara sistem dengan dunia luarnya (kesatuan luar), dapat dilihat pada gambar 5.



Gambar 5. Diagram konteks



Gambar 6. Diagram berjenjang

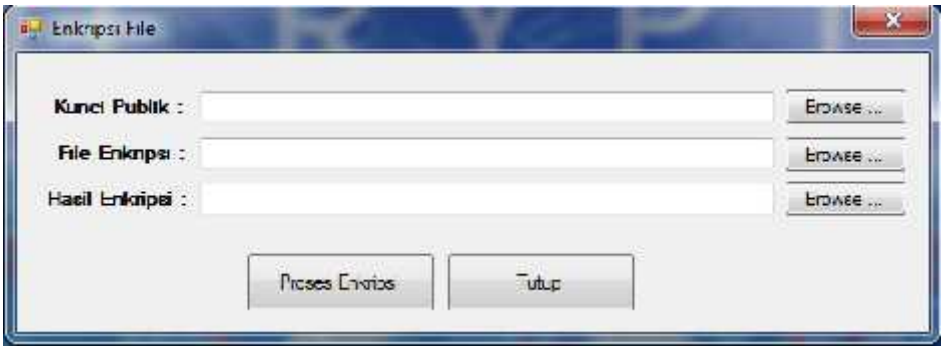
3.6. Form Pembangkitan Kunci

Form untuk membangkitkan kunci yaitu dengan memasukkan nilai batas random antara nilai 1 sampai 10. Nilai batas random yang telah dimasukkan tersebut kemudian digunakan untuk membangkitkan nilai prima (*p*), nilai (*g*), nilai (*x*) dengan cara menekan tombol **Buat Kunci**. Halaman form membangkitkan kunci dapat dilihat seperti pada gambar 7.

Gambar 7. Halaman pembangkitan kunci

3.7. Form Proses Enkripsi

Untuk menjalankan proses enkripsi yaitu dengan memasukkan kunci publik, proses ini dilakukan untuk mengambil nilai kunci publik (*p, g, y*) dari dalam basis data yang merupakan hasil dari proses *generate key*. Selanjutnya mengambil file dokumen (word, excel, pdf), selanjutnya proses enkripsi dilakukan dengan menekan tombol **Proses Enkripsi**. Hasil proses enkripsi dapat disimpan dengan menekan **tombol browse** pada bagian hasil enkripsi. Halaman proses enkripsi dapat dilihat pada gambar 8.



Gambar 8. Halaman proses enkripsi

3.8. Proses Dekripsi

Proses dekripsi dilakukan adalah mencari file dokumen yang akan didekripsi, kemudian memasukkan kunci *private*, verifikasi kunci *private*. Selanjutnya menekan tombol **Proses Dekripsi** untuk memulai proses dekripsi file dokumen. Hasil proses dekripsi file dokumen dapat disimpan dengan menekan **tombol browse** pada bagian Lokasi Hasil Dekripsi. Halaman dekripsi dapat dilihat pada gambar 9.

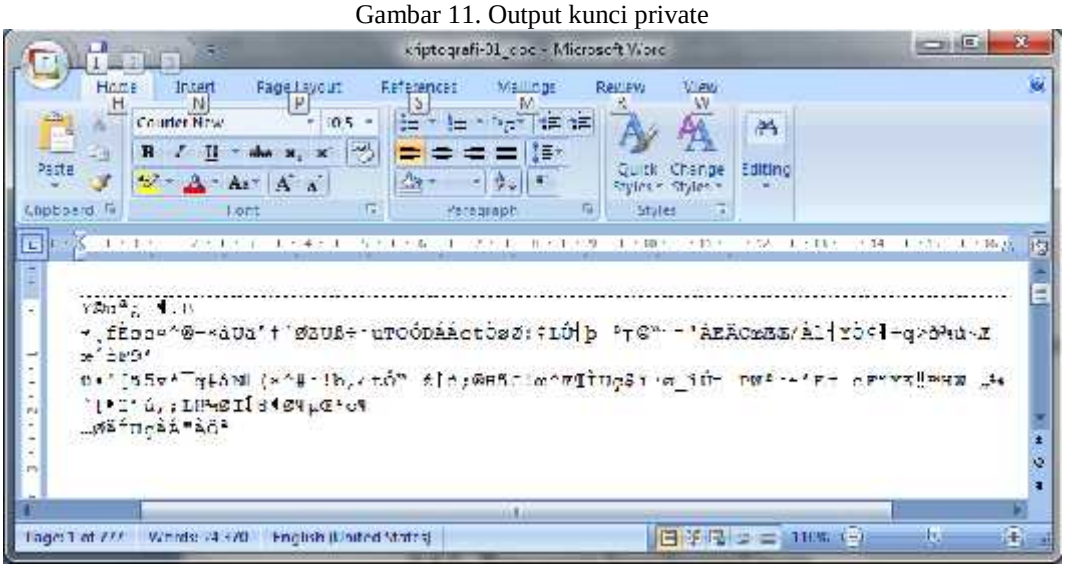
Gambar 9. Halaman proses dekripsi

3.9. *Output* Aplikasi

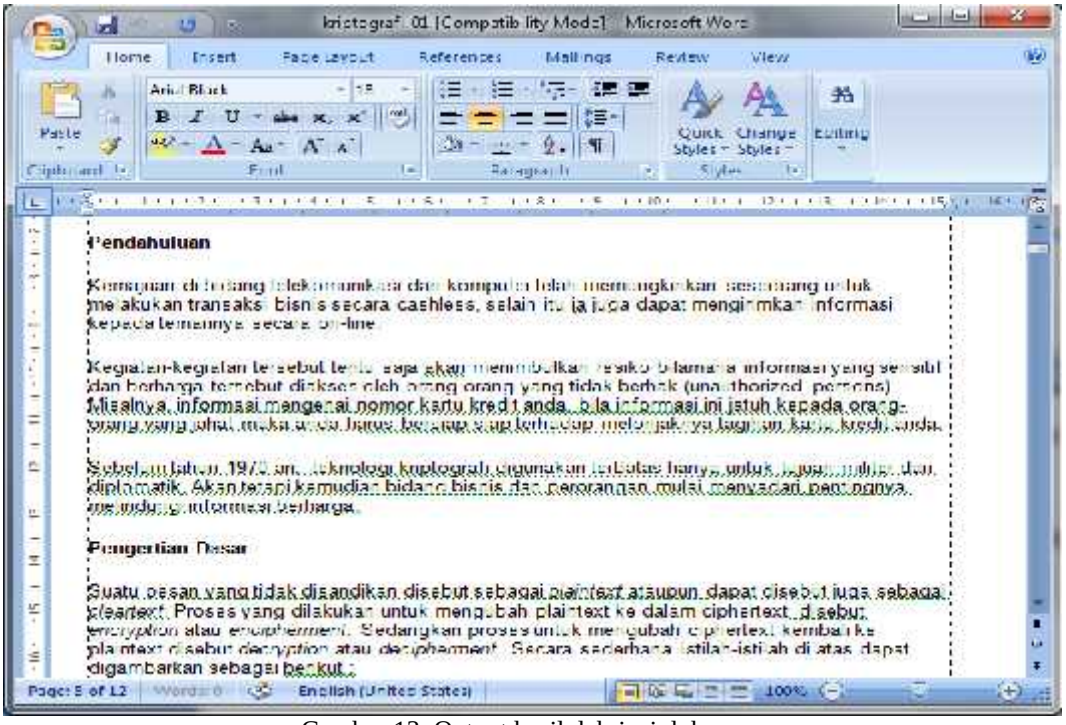
Output aplikasi enkripsi dekripsi dengan metode elgamal adalah sebagai berikut:

Gambar 10. Output kunci publik

Gambar 11. Output kunci private



Gambar 12. Output hasil enkripsi dokumen



Gambar 13. Output hasil dekripsi dokumen

3. Kesimpulan

Berdasarkan permasalahan dan aplikasi yang telah dibuat, maka dapat ditarik kesimpulan antara lain adalah aplikasi ini sangat mudah untuk dimengerti dan digunakan oleh pengguna serta dapat membantu mengamankan data atau informasi dalam bentuk file dokumen yang sebelumnya dapat dilihat oleh umum atau orang lain. Aplikasi enkripsi ini memiliki tingkat kesulitan enkripsi yaitu 32bit.

Daftar Pustaka

[1] Kromodimoeljo, Sentot. Teori dan Aplikasi Kriptografi. Edisi 1. Jakarta: SPK IT Consulting. 2009.
[2] M. Taufik Tamam, dkk. Penerapan Algoritma Kriptografi ElGamal untuk Pengamanan File Citra. *Jurnal EECCIS*. 2010; Vol. IV: 1.
[3] Yudi Wiharto, Ari Irawan. Enkripsi Data Menggunakan Advanced Encryption Standard 256. *Jurnal Kilat.* 2018; Vol. 7, No. 2.
[4] Ariyus D. Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi. Edisi 1. Yogyakarta: Andi. 2008.
[5] *Daulay, Melwin Syafrizal. Mengenal Hardware-Software dan Pengelolaan Instalasi Komputer. Edisi 1. Yogyakarta: Andi. 2007.*
[6] *Jogiyanto, H.M. Analisa dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktik Aplikasi Bisnis. Yogyakarta: Andi: 2010.*
[7] *A. Sadikin, Rifki. Kriptografi untuk Keamanan Jaringan. Yogyakarta: Andi. 2012.*
[8] *Santoso, dkk. Kriptografi Pada Aplikasi Komunikasi Data dengan Algoritma AES 256. Jurnal Ilmu Komputer SNIK:2014. Semarang.*