Implementasi Kriptografi Metode Elgamal Untuk Keamanan Data Teks

[1]Muhamad Akbar, [2]Indra Kanedi, [3]Ockhy Jey Fhiter.W

[1] Mahasiswa, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: muhamadakbar217@gmail.com
[2, 3] Dosen Tetap, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: indra.kanedi@unived.ac.id Ockhy@unived.ac.id

(Received: Mei 2025, Revised: Agustus 2025, Accepied: Oktober 2025)

Abstract-The development of technology and information today greatly affects data security and privacy. Data, which includes facts or details about an event, can be in various forms and requires reliable management. Cryptography is the main solution to securing information, which involves two main processes: encryption and decryption. The ElGamal method, an asymmetric cryptography algorithm, uses a pair of public and private keys, increasing data security without sharing the secret key. ElGamal's strength lies in the Discrete Logarithm Problem, which provides resistance to brute force attacks. It can also be used for digital signatures, ensuring the authenticity and integrity of dataThe implementation results concluded that ElGamal effectively secures text data by encrypting it into a sequence of unrepresentative characters. This implementation provides an additional layer of security by making the encrypted data unconnected to the original information
Keywords: Cryptography, ElGamal, Data Security

Intisari-Perkembangan teknologi dan informasi saat ini sangat mempengaruhi keamanan dan privasi data. Data, yang mencakup fakta atau detail tentang suatu kejadian, dapat dalam berbagai bentuk dan membutuhkan pengelolaan yang handal. Kriptografi adalah solusi utama untuk mengamankan informasi, yang melibatkan dua proses utama: enkripsi dan dekripsi.Metode ElGamal, sebuah algoritma kriptografi asimetris, menggunakan pasangan kunci publik dan privat, meningkatkan keamanan data tanpa berbagi kunci rahasia. Kekuatan ElGamal terletak pada Discrete Logarithm Problem, yang memberikan perlawanan terhadap serangan brute force. Ini juga dapat digunakan untuk tanda tangan digital, memastikan keaslian dan integritas data. Hasil implementasi menyimpulkan bahwa ElGamal secara efektif mengamankan data teks dengan mengenkripsinya ke dalam urutan karakter yang tidak representatif. Implementasi ini memberikan lapisan keamanan tambahan dengan membuat data yang dienkripsi tidak terhubung ke informasi asli
Kata kunci : Kriptografi, ElGamal, Keamanan Data

I.PENDAHULUAN

Teknologi dan pengembangan informasi saat ini memiliki dampak besar pada keamanan data dan kerahasiaan. Data adalah aspek penting yang mencakup fakta atau rincian peristiwa yang tidak diperlakukan sebagai sumber yang dapat diandalkan. Data dapat dibuat dalam bentuk angka, tanda, simbol, atau huruf lain yang dapat digunakan sebagai media informasi. Keamanan dan integrasi data adalah aspek penting yang perlu dipertimbangkan, menjadi topik penting dan berkembang dengan kemajuan pada saat itu. Kebutuhan untuk meningkatkan keamanan data telah menghasilkan berbagai jenis metode dan teknik yang dapat digunakan untuk kegiatan keamanan data. Banyak pilihan digunakan untuk melindungi data dari ancaman dari pihak yang tidak memiliki hak untuk memproses data dokumen. Juga, sejumlah besar orang membaca data yang bukan haknya. Oleh karena itu, diperlukan mekanisme yang dapat menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan keaslian (*authenticity*) pesan teks. Salah satu solusi untuk mengatasi masalah ini adalah dengan menerapkan kriptografi. Kriptografi merupakan salah satu teknik yang dapat digunakan untuk mengamankan suatu informasi. Kriptografi memiliki dua tahap yang umum dilakukan adalah tahap enkripsi dan dekripsi. Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi cipher text, sedangkan dekripsi adalah proses yang dilakukan untuk mengubah pesan tersandi menjadi pesan yang dapat dibaca dan dimengerti (Ridho et al., 2022).

Berdasarkan kunci yang digunakan, algoritma kriptografi terdiri dari dua jenis yaitu algoritma simetris dan asimetris. Kriptorgafi dengan algoritma simetris menggunakan kunci yang sama baik pada proses enkripsi maupun dekripsi sedangkan kriptografi dengan algoritma asimetris menggunakan kunci yang enkripsi yang berbeda dengan kunci dekripsi (Arif & Nurokhman, 2023). Salah satu metode kriptografi adalah ElGamal. Algoritma ElGamal termasuk dalam kriptografi asimetris. Berbeda dengan kriptografi simetris yang menggunakan kunci tunggal, ElGamal memanfaatkan pasangan kunci *public* dan *private*, sehingga memungkinkan pengguna untuk mengenkripsi data tanpa harus membagikan kunci rahasia terlebih dahulu. Keamanan ElGamal didasarkan pada kesulitan masalah *Discrete Logarithm Problem* (DLP), yang membuatnya tahan terhadap serangan *brute-force* selama parameter kriptografis

P-ISSN 1858-2680
E-ISSN2723-4673

dipilih dengan benar. Selain itu, ElGamal tidak hanya dapat digunakan untuk enkripsi tetapi juga untuk tanda tangan digital (*digital signature*), sehingga memastikan keaslian dan integritas data.

II. TINJAUAN PUSTAKA

A. Implementasi

Implementasi berasal dari bahasa Inggris "to implement" yang artinya mengimplementasikan. Implementasi bukan hanya suatu aktivitas, tetapi implementasi juga merupakan suatu kegiatan yang direncanakan serta dilaksanakan dengan serius dan mengacu pada norma-norma tertentu, guna mencapai tujuan kegiatan (Wahidin, et.all, 2021). Sedangkan menurut Eka dkk (2021) implementasi merupakan realisasi fisik dari basis data dan desain aplikasi yang dicapai dengan menggunakan DDL (*Data Definition Language*) untuk membuat skema basis data dan *database file* yang kosong.

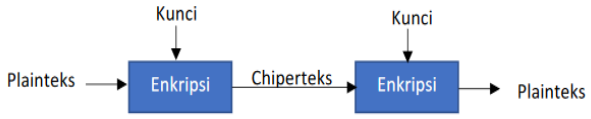
B. Keamanan Data

Keamanan adalah kondisi yang menunjukkan keadaan bebas dari bahaya maupun ancaman. Keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi Masalah keamanan sering berada diurutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Istilah keamanan (*security*) dan proteksi (*protection*) sering digunakan secara bergantian. Untuk menghindari kesalahpahaman, istilah keamanan mengacu ke seluruh masalah keamanan dan istilah mekanisme proteksi mengacu ke mekanisme sistem yang digunakan untuk memproteksi atau melindungi informasi pada sistem komputer (Silalah & Sindar, 2020). Ada begitu banyak peristiwa pertukaran informasi setiap detik di internet. Pertukaran informasi tersebut tentu tak lepas dari terjadinya pencurian informasi oleh pihak-pihak yang tidak bertanggung jawab. Beberapa ancaman keamanan terhadap informasi adalah :

1. *Interruption*, merupakan ancaman terhadap ketersediaan informasi.
2. *Interception*, merupakan ancaman terhadap kerahasiaan informasi.
3. Modifikasi, merupakan ancaman terhadap integritas informasi (modifikasi informasi).
4. *Fabrciation*, merupakan ancaman terhadap integritas informasi (meniru informasi)

C. Pengertian Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*) "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Jadi, kriptologi adalah ilmu dan seni untuk menjaga keamanan pesan (Sasono, et.all, 2023). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi , seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Definisi lain menurut kriptografi yaitu seni untuk menjaga keamanan pesan (Dairi, Asih, & Khairunnisa, 2023). *Criptography* berasal dari bahasa Yunani. Menurut bahasanya, istilah tersebut terdiri dari kata kripto dan graphia. Kripto berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan) (Fauzah & Iqbal, 2021). Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu himpunan yang berisi elemen plainteks dan himpunan yang berisi elemen chipteks. Enkripsi dan dekripsi merupakan fungsi transformasi antara dua himpunan tersebut.Enkripsi adalah proses menggunakan algoritma tertentu untuk mengubah data atau informasi menjadi format yang hampir tidak dapat diidentifikasi sebagai informasi asli. *Plaintext* atau teks biasa adalah informasi atau pesan yang dikirim dalam format yang mudah dibaca atau asli (Ziliwu & Maslan, 2022).Dekripsi adalah kebalikan dari kegiatan enkripsi karena tujuan dari deskripsi mengembalikan pesan yang tersandi atau informasi palsu ke pesan asli. Pada proses mengembalikan isi pesan tersamar harus menggunakan kode yang telah disiapkan sebelumnya. Kegiatan perubahan isi pesan dari plaintext ke ciphertext disebut enkripsi, dan prosedur mengembalikan teks dari ciphertext ke plaintext disebut dekripsi (Ziliwu & Maslan, 2022). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi ciphertext, sedangkan dekripsi adalah proses yang dilakukan untuk mengubah pesan tersandi menjadi pesan yang dapat dibaca dan dimengerti (Ridho et al., 2022).



Gambar 1 Diagram Enkripsi dan Dekripsi

i. Tujuan Kriptografi

Kriptografi bertujuan untuk layanan keamanan yang memiliki beberapa aspek keamanan yang memiliki yaitu sebagai berikut:

P-ISSN 1858-2680
E-ISSN2723-4673

a. Authentication

Layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data atau informasi. Fasilitas yang berkaitan untuk melakukan identifikasi terlebih dahulu antara pengirim dan penerima pesan.

b. Integrity

Keuntungan yang didapatkan dalam menggunakan teknik kriptografi yaitu menjamin bahwa pesan akan diterima dalam keadaan masih utuh dan belum mengalami perubahan selama proses pengiriman. Layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

c. *Confidelity*

Layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima/pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

d. Non-repudiation

Layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya.

ii. Jenis Kriptografi

1. Kriptografi`Klasik

Kriptografi klasik digunakan sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Teknik ini melibatkan pengacakan huruf pada kata terang atau *plaintext* menggunakan penggantian huruf atau substitusi dan pengacakan posisi huruf atau transposisi. Teknik substitusi adalah mengganti karakter dalam *plaintext* menjadi karakter lain yang hasilnya adalah *ciphertext*. Sedangkan transposisi adalah teknik mengubah *plaintext* menjadi *ciphertext* dengan cara melakukan permutasi pada karakternya. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher*, *Vigenere Cipher*, dan *Hill Cipher* (Sasono, et,all, 2023).

2. Kriptografi Modern

Kriptografi Modern merupakan suatu perbaikan dari Teknik yang digunakan pada kriptografi klasik. Algoritma di kriptografi modern ini menggunakan pengolahan dan penggunaan simbol biner yang dibentuk dari kode ASCII (*American Standard Code for Information Interchange*) karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya. Algoritma ini juga memiliki tingkat kesulitan yang lebih kompleks yang menyebabkan kriptanalis sangat sulit memecahkan *ciphertext* tanpa mengetahui kuncinya. Adapun jenis kunci dalam kriptografi modern terdiri dari 3 yaitu: simetris, asimetris, dan hibrida. Pada kriptogarfi modern terdapat berbagai macam algoritma yang memiliki tujuan untuk mengamankan informasi yang dikirim melalui jaringan computer, contoh kriptografi modern yaitu MD5, RC4, AES dan lain-lain (Sasono, et,all, 2023)

a. Algoritma Simetris

Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Karena prosesnya cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara *real time.*

b. Algoritma Asimetris

Algoritma Asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi *deskripsi*. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (*Rivest, Shamir dan Adleman), Rabin, El Gamal.*

III. METODOLOGI PENELITIAN

A. Mettode Penelitian

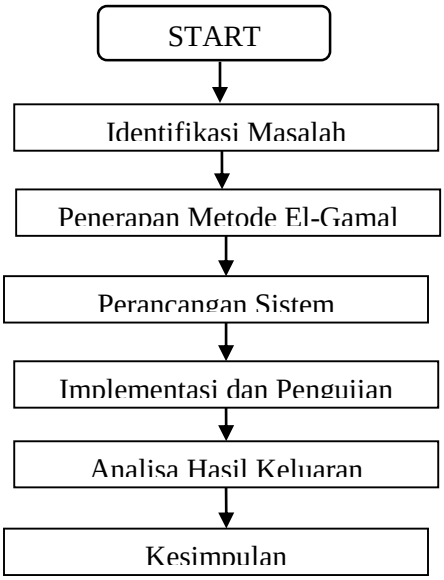
Dalam melakukan penelitian ini, penulis menggunakan metode terapan (*applied research*). Penelitian terapan atau *applied research* dilakukan berkenaan dengan kenyataan-kenyataan praktis, penerapan, dan pengembangan ilmu pengetahuan yang dihasilkan oleh penelitian dasar dalam kehidupan nyata. Penelitian terapan berfungsi untuk mencari solusi tentang masalah-masalah tertentu. Dalam melaksanakan penelitian terapan ini terdapat 5(lima) langkah, diantaranya :

a. Melakukan sesuatu yang sedang diperlukan, dipelajari, diukur, dan diperiksa kelemahannya.
b. Mencari satu dari kelemahan-kelemahan yang diperoleh dipilih untuk penelitian.
c. Mencari dan memberikan solusi dalam melakukan pemecahan masalah
d. Kemudian dilakukan modifikasi sehingga penyelesaian dapat dilakukan untuk diterapkan.

P-ISSN 1858-2680
E-ISSN2723-4673

e. Pemecahan dipertahankan dan menempatkannya dalam suatu kesatuan sehingga jadi bagian permanen dalam satu sistem

Adapun tahapan dari penelitan dapat dilihat pada gambar berikut :



Gambar 2. Tahapan Peneliitan

Berdasarkan pada gambar 1 maka masing-masing langkahnya dapat diuraikan seperti berikut ini:

1. Identifikasi Masalah

Pada tahap ini dirumuskan masalah yang akan menjadi objek penelitian. Perumusan masalah dilakukan untuk menentukan masalah apa saja yang terdapat pada objek penelitian serta memberikan batasan dari permasalahan yang akan diteliti yang berfokus pada pengamanan teks menggunakan El-Gamal.

2. Penerapan Metode El-Gamal

Pada tahap ini dilakukan penerapan terhadap metode *El-Gamal* pada contoh sample teks yang dilakukan secara manual dimana proses pembangkitan kunci, enkripsi dan dekripsi pada teks dihitung secara bertahap untuk menganalisa proses komputasi dari metode *El-Gamal* sehingga dapat membantu dalam membangun aplikasi atau sistem yang akan digunakan dalam mengamankan teks.

3. Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem pengamanan teks menggunakan metode *El-Gamal* yang akan dibangun. Proses pembangkitan kunci, enkripsi dan dekripsi serta tahap – tahapnya dirancang dengan menggunakan diagram bantuk seperti *flowchart* serta perancangan antarmuka.

4. Implementasi dan Pengujian

Implementasi meliputi instalasi dan pengembangan aplikasi yang akan digunakan pada pengamanan teks menggunakan metode *El-Gamal*. Setelah aplikasi dan bangun dan di-instalasi selanjutnya dilakukan pengujian dengan melakukan percobaan enkripsi dan dekripsi terhadap beberapa teks pengujian untuk memperoleh validasi terhadap fungsional dan keluaran dari aplikasi.

5. Analisa Hasil Keluaran

Tahap ini dilakukan dengan menganalisa dan mengamati bagaimana hasil keluaran dari aplikasi yang dibangun. Adapun keluaran yang diamati pada kegiatan ini adalah keluaran dari proses enkripsi dan dekripsi dari aplikasi yang dibangun. Pada hasil enkripsi akan diamati apakah tekshasil enkripsi tidak dapat dikenali lagi atau tidak lagi sama dengan teksaslinya, sedangkan pada tekshasil dekripsi diamati untuk memastikan bahwa tekshasil dekripsi harus sesuai dengan teksasli sebelum di – enkripsi.

6. Kesimpulan

Pada tahap ini dilakukan penyusunan kesimpulan – kesimpulan yang diperoleh dari kegiatan penelitian implementasi metode *El-Gamal* pada teks. Bagaimana hasil keluaran aplikasi serta keadaan – keadaan lain yang terdapat pada aplikasi akan di paparkan di bagian kesimpulan ini

B. Metode Pengumpulan Data

Metode pengumpulan data digunakan untuk memperoleh data yang dapat mendukung permasalahan yang akan dibahas. Sehubungan dengan hal ini maka digunakan metode pengumpulan data yang meliputi :

A. Observasi

Dalam pengumpulan data melalui observasi, penulis mengamati dan menganalisa bagaimana cara sistem melakukan enkripsi dan dekripsi yang berbentuk data.

B. Studi Pustaka

Studi pustaka adalah suatu metode pengumpulan data yang diambil dari perpustakaan yang berupa karya ilmiah, jurnal, buku-buku serta dari *internet* yang berhubungan dengan penulisan ini. Tujuan dari studi pustaka ini adalah untuk mendalami dan memperoleh keterangan yang lengkap terhadap objek yang diteliti

IV.HASIL DAN PEMBAHASAN

A. Hasil Aplikasi

Sesuai dengan analisa dan perancangan seperti yang telah dijabarkan pada bab sebelumnya yaitu bab metodologi penelitian, maka pada bagian ini akan dipaparkan hasil dari aplikasi yang dibangun menggunakan perancangan yang telah di lakukan pada bab sebelumnya. Pada bab ini pembahasan akan dilakukan terhadap hasil dari sistem yang dibangun, fungsional sistem dan analisis terhadap kinerja sistem berdasarkan hasil output yang dihasilkan oleh sistem.

P-ISSN 1858-2680
E-ISSN2723-4673

Implementasi kriptografi metode Elgamal pada sistem yang dibangun yaitu proses enkripsi dan dekripsi data teks. Pada aplikasi ini terdapat beberapa antarmuka (*interface*) diantaranya adalah sebagai berikut :

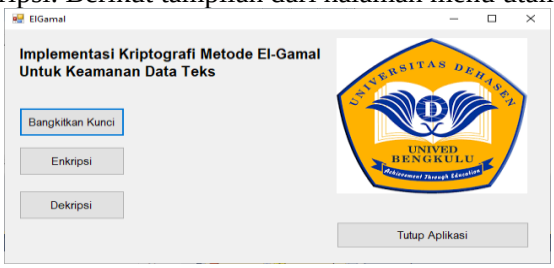
1. *Form* Menu Utama
2. *Form* Bangkitkan Kunci
3. *Form* Enkripsi
4. *Form* Dekripsi

B. Pembahasan Sistem

Pada aplikasi implementasi implementasi kriptografi metode Elgamal untuk keamanan data teks terdapat beberapa *interface* atau antarmuka yang di desain untuk mempermudah *user* atau pemakai dalam menggunakan atau menjalankan aplikasi ini. Pada sub bab ini akan menjabarkan *form-form* yang ada beserta fungsi dari masing-masing *form* yang ada pada aplikasi

1. *Form* Menu Utama

Form menu utama adalah bagian pertama sistem yang akan diakses oleh pengguna. Pada bagian ini pengguna dapat mengarahkan atau menavigasikan dirinya untuk melakukan proses bangkitkan kunci, enkripsi dan dekripsi. Berikut tampilan dari halaman menu utama.



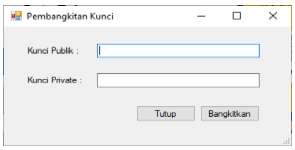
Gambar 3. Tampilan Menu Utama Aplikasi

Adapun bagian-bagian dari menu utama yaitu:

a. Pembangkit Kunci
   Fungsi dari menu pembangkit kunci untuk membangkitkan kunci private dan kunci publik
b. Enkripsi
   Fungsi dari menu enkripsi adalah untuk menampilkan tampilan enkripsi yang digunakan untuk meng-enkripsi Teks dari pengguna
c. Dekripsi
   Fungsi dari menu dekripsi adalah untuk menampilkan tampilan dekripsi yang digunakan untuk men-dekripsi Teks dari pengguna
d. Tutup Aplikasi
   Fungsi dari menu *exit* adalah untuk keluar dan menutup aplikasi

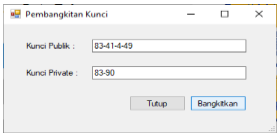
2. *Form* Bangkitkan Kunci

Sebelum dapat melakukan proses enkripsi atau pun dekripsi, pertama kali pengguna harus melakukan pembangkitan kunci public dan kunci private untuk dapat menggunakan aplikasi. Berikut tampilan program pada saat membangkitkan kunci



Gambar 4. Tampilan Form Pembangkitan Kunci

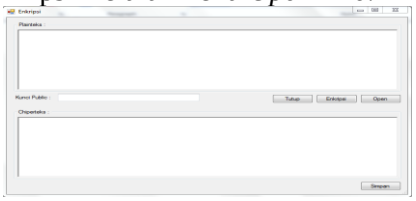
Pembangkitan kunci ini dilakukan dengan memanfaatkan algoritma pembangkit kunci yang terdapat pada metode El-Gamal. Kunci yang dibangkitkan kemudian akan dibagi menjadi 2 yaitu kunci public yang akan di distribusikan pada seluruh pengguna sistem untuk proses enkripsi sedangkan kunci private hanya akan dimiliki oleh satu orang yaitu penerima data yang akan digunakan untu proses dekripsi. Untuk membangkitkan kunci dengan cara meng-klik tombol "Bangkitkan". Adapun hasil kunci yang dihasilkan



Gambar 5. Proses Pembangkitan Kunci Public dan Private

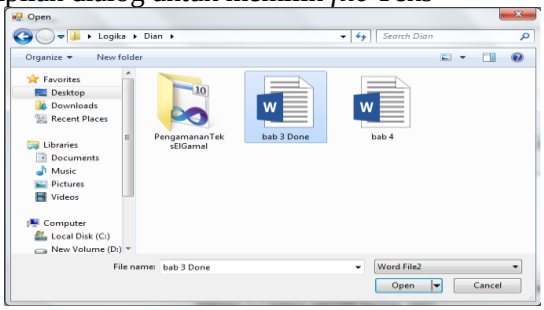
3. *Form* Enkripsi

Form ini digunakan untuk melakukan enkripsi terhadap Teks digital yang di masukkan oleh pengguna. Pengguna pertama sekali membuka berkas Teks yang akan di enkripsi melalui menu *Open File*.



Gambar 5.Form Enkripsi

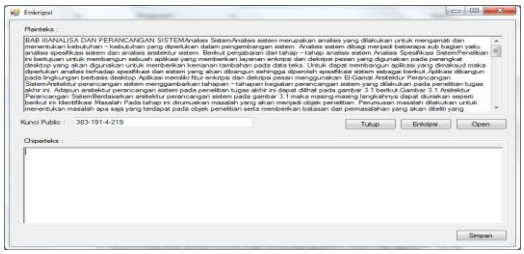
Berkas Teks dapat dibuka dengan menggunakan tombol "*Open File*" yang kemudian akan menampilkan dialog untuk memilih *file* Teks yang akan di-enkripsi. Tampilan dialog untuk memilih *file* Teks



Gambar 7. Dialog Memilih Berkas Teks

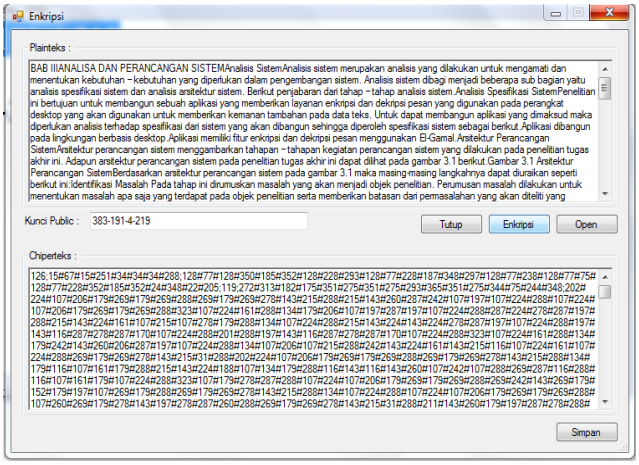
Setelah Teks dibuka aplikasi akan menampilkan tampilan Teks yang dipilih.

P-ISSN 1858-2680
E-ISSN2723-4673



Gambar 8. Tampilan Teks Awal

Selanjutnya pengguna dapat melakukan proses enkripsi dengan memasukkan kunci dan melakukan proses enkripsi dengan menekan tombol "Enkripsi" sehingga proses enkripsi akan dilakukan dan akan menampilkan Teks digital seperti yang terlihat pada gambar 4.7. pada proses enkripsi ini digunakan kunci atau password "8-191-4-219"



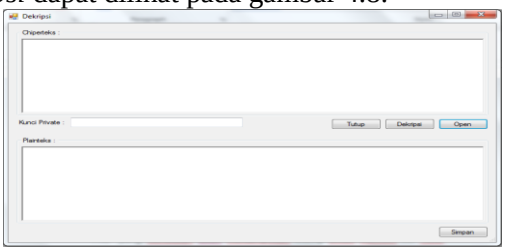
Gambar 9. Tampilan Hasil Proses Enkripsi

Teks hasil enkripsi kemudian dapat disimpan menjadi file menggunakan tombol "*Save*" sehingga dapat di dekripsi kembali menggunakan *form dekripsi* yang akan dijabarkan pada sub bab berikutnya.

Hasil enkripsi menunjukkan objek Teks yang terdapat pada teks tidak dapat dikenali lagi sehingga proses enkripsi berhasil mengamankan informasi yang terdapat pada teks yang dienkripsi

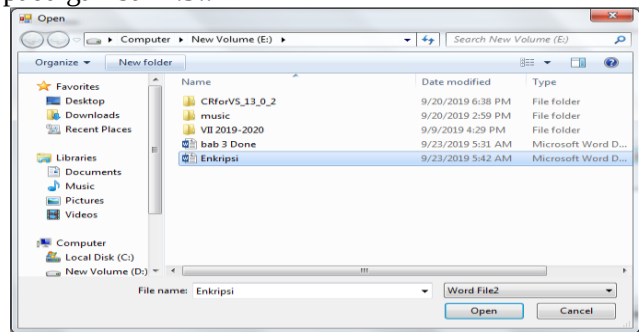
4. *Form* Dekripsi

Form ini digunakan untuk melakukan dekripsi terhadap Teks yang terenkripsi yang di masukkan oleh pengguna. Pengguna pertama sekali membuka berkas Teks yang akan di dekripsi. Adapun tampilan dari *form dekripsi* dapat dilihat pada gambar 4.8.



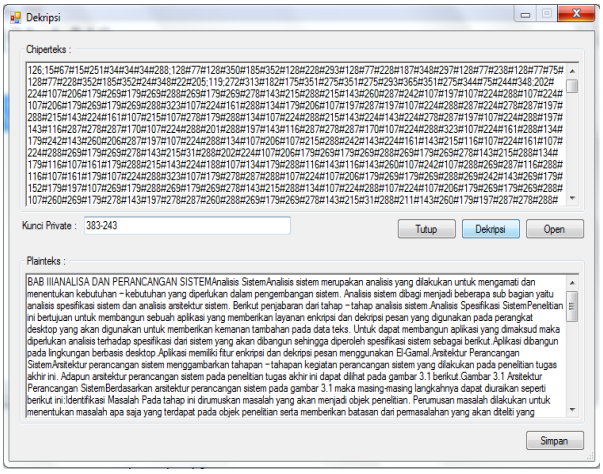
Gambar 10. Tampilan Dekripsi

Berkas Teks dapat dibuka dengan menggunakan tombol "*Open File*" yang kemudian akan menampilkan dialog untuk memilih *file* Teks yang akan di-dekripsi. Tampilan dialog untuk memilih *file* Teks dapat dilihat pada gambar 4.9..



Gambar 11. Dialog memilih Teks terenkripsi

Setelah Teks terenkripsi dibuka selanjutnya pengguna dapat melakukan proses dekripsi dengan memasukkan kunci yang telah digunakan pada saat enkripsi sebelumnya dan melakukan proses dekripsi dengan menekan tombol "Dekripsi" sehingga proses dekripsi akan dilakukan dan akan menampilkan Teks asli kembali.



Gambar 12. Tampilan Hasil Proses Dekripsi

Teks hasil dekripsi kemudian dapat disimpan menjadi *file* menggunakan tombol "*Save*" sehingga dapat di gunakan lebih lanjut oleh pengguna.

a. Pengujian Sistem

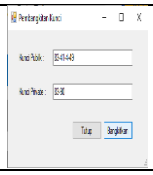
Pengujian yang dilakukan pada aplikasi ini adalah dengan menggunakan teknik *black box*, teknik *black box* ini merupakan teknik pengujian yang berfokus pada keluaran hasil dari respon, atau secara simpel untuk mengetahui apakah ada *error* atau ada fungsi yang tidak berjalan sesuai dengan harapan. Tujuan dari pengujian ini adalah untuk menjamin bahwa perangkat lunak yang dibangun memiliki kualitas yang handal, yaitu mampu mempresentasikan kajian pokok dari spesifikasi analisis, perancangan dan pengkodean dari perangkat lunak itu sendiri. Berikut tabel pengujian *black box*

P-ISSN 1858-2680
E-ISSN2723-4673

Tabel 1 Pengujian *Black Box*

Jenis Uji	Keterangan Uji	Jenis Pengujian
Bangkitkan kunci	Proses Generate Key Public dan Private	*Black Box*
Open	Mencari file	*Black Box*
Enkripsi	Proses Enkripsi	*Black Box*
Dekripsi	Proses Deksipsi	*Black Box*

Tabel 2 Pengujian *Aplikasi*

Kasus dan Hasil Uji File			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Bangkitkan kunci	Kunci public dan private berhasi digenerate		[x] diterima [ ] ditolak
Masukan file.docx	File dapat diproses	File berhasil diproses	[x] diterima [ ] ditolak
Enkripsi	File berhasil di enkripsi	file berhasil berubah sesuai dengan kunci yang digunakan 	[x] diterima [ ] ditolak
Dekripsi	File berhasil di dekripsi	File berhasil kembali menjadi plainteks dengan menggunakan kunci private 	[x] diterima [ ] ditolak

V. PENUTUP

A. Kesimpulan

Dalam perancangan, pembuatan, dan pengujian penerapan algortima kriptografi El-Gamal pada pengamanan data terdapat beberapa kesimpulan diantaranya adalah sebagai berikut :

1. ALgoritma El-Gamal dapat diimplementasikan dengan baik pada data teks.
2. Algoritma El-Gamal dapat memberikan keamanan tambahan bagi data yang dimiliki oleh sekolah, hal ini dikarenakan data teks yang dimiliki oleh pengguna akan di eknripsi dan digantikan dengan deretan karakter yang tidak mewakilkan isi dari data yang asli.
3. Aplikasi dapat berjalan sesuai dengan tujuan awal algoritma dan dapat melakukan proses enkripsi, dekripsi, dan juga pembangkitan kunci dengan baik
4. Sistem pengamaman data yang dibuat oleh penulis dapat memberikan keamanan tambahan pada data teks, dikarenakan data yang sudah dienkripsi tidak lagi bisa dikaitkan dengan informasi apapun.

B. Saran

Adapun saran-saran yang bisa diberikan untuk program ini agar bisa didapatkan hasil yang maksimal adalah:

1. Untuk pengembangannya aplikasi ini juga dapat sekaligus dibuat dengan memberikan keamanan tambahan seperti steganografi atau kompresi data untuk memberikan keamanan yang lebih baik..
2. Untuk dapat lebih menggali kemampuan dari algoritma El-Gamal ada baiknya algoritma dibandingkan dengan algoritma kriptografi lain atau dimodfikasi

DAFTAR PUSTAKA

[1] Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *JTSI (Jurnal Teknologi Sistem Informasi)*, 394-405.

[2] Ayumida, S., Azis, M. S., & Fiano, Z. G. (2020). Implementasi Program Administrasi Pembayaran Berbasis Dekstop (Studi Kasus: SMA Negeri 1 Cikampek). *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi dan Komunikasi*, 72-83.

[3] Dairi, M., Asih, M. S., & Khairunnisa. (2023). Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan. *Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI)* , 214-223.

[4] Ekta , N., Christian, A., & Wijaya, K. (2021). Implementasi Metode (User Centered Design) PadaRancang Bangun Sistem Informasi Perpustakaan : Studi Kasus : SMK Negeri 1 Gelumbang. *Jurnal Pengembangan Sistem Informasi dan Informatika*, 69-77.

[5] Fauzi, R. (2024). Implementasi Algoritma Kriptografi Elgamal Untuk Pesan Rahasia Berbasis Web Di Markas Pmi Kota Tangerang. *Jurnal Ilmu Komputer (JIK)*, 50-54.

[6] Hasan, H. I., & Safrizal, S. (2024). Penerapan Algoritma Affine Cipher Untuk Keamanan Data Registrasi Siswa Baru. *Seminar Nasional Multi Disiplin Ilmu (SENADIMU)*, 1029-1042.

[7] Limantoro, R. R., & Kristiadi, D. P. (2021). Pengembangan Sistem Informasi Pendataan Green Folder Menggunakan Metode Berorientasi Objek Dan UML Berbasis Web Pada TKHarvest

P-ISSN 1858-2680
E-ISSN2723-4673

Christian School. *JURNAL SISTEM INFORMASI DAN TEKNOLOG (SINTEK)*, 7-14.

[8] Muafi, Wijaya, A., & Aziz, V. A. (2020). Sistem Pakar Mendiagnosa Penyakit Mata Pada Anusia Menggunakan Metode Forward Chaining. *Jurnal Komputasi dan Teknologi Informasi*, 43-49.

[9] Nugraha, S. N. (2024). Penerapan Algoritma Kriptografi Elgamal Pada Aplikasi Pengamanan Pesan Berbasis Website. *JITET (urnal Informatika dan Teknik Elektro Terapan)*, 2513-2524.

[10] Ridho, A., Mutia, C., & Sinaga, A. P. (2022). Analisis Enkripsi Dan Dekripsi Cipher Teks Menggunakan Kombinasi Gronsfeld Cipher Dengan Reverse Cipher. *JTIK (Jurnal Teknik Informatika Kaputam)*, 87-94.

[11] Samsudin, A., & Islami, H. H. (2023). Sistem Pengaduan Masyarakat Menggunakan Metode Agile Extreme Programming. *Jurnal Infotex*, 214-226.

[12] Sasono, D. M., Tahir, M., Angel M, F., Azizah, M., Utami, L. F., & Septiana, N. (2023). Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Kompute. *Jurnal Informasi, Sains dan Teknologi*, 72-77.

[13] Siagian, K. Z., & Triandi, B. (2024). Implementasi Aplikasi KeamananData Karyawan Pada PT. Jaya Diesel Menggunakan Metode Affine Chiper Dan Rsa Berbasis Web. *Jurna l Info Digit (JDI)*, 672-683.

[14] Silalah, L., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *Jurnal Nasional Komputasi dan Teknologi Informasi*, 182-186.

[15] Sutrisno, J., & Karnadi, V. (2021). Aplikasi Pendukung Pembelajaran Bahasa Inggris Menggunakan Media Lagu Berbasis Android. *JURNAL COMASIE*, 31-41.

[16] Wahidin, U., Sarbini, M., Maulida, A., & Wangsadanureja, M. (2021). Implementasi Pembelajaran Agama Islam Berbasis Multimedia Di Pondok Pesantren. *Edukasi Islami: Jurnal Pendidikan Islam*, 21-32.

P-ISSN 1858-2680
E-ISSN2723-4673