Implementasi Algoritma *Rivest Shamir Adleman* Untuk Keamanan Pesan Teks

[1]Haggy Sandy Prayogy, [2]Indra Kanedi, [3]Devi Sartika

[1] Mahasiswa, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Jl. Siti Khadijah No. 562, Bengkulu Utara (Telp. (0736) 22027, 26957 Fax. (0736) 341139; e-mail: haggy23010177p@gmail.com
[2,] Dosen Tetap, Program Studi Sistem Informasi, 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
[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: devisartika@unived.ac.id

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

Abstract*-Security is a set of procedures, steps, and policies to prevent and monitor unauthorized access, problem solving, disclosure, and disruption of computer data communication. Data or message security can be achieved using cryptography. Cryptography is an important component for communication and information transmission through security services. Cryptography is both an art and a science that produces secret messages. One cryptographic method that can be utilized is RSA method. RSA is an asymmetric cryptographic method that operates in block mode and requires two different keys for the encryption and decryption processes. The advantage of this algorithm is that its difficulty lies in factoring non-prime numbers into their prime factors. The results of the tests conducted show that RSA algorithm can provide additional security for files by using different keys during the encryption and decryption processes. This is because the text data owned by the user will be encrypted and replaced with a series of numbers that do not represent the content of the original data.*
Keywords: Cryptography, Rivest Shamir Adleman, Data Security.

Intisari*-Keamanan merupakan sekumpulan prosedur, tahapan, dan kebijakan untuk menghentikan dan memonitoring akses tidak sah, problem solving, pengungkapan, gangguan pada suatu komunikasi data komputer. Pengamanan data atau pesan dapat dilakukan dengan menggunakan kriptografi. Kriptografi salah satu komponen penting untuk komunikasi dan transmisi informasi melalui layanan keamanan. Kriptografi merupakan seni maupun ilmu yang menghasilkan pesan yang rahasia. Salah satu metode kriptografi yang bisa dimanfaatkan adalah metode RSA. RSA merupakan metode kriptografi asimetris yang beroperasi pada mode blok dan membutuhkan dua kunci yang berbeda pada proses enkripsi dan dekripsi nya. Keunggulan dari algoritma ini adalah tingkat kesulitannya adalah dalam memfaktorkan bilangan non prima menjadi faktor primanya. Dimana hasil pengujian yang telah dilakukan diperoleh hasil dimana Algoritma RSA dapat memberikan keamanan tambahan terhadap file dengan menggunakan kunci yang berbeda pada saat proses enkripsi dengan dekripsi, hal ini dikarenakan data teks yang dimiliki oleh pengguna akan di enkripsi dan digantikan dengan deretan angka yang tidak mewakili isi dari data yang asli.*
Kata Kunci: Kriptografi, Rivest Shamir Adleman, Keamanan Data.

I. PENDAHULUAN

Kemajuan dan perkembangan teknologi informasi menjadi salah satu alasan perlunya peningkatan keamanan data dalam melakukan aktivitas di berbagai bidang seperti bisnis, industri, kesehatan, pendidkan dan. Kemajuan komunikasi data kini berdampak pada hampir semua bidang, sehingga mengakibatkan kebutuhan akan teknik dan metode yang dapat menjaga serta melindungi infromasi dengan cara menyandikan atau membuat isi informasi ke dalam bentuk kode atau bentuk acak yang tidak dapat dipahami oleh pihak yang tidak bertanggung jawab. Keamanan merupakan sekumpulan prosedur, tahapan, dan kebijakan untuk menghentikan dan memonitoring akses tidak sah, *problem solving*, pengungkapan, gangguan pada suatu komunikasi data komputer. Beberapa aspek yang perlu diperhatikan pada keamanan data yang didasarkan dengan kebutuhan dalam hal keamanan, yaitu rahasia yang berupa akses untuk membaca data dan informasi di dalamnya. Data dan informasi tersebut hanya dapat diakses dan dibaca oleh pihak yang berkepentingan. Pengamanan data atau pesan dapat dilakukan dengan menggunakan kriptografi. Kriptografi salah satu komponen penting untuk komunikasi dan transmisi informasi melalui layanan keamanan. Kriptografi merupakan seni maupun ilmu yang menghasilkan pesan yang rahasia (Yusrizal, 2019), selain itu kriptografi juga memiliki sebuah kunci untuk mengubah kode atau pesan itu sendiri kembali seperti semula. Dalam bidang kriptografi terdapat dua konsep yang sangat penting yakni 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, Mutia, & Sinaga, 2022). Kebutuhan akan keamanan data yang lebih baik telah melahirkan berbagai jenis metode dan teknik yang dapat digunakan pada kegiatan pengamanan pesan salah satu diantaranya adalah metode RSA (*Rivest Shamir Adleman*) *Rivest Shamir Adleman* (RSA) merupakan metode kriptografi pertama yang menggunakan *public key* dalam prosesnya. RSA merupakan metode kriptografi asimetris yang beroperasi pada mode blok. RSA membutuhkan dua kunci yang berbeda pada proses enkripsi dan dekripsi nya sehingga proses enkripsi dan dekripsi hanya dapat dilakukan oleh pihak yang memiliki kunci yang sesuai. Walaupun kunci enkripsi

P-ISSN 1858-2680
E-ISSN 2723-4673

diketahui oleh pihak yang tidak berhak, pesan tidak dapat di dekripsi menggunakan kunci tersebut. Keunggulan dari algoritma ini adalah tingkat kesulitanya adalah dalam memfaktorkan bilangan non prima menjadi faktor primanya. Di dalam implementasinya, algoritma RSA membangkitkan dua kunci. Yang pertama adalah kunci umum atau *public key*, kunci ini digunakan untuk melakukan enkripsi. Sedangkan kunci yang kedua adalah kunci privat atau *private key*. Kunci ini digunakan pada saat melakukan dekripsi *chipertext* menjadi *plaintext* yang asli.

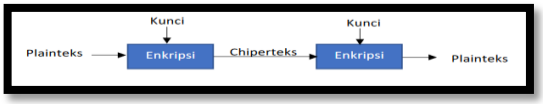
II. TINJAUAN PUSTAKA

A. Pengertian Implementasi

Implementasi adalah pelaksanaan dan penerapan, dimana kedua hal ini bermaksud untuk mencari bentuk tentang hal yang disepakati terlebih dahulu. Tujuan dari implementasi sebuah sistem adalah untuk menyelesaikan desain sistem yang telah disetujui, menguji serta mendokumentasikan program-program dan prosedur sistem yang diperlukan, memastikan bahwa personil yang terlibat dapat mengoperasikan sistem yang baru dan memastikan bahwa konversi sistem lama ke sistem baru dapat berjalan dengan baik dan benar (Gunawan & Kirman, 2019)

B. 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). Terdapat dua proses dalam kriptografi yaitu proses enkripsi dan proses dekripsi. Enkripsi merupakan proses untuk melakukan perubahan kode dari yang sebelumnya dapat dipahami oleh manusia untuk membacanya menjadi sesuatu tidak dapat dipahami (*unreadable*) bagi manusia, pengubahan itu bisa mengubah teks asli menjadi susunan karakter maupun simbol dengan susunan yang jauh berbeda dari teks aslinya. (Ridho, Mutia, & Sinaga, 2022). Sedangkan 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)



Gambar 1 Diagram Enkripsi dan Dekripsi

Prinsip-prinsip yang mendasari kriptografi yakni:

1. *Secrecy* (kerahasiaan), layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka maupun menghapus informasi yang telah disandi.
2. *Authentication*, berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Dimana informasi yang dikirimkan melalui kanal harus diautentifikasi keaslian, isi datanya, waktu pengiriman dan lain-lain.
3. Hak Akses terhadap suatu *file* atau fasilitas lain dalam sebuah sistem pemrosesan informasi masih dalam area lain dimana gagasan kriptografi telah diterapkan

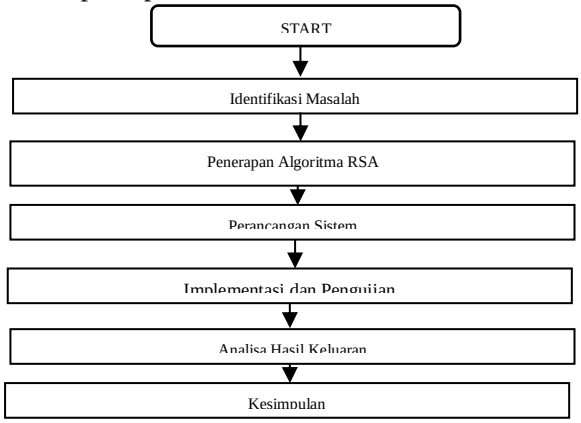
C. Metode RSA (*Rivest Shamir Adleman*)

Metode RSA pertama kali diperkenalkan pada tahun 1976 oleh tiga peneliti yang berasal dari *Massachusetts Institute of Technology*, yaitu Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari inisial ketiga peneliti tersebut (Zachary, Sylviani, & Kurniadi, 2024). Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi factor-faktor prima. Pemfaktoran dilakukan unutk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi factor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin (Firmansyah & Permana, 2019).

III. METODOLOGI PENELITIAN

A. Metode Penelitian

Adapun tahapan sistem kegiatan penelitian yang dilakukan pada penelitian



Gambar 2. Tahapan Penelitian

P-ISSN 1858-2680
E-ISSN 2723-4673

Keterangan :

a. 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 dokumen menggunakan metode RSA.

b. Penerapan Metode RSA

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

c. Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem pengamanan dokumen menggunakan metode RSA yang akan dibangun. Proses pembangkitan kunci, enkripsi dan dekripsi serta tahap – tahapnya dirancang dengan menggunakan diagram bantu seperti *flowchart* serta perancangan antarmuka.

d. Implementasi dan Pengujian

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

e. 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 data hasil enkripsi tidak dapat dikenali lagi atau tidak lagi sama dengan data aslinya, sedangkan pada data hasil dekripsi diamati untuk memastikan bahwa data hasil dekripsi harus sesuai dengan data asli sebelum di – enkripsi.

f. Kesimpulan

Pada tahap ini dilakukan penyusunan kesimpulan yang diperoleh dari kegiatan penelitian implementasi RSA pada data. Bagaimana hasil keluaran aplikasi serta keadaan – keadaan lain yang terdapat pada aplikasi akan di paparkan di bagian kesimpulan ini.

IV. HASIL DAN PEMBAHASAN

A.Hasil Aplikasi

Aplikasi implementasi metode lucas number pada pengamanan berkas digital dibangun 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. Adapun sistem yang dikembangkan pada penelitian ini terdiri dari beberapa *form* yaitu *form* utama, *form* Pembangkitan Kunci, *form* Enkripsi, *form* dan *form* Dekripsi berdasarkan metode yang digunakan.

B.Implementasi Sistem

A. Halaman Menu Utama

Pada tampilan halaman Menu Utama, terdapat informasi mengenai judul dari aplikasi yang dibangun. Tampilan halaman pembuka merupakan tampilan yang pertama sekali muncul pada saat aplikasi dijalankan.

Gambar 3. Tampilan Halaman Pembuka

Adapun bagian – bagian dari menu utama yaitu :

1. Pembuatan Kunci

Fungsi dari menu pembuatan kunci adalah untuk menampilkan tampilan pembuatan kunci yang dapat membuat kunci baru bagi pengguna yang belum memiliki kunci baik kunci *public* maupun kunci *private*.

2. Enkripsi Dokumen

Fungsi dari menu enkripsi adalah untuk menampilkan tampilan enkripsi yang digunakan untuk meng-enkripsi dokumen dari pengguna.

3. Dekripsi Dokumen

Fungsi dari menu dekripsi adalah untuk menampilkan tampilan dekripsi yang digunakan untuk men-dekripsi dokumen dari pengguna.

4. Keluar

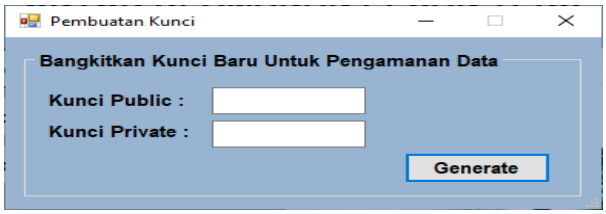
Fungsi dari menu keluar adalah untuk keluar dan menutup aplikasi.

B. Form Pembuatan Kunci

Form ini digunakan untuk melakukan pembuatan kunci baru yang dapat digunakan oleh pengguna pada proses enkripsi dan dekripsi pada berkas digital. Kunci yang dibuat terdiri dari dua jenis kunci yaitu kunci *public* dan kunci *private*. Pembuatan kunci dilakukan dengan mengambil nilai waktu detik dan menit dari saat proses pembuatan kunci dilakukan dan melakukan proses mengikuti algoritma dari *Rivest*

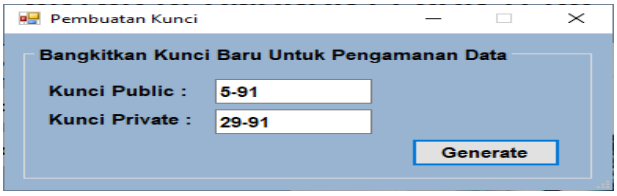
P-ISSN 1858-2680
E-ISSN 2723-4673

Shamir Adleman (RSA) sehingga dapat digunakan baik pada proses enkripsi dan dekripsi.



Gambar 4. Tampilan Pembuatan Kunci

Proses pembuatan kunci dapat dilakukan dengan menekan tombol "Generate" sehingga aplikasi akan membuat kunci *public* dan kunci *private*

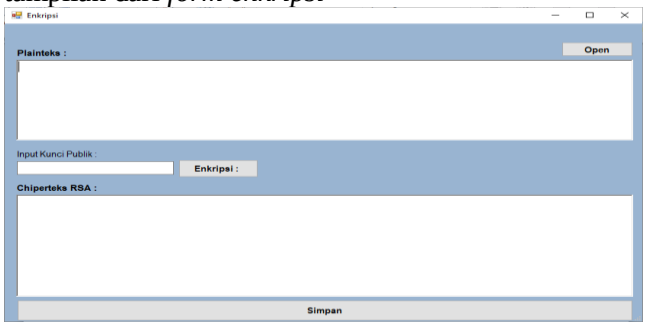


Gambar 5. Hasil Pembuatan Kunci

Hasil pembangkitan kunci seperti yang terlihat pada gambar 4.3 menghasilkan dua kunci berbeda yaitu "5-91" untuk kunci public dan "29-91" untuk kunci private.

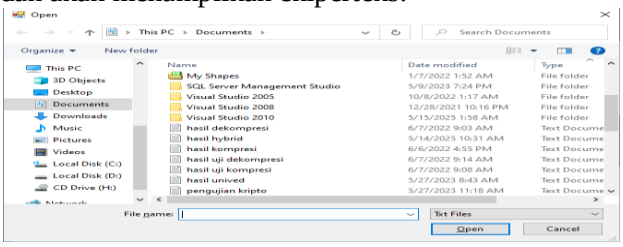
C. *Form* Enkripsi Dokumen

Form ini digunakan untuk melakukan enkripsi terhadap *file* atau dokumen yang di masukkan oleh pengguna. Pengguna pertama sekali membuka *file* atau dokumen yang akan di enkripsi. Adapun tampilan dari *form enkripsi*

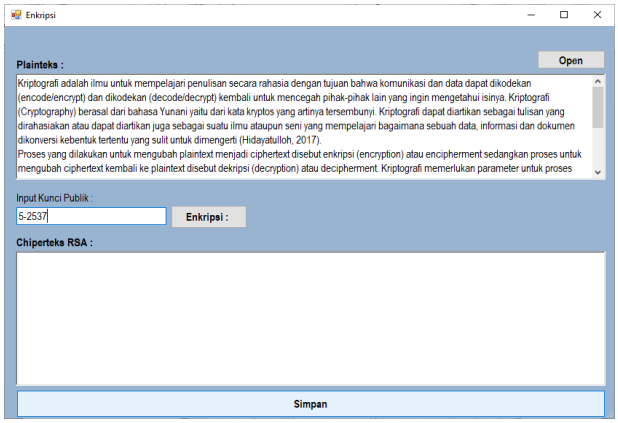


Gambar 6. *Form* Enkripsi Dokumen

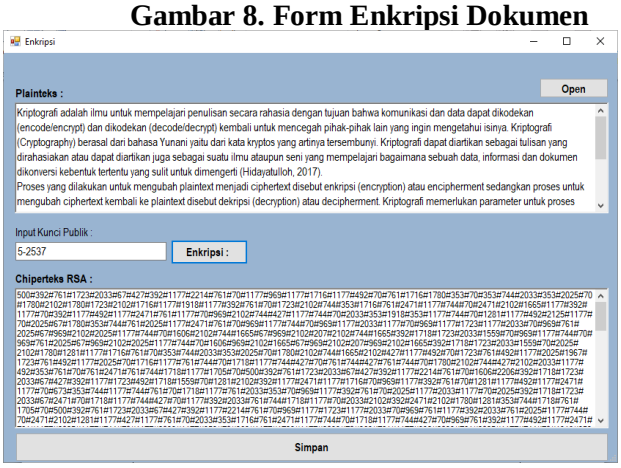
Seperti yang dapat kita lihat diatas, halaman tersebut memiliki dua halaman tampilan yaitu halaman data teks asli dan halaman data chiperteks. Seperti yang tampak pada halaman enkripsi, kunci yang digunakan adalah kunci publik. Pada algoritma RSA kunci *public* dan kunci *private* di generate sebelum proses enkripsi dan dekripsi. *File* atau dokumen dapat dibuka dengan menggunakan tombol "*Open*" yang kemudian akan menampilkan dialog untuk memilih *file* atau dokumen yang akan di – enkripsi. Setelah berkas dibuka selanjutnya pengguna dapat melakukan proses enkripsi dengan memasukkan kunci yang telah dibangkitkan sebelumnya dan melakukan proses enkripsi dengan menekan tombol "Enkripsi" sehingga proses enkripsi akan dilakukan dan akan menampilkan chiperteks.



Gambar 7. Halaman Load Data Teks

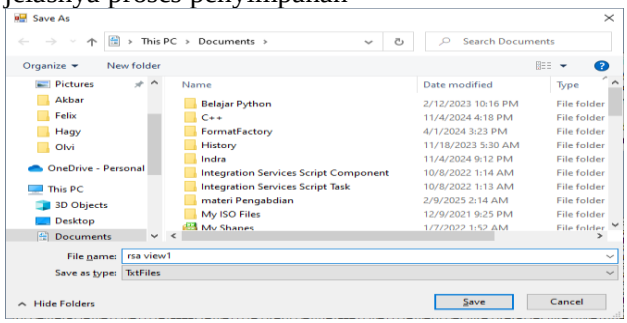


Gambar 8. Form Enkripsi Dokumen



Gambar 9. Tampilan hasil proses enkripsi

Pada gambar diatas dapat dilihat kunci yang digunakan adalah kunci publik yaitu "5-91". Gambar diatas jug menunjukkan proses enkripsi yang berhasil dimana sistem mampu mengubah data dan bisa merepresentasikan isi dari data asli. Kemudian data hasil enkripsi atau chipperteks akan disimpan untuk keperluan pengujian proses dekripsi. Untuk lebih jelasnya proses penyimpanan

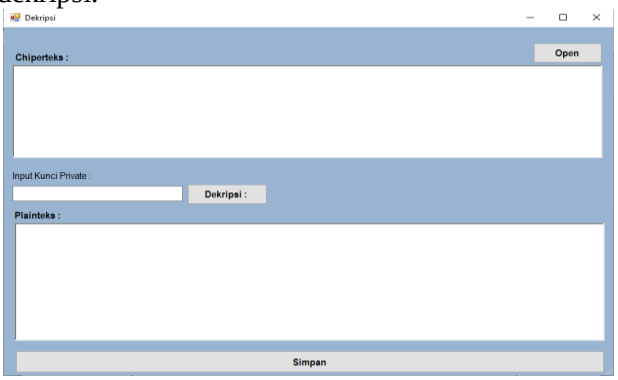


Gambar 10. *Dialog Box* Penyimpanan Hasil Enkripsi

P-ISSN 1858-2680
E-ISSN 2723-4673

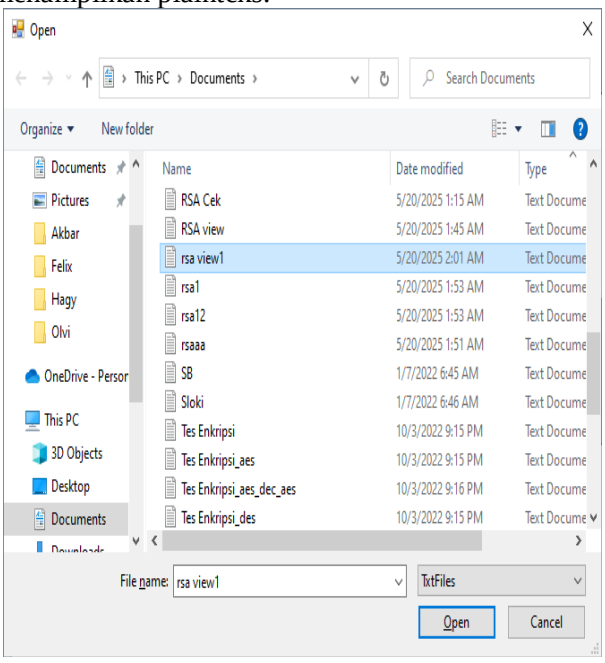
D. *Form* Dekripsi Dokumen

Form ini digunakan untuk melakukan dekripsi terhadap *file* atau dokumen chiperteks yang di masukkan oleh pengguna. Pengguna pertama sekali membuka berkas digital chiperteks yang akan di dekripsi.



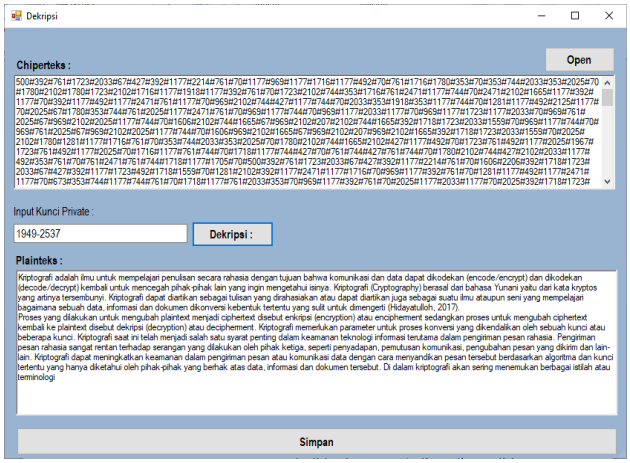
Gambar 11. *Form* Dekripsi Dokumen

File atau dokumen chiperteks dapat dibuka dengan menggunakan tombol "Open" yang kemudian akan menampilkan dialog untuk memilih file chiperteks yang akan di – dekripsi. Setelah chiperteks dibuka selanjutnya pengguna dapat melakukan proses dekripsi dengan memasukkan kunci yang telah dibangkitkan sebelumnya dan melakukan proses dekripsi dengan menekan tombol "Dekripsi" sehingga proses dekripsi akan dilakukan dan akan menampilkan plainteks.



Gambar 12. Halaman Pemilihan Data Chiperteks

Setelah data chiperteks berhasil diload, langkah selanjutnya adalah melakukan proses dekripsi. Kunci yang digunakan adalah kunci *private* yaitu "1949-2537". Untuk lebih jelasnya dapat dilihat pada gambar berikut



Gambar 13. Tampilan Hasil Proses Dekripsi

File atau dokumen hasil dekripsi kemudian dapat disimpan menjadi file menggunakan tombol "Simpan" sehingga dapat di gunakan lebih lanjut oleh pengguna.

B. Pengujian

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*

Tabel 1 Pengujian

Kasus dan Hasil Uji			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Masukan file.txt	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 sama pada saat enkripsi	[x] diterima [ ] ditolak

Tabel2 Kasus dan Hasil Uji

Kasus dan Hasil Uji			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Masukan file.txt	File dapat diproses	File berhasil diproses	[x] diterima [ ] ditolak

P-ISSN 1858-2680
E-ISSN 2723-4673

Kasus dan Hasil Uji			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Enkripsi	File berhasil di enkripsi	File berhasil berubah sesuai dengan kunci yang digunakan 	[x] diterima [ ] ditolak
Dekripsi tanpa kunci private	Akan tampil kotak yang yang memberi peringatan untuk memasukkan kunci private		[x] diterima [ ] ditolak
Dekripsi dengan kunci private	File berhasil di dekripsi	File berhasil di dekprisi dan kembali menjadi plainteks 	[x] diterima [ ] ditolak

V. PENUTUP

A. Kesimpulan

Berdasarkan pembahasan dan pengujian program yang dilakukan, maka dapat di tarik kesimpulan sebagai berikut :

1. Algoritma RSA dapat memberikan keamanan tambahan file, hal ini dikarenakan data teks yang dimiliki oleh pengguna akan di eknripsi dan digantikan dengan deretan angka yang tidak mewakilkan isi dari data yang asli.
2. Dari hasil pengujian yang telah dilakukan dapat dilihat bahwa aplikasi yang dikembangkan dapat bekerja sesuai dengan yang diharapkan. Pengujian normal menghasilkan chiperteks dan plainteks yang sesuai.
3. Pengujian enkripsi dan dekripsi menggunakan kunci yang berbeda untuk melihat fungsi aplikasi jika diberikan kunci yang tidak sama pada saat proses enkripsi dengan dekripsi. Dari pengujian yang dilakukan chiperteks tidak dapat dikembalikan yang mana menunjukkan hal yang normal dikarenakan metode yang digunakan merupakan kriptografi simetris sehingga proses dekripsi hanya bisa dilakukan menggunakan kunci yang sama dengan kunci pada saat dekripsi

B. Saran-saran

Adapun saran-saran yang bisa diberikan oleh penulis untuk memberikan kontribusi bagi pengembangan .program ini agar bisa didapatkan hasil yang maksimal adalah:

1. Penelitian selanjutnya diharapkan dapat mengembangkan lagi kompleksitas kombinasi kriptografi berbasis karakter yang dapat meningkatkan keamanan khususnya pada pesan teks.
2. Memberikan keamanan tambahan seperti steganografi atau kompresi data didalam sistem untuk memberikan keamanan yang lebih baik bagi perusahaan atau pengguna sistem
3. Penelitian selanjutnya diharapkan dapat mengembangkan aplikasi keamanan pada *framework* yang berbeda seperti website dan lain sebagainya

DAFTAR PUSTAKA

[1] Alfina, O., & Harahap, F. (2019). Pemodelan UML Sistem Pendukung Keputusan Dalam Penentuan Kelas Siswa Siswa Tunagrahita. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 143-150.

[2] Andhika, D. I., Muharrom, M., Prayitno, E., & Siregar, J. (2022). Rancang Bangun Sistem Penerimaan Dokumen Pada PT. Reasuransi Indonesia Utama. *JITEK (Jurnal Informatika dan Teknologi Komputer)*, 136-145.

[3] Arianti, T., Fa'izi, A., Adam, S., & Wulandari, M. (2022). Perancangan Sistem Informasi Perpustakaan Menggunakan Diagram UML (Unified Modelling Language). *Jurnal Ilmiah Komputer Terapan dan Informasi (JIKTI)*, 19-25.

[4] 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.

[5] 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.

[6] Firmansyah, R., & Permana, A. A. (2019). Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma RSA Dengan Metode Waterfall Berbasis Java. *JOUTICA* , 217-221.

[7] Gunawan, & Kirman. (2019). Implementasi Algoritma Turbo Boyer Moore Untuk Pencarian Data Pada Transaksi Keuangan Duta Phonecell Sawah Lebar. *Jurnal Media Infotama*, 9-15.

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

P-ISSN 1858-2680
E-ISSN 2723-4673

SISTEM INFORMASI DAN TEKNOLOG (SINTEK), 7-14.

[9] 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.

[10] R.H Sianipar. (2019). *Visual Basic.Net Untuk Programmer*. Yogyakarta: Andi Offset.

[11] 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.

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

[14] 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.

[15] Wahyudi, Hartama, D., Kirana, I. O., Sumarno, & Gunawan, I. (2022). Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun. *Jurnal Ilmu Komputer dan Informatika (JIKI)*, 57-66.

[16] Yusrizal. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *JTIK (Jurnal Teknik Informatika Kaputama)*, 29-37.

[17] Zachary, M. Z., Sylviani, S., & Kurniadi, E. (2024). Implementasi Algoritma RSA (Rivest-Shamir-Adleman) Pada Kriptografi Klasik. *Mathematical Sciences and Applications Journal*, 54-59.

[18] Ziliwu, K., Maslan, A., & Kremer, H. (2022). Implementasi Caesar Cipher Pada Algoritma Kriptografi Dalam Penyandian Pesan Whatsapp. *Jurnal Comasie*, 117-125.

P-ISSN 1858-2680
E-ISSN 2723-4673