Volume 9 Nomor 1, 2023, 1-7
ISSN: 2460-1799 P-ISSN: 1432-602743

Aplikasi Penomoran Surat dengan Metode AES dan RSA untuk Penyimpanan Surat berbasis WEB

Topaz Malik Aziz[1], Saruni Dwiasnati[2]

[1,2] *Teknik Informatika, Universitas Mercu Buana*
Jl. Raya, RT.4/RW.1, Meruya Sel., Kec. Kembangan, Jakarta, Daerah Khusus Ibukota Jakarta, Indonesia
[1]41516120104@student.mercubuana.ac.id
[2*]saruni.dwiasnati@mercubuana.ac.id

Abstrak — **Tujuan dari penelitian ini adalah untuk mengamankan data dengan penerapan enkripsi agar menjamin keamanan dan kerahasiaan dokumen surat dengan aplikasi penomoran dan penyimpanan surat. Organisasi yang memiliki banyak unit kerja serta seringkali bersurat dengan pelanggan dan atau mitra diperlukan sistem aplikasi yang mencegah terjadinya kesalahan pada penomoran surat dan kontrol hak akses khususnya informasi yang hanya boleh diketahui oleh pihak tertentu. Dalam suatu organisasi sering kali ditemukan penomoran dokumen yang tidak rapi dan penyimpanan dokumen yang tidak terpusat dan umumnya tersimpan pada perangkat local karyawan. Keamanan data dan kerahasiaan dokumen menjadi tidak aman dan tidak dapat dikendalikan secara terpusat. Seperti dokumen berita acara, surat keluar dan PO. Oleh karenanya untuk meningkatkan dan menjamin keamanaan, efisiensi dan memudahkan suatu organisasi dalam aktifitas surat menyurat agar penyimpanan surat. Aplikasi penomoran dan penyimpanan surat dibuat dengan menggunakan bahasa pemrogramaan C# dan database SQL Server, dandengan implementasi enkripsi gabungan algoritma enkripsi AES dan RSA agar data yang disimpan terjamin keamaan data nya serta penyimpanan data menjadi terpusat.**
Kata kunci— AES, C#, Penomoran Surat, RSA, SQL Server

Abstract— **The purpose of this research is to secure data by applying encryption to ensure the security and confidentiality of letter documents with the application of letter numbering and storage. Organizations that have many work units and often correspond with customers and or partners need an application system that prevents errors in letter numbering and controls access rights, especially information that can only be known by certain parties. In an organization it is often found that the numbering of documents is not neat and the document storage is not centralized and is generally stored on the employee's local device. Data security and document confidentiality are insecure and cannot be controlled centrally. Such as document minutes, outgoing letters and POs. Therefore to improve and guarantee security, efficiency and facilitate an organization in correspondence activities so that mail is stored. Numbering and letter storage applications are made using the C# programming language and SQL Server database, and with the implementation of a combined encryption algorithm of AES and RSA encryption so that the stored data is guaranteed data security and centralized data storage.**
Index Terms— AES, C#, Penomoran Surat, RSA, SQL Server

I. PENDAHULUAN

Pada perkembangan teknologi saat ini keamanan data merupakan hal yang harus diperhatikan dalam menjaga kerahasiaan informasi. Perkembangan teknologi informasi yang pesat menjadikan informasi menjadi permintaan utama setiap orang atau setiap organisasi, karena informasi sangat penting untuk membantu individu atau organisasi berkembang dalam persaingan global. Bagi organisasi yang memiliki banyak unit kerja serta seringkali bersurat dengan pelanggan dan atau mitra diperlukan sistem aplikasi yang mencegah terjadinya kesalahan pada penomoran surat dan kontrol hak akses khususnya informasi yang hanya boleh diketahui oleh pihak tertentu. Dalam suatu organisasi sering kali ditemukan penomoran dokumen yang tidak rapi dan penyimpanan dokumen yang tidak terpusat dan umumnya tersimpan pada perangkat local karyawan. Dengan kejadian tersebut menjadi menyulitkan bagi organisasi untuk memastikan penomoroan yang benar dan pencarian dokumen yang efisien saat dokumen diperlukan. Keamanan dan kerahasiaan dokumen juga menjadi konsentrasi suatu organisasi khususnya dokumen surat yang bersifat konfidensial yang ditujukan khusus suatu organisasi kepada organisasi lainnya.

Untuk melakukan pengemanan suatu dokumen terdapat banyak metode seperti, Menurut Kurniawan, D., Afyenni, R. and Hidayat, R. Kriptografi adalah cara dalam menjaga keamanan informasi atau pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak dapat dibaca. Bentuk tersandi tersebut hanya bisa dibaca atau diketahui oleh pihak yang berhak untuk membacanya seperti penerima atau pengirim pesan. Pesan atau informasi yang belum disamarkan

disebut dengan plaintext, sedangkan pesan yang sudah disamarkan disebut dengan chipertext. Enkripsi merupakan cara penyamaran sebuah pesan asli menjadi tidak terbaca, sedangkan proses mengembalikannya menjadi dapat terbaca disebut dengan dekripsi [1] Dan Menurut Kodar, A. Steganografi adalah seni penyembunyian pesan ke dalam pesan lain sedemikian rupa sehingga orang lain tidak menyadarinya ada sesuatu dalam pesan yang dengan mudah mengirim pesan rahasia ke gambar. Dengan cara ini akan sangat sulit membaca pesan tak kasat mata yang disisipkan pada media gambar jika pesan tidak diekstrak dari gambar media terlebih dahulu, dan pesan akan disimpan dengan aman [12]. Menurut Prameshwari, A. and Sastra, N. Algoritma Advanced Encryption Standard (AES) adalah suatu algoritma block chiper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya. Menurut Farisi Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit [3]. Menurut Nasution, R. and Triandi, B. RSA adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi [5].

Dengan implementasi algoritma kriptografi Advanced Encryption Standard (AES) dan RSA pada aplikasi penomoran dan penyimpanan surat berbasis web ini akan memberikan keamanan ganda pada surat-surat yang tersimpan didalam aplikasi karena menggunakan dua algoritma.

Didalam suatu organisasi penomoran dokumen surat sering kali dilakukan secara manual dan terbatas hanya dapat diakses oleh karyawan yang bertugas sebagai admin dokumen. Penentuan nomor dokumen surat menjadi penting karena diperlukan ketelitian untuk menentukan urutan nomor dokumen surat, serta format nomor dokumen surat juga harus sesuai dengan peraturan suatu organisasi yang pada umumnya suatu organisasi terbagi dalam beberapa bagian seperti bagian human resources, finance, information technology dan nomor dokumen surat perlu dibuat secara unik agar dokumen surat dapat mudah dicari dan diidentifikasi, dokumen surat tersebut dikirim oleh bagian apa dan berisikan deskripsi singkat perihal isi dari dokumen surat tersebut agar memudahkan pada saat melakukan pencarian.

Pada aplikasi penomoran dan penyimpanan surat berbasis web ini, data sample yang digunakan diambil dari tempat mahasiswa bekerja yaitu PT. Arranet Indonesia Sejahtera “ARRANET” atau “Perusahaan” dan kelompok usahanya adalah perusahaan swasta nasional bidang jasa Teknologi Informasi berbasis di Jakarta, Indonesia yang memberikan layanan implementasi, pembangunan, pengembangan, dukungan teknis dan dukungan operasional electronic payment switching dan solusi pembayaran elektronik/digital lainnya.

Didalam aplikasi penomoran dan penyimpanan surat berbasis web akan dibangun sebuah fitur yang akan berfungsi untuk membuat nomor surat secara otomatis sehingga tidak lagi diperlukan pengecekan secara manual karena aplikasi akan memastikan nomor dokumen surat sudah unik. Setelah nomor dokumen surat dibuat oleh sistem maka nomor dokumen surat tersebut sudah bisa langsung digunakan untuk dimasukan kedalam dokumen surat, jika surat sudah selesai dibuat maka pembuat surat bisa mengunggah dokumen surat kedalam aplikasi penomoran dan penyimpanan surat berbasis web ini.

Pada saat proses unggah dokumen surat akan dilakukan proteksi pada dokumen surat yang diunggah dengan melakukan implementasi algoritma kriptografi Advanced Encryption Standard (AES) dan RSA dimana dokumen surat hanya bisa diakses jika diunduh melalui aplikasi penomoran dan penyimpanan surat dimana jika ada orang yang mencoba meretas dokumen surat akan aman sehingga organisasi tidak ragu akan keamanaan dan kerahasiaan dokumen surat tersebut.

Didalam aplikasi penomoran dan penyimpanan surat berbasis web ini juga akan ada sebuah fitur yang akan berfungsi untuk mengatur peran karyawan pada suatu organisasi dimana karyawan yang memiliki keperluan dalam surat menyurat dapat mengakses aplikasi untuk membuat ataupun mencari dokumen surat. Data yang akan digunakan pada penelitian ini adalah dokumen surat keluar dan dokumen berita acara.

II. METODOLOGI PENELITIAN

Penelitian ini merupakan penelitian kualitatif berdasarkan hasil observasi dengan melakukan tinjauan langsung ke lapangan atau lokasi penelitian yaitu PT. Arranet Indonesia Sejahtera dan studi literatur untuk mengimplementasikan tindakan dengan harapan dapat melakukan rancangan desain, installasi sistem dan pengujian.

A. Metode Pengumpulan Data

Metode pengumpulan data merupakan salah satu aspek yang berperan dalam kelancaran dan keberhasilan dalam suatu penelitian. Dalam penelitian ini metode pengumpulan data yang digunakan adalah sebagai berikut:

1) Observasi

Peneliti melakukan pengematan secara langsung ke lapangan untuk mengetahui dan mempelajari proses untuk mendukung penelitian.

2) Studi Literatur

Peneliti melakukan studi literatur mengenai teori-teori berkaitan dengan topik penelitian dan rumusan masalah yang ditentukan. Studi literatur pada penulisan ini adalah mencari literatur melalui jurnal-jurnal mengenai algoritma yang penulis gunakan dalam penelitian.

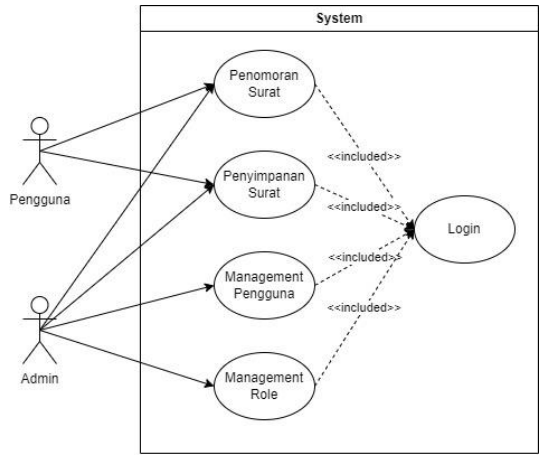
Volume 9 Nomor 1, 2023, 1-7
ISSN: 2460-1799 P-ISSN: 1432-602743

Tahap Pertama Melakukan Observasi dan Studi Literatur, penulis melakukan observasi secara langsung ke lapangan untuk mendapatkan data dan menganalisa proses yang sudah berjalan pada PT. Arranet Indonesia Sejahtera dan melakukan studi literatur yang berkaitan dengan topik dan rumusan masalah pada penelitian ini.

B. Identifikasi Kebutuhan

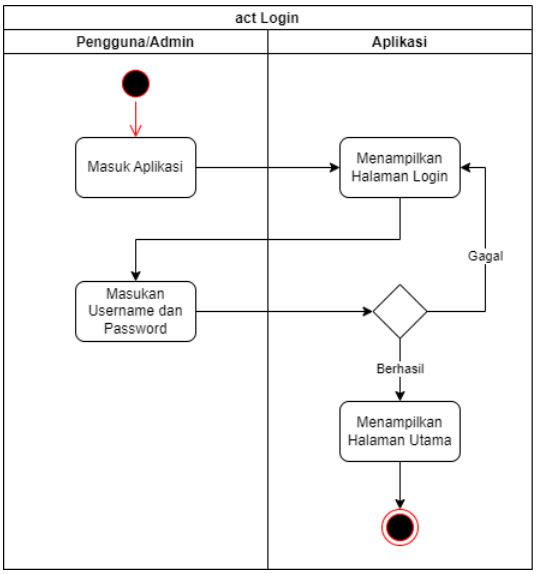
Tahap Kedua Identifikasi Kebutuhan, penulis melakukan identifikasi kebutuhan yang akan diimplementasi kedalam sistem. Hasil identifikasi kebutuhan tersebut akan dikoversi kedalam format Diagram yang berisikan informasi tentang kebutuhan aplikasi dan Implementasi algoritma kriptografi advanced encryption standard (AES) dan RSA pada aplikasi penomoran dan penyimpanan surat berbasis WEB.

1) Kebutuhan Aplikasi



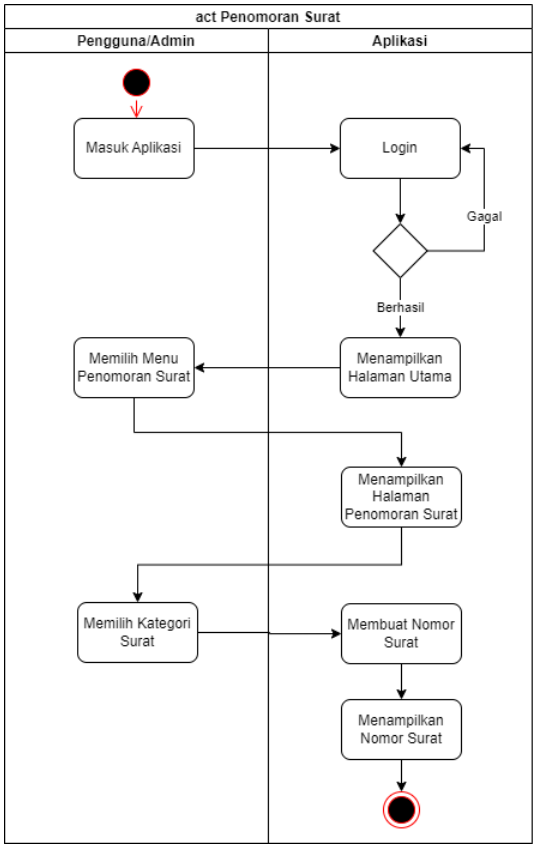
Gambar 1. Use Case Diagram Aplikasi Penomoran Dan Penyimpanan Surat.

Gambar 1 Menjelaskan tentang use case pada penelitian ini.



Gambar 2. Activity Diagram Login.

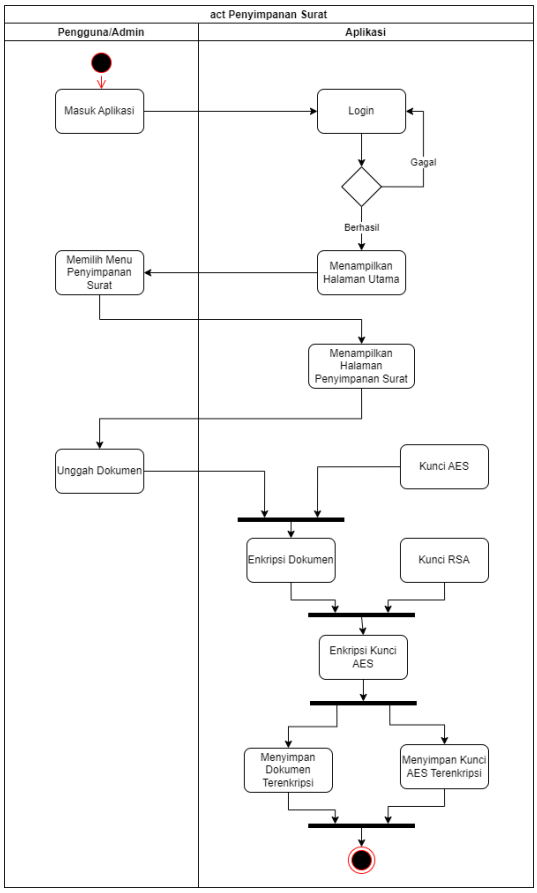
Gambar 2 Menjelaskan tentang aktifitas login.



Gambar 3. Activity Diagram Penomoran Surat.

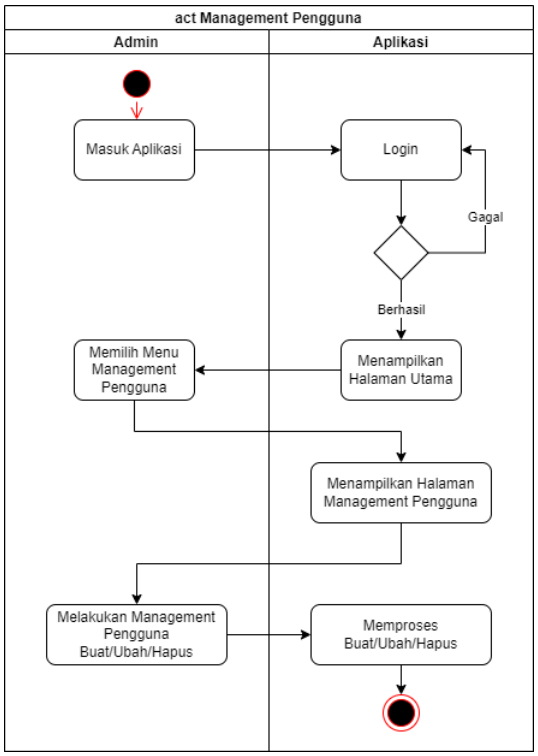
Gambar 3 Menjelaskan tentang aktifitas penomoran surat.

Volume 9 Nomor 1, 2023, 1-7
ISSN: 2460-1799 P-ISSN: 1432-602743



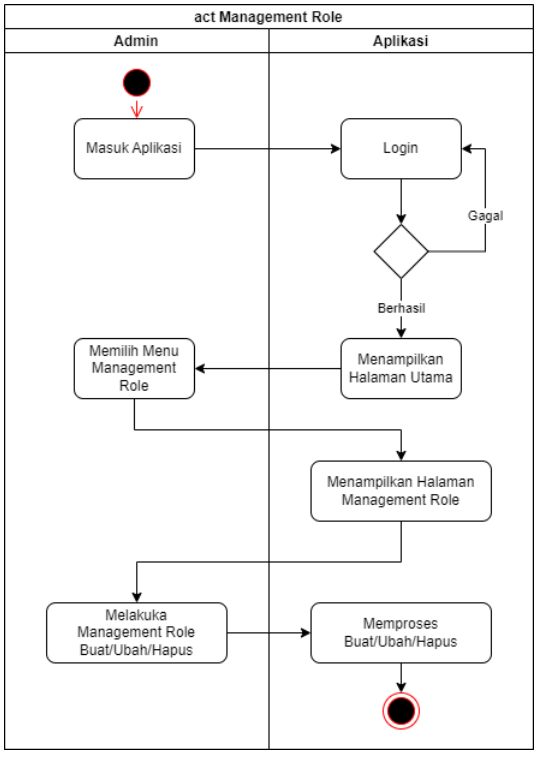
Gambar 4. Activity Diagram Penyimpanan Surat.

Gambar 4 Menjelaskan tentang aktifitas penyimpanan surat.



Gambar 5. Activity Diagram Management Pengguna.

Gambar 5 Menjelaskan tentang aktifitas management pengguna.

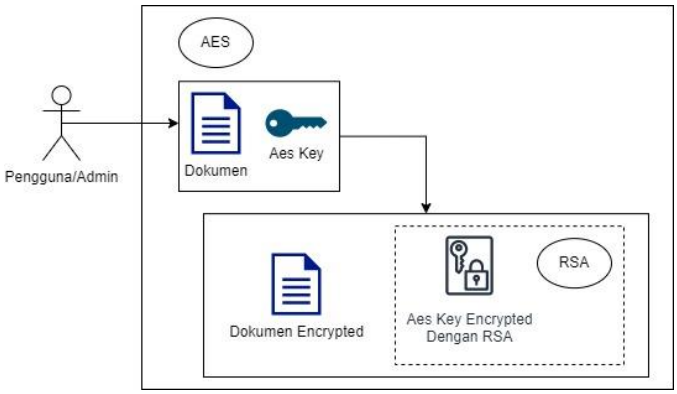


Gambar 6. Activity Diagram Management Role.

Volume 9 Nomor 1, 2023, 1-7
ISSN: 2460-1799 P-ISSN: 1432-602743

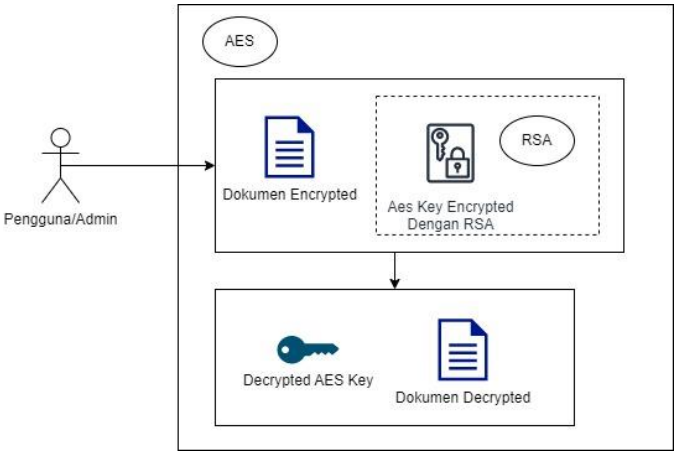
Gambar 6 Menjelaskan tentang aktifitas management role.

2) Kebutuhan Enkripsi & Dekripsi



Gambar 7. Alur Enkripsi Dokumen.

Gambar 7 Menjelaskan tentang alur enkripsi dokumen surat.



Gambar 8. Alur Dekripsi Dokumen.

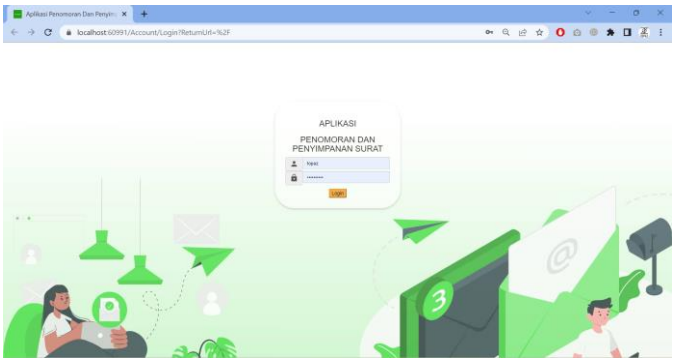
Gambar 8 Menjelaskan tentang alur dekripsi dokumen surat.

Tahap Ketiga Pengembangan Sistem, Melakukan pengembangan sistem sesuai dengan kebutuhan berdasarkan kebutuhan yang sudah diidentifikasi. Tahap Keempat Implementasi Sistem, proses pengujian pada sistem untuk menguji implementasi algoritma advanced encryption standard (AES) dan RSA pada aplikasi penomoran dan penyimpanan surat berbasis web.

III. HASIL DAN PEMBAHASAN

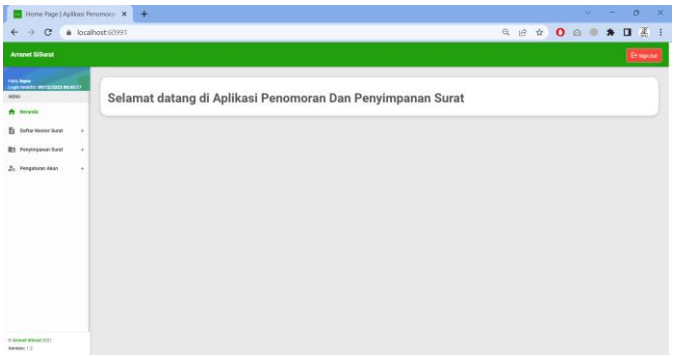
A. Implementasi Sistem

Berikut ini tampilan dari beberapa menu yang sudah dibuat, merupakan hasil identifikasi masalah pada tahap metodologi.



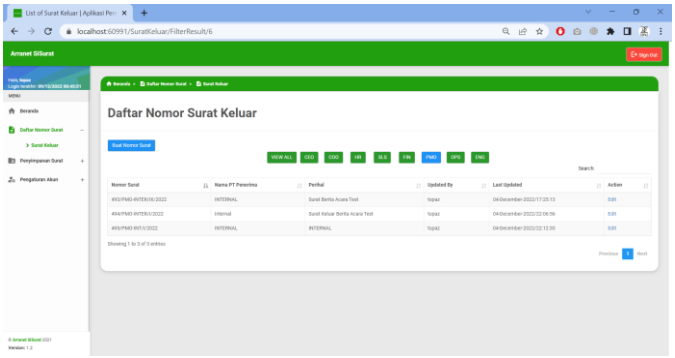
Gambar 9. Tampilan Halaman Login.

Gambar 9 Menjelaskan tentang tampilan login.



Gambar 10. Tampilan Halaman Utama.

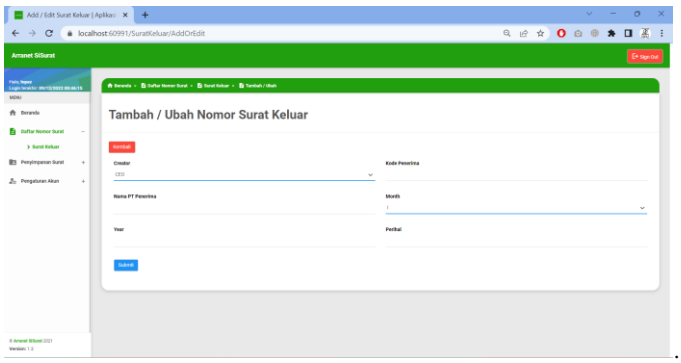
Gambar 10 Menjelaskan tentang tampilan halaman utama.



Gambar 11. Tampilan Halaman Daftar Nomor Surat

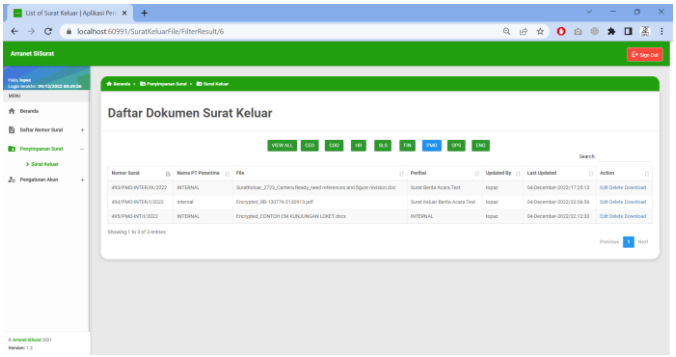
Gambar 11 Menjelaskan tentang tampilan daftar nomor surat.

Volume 9 Nomor 1, 2023, 1-7
ISSN: 2460-1799 P-ISSN: 1432-602743



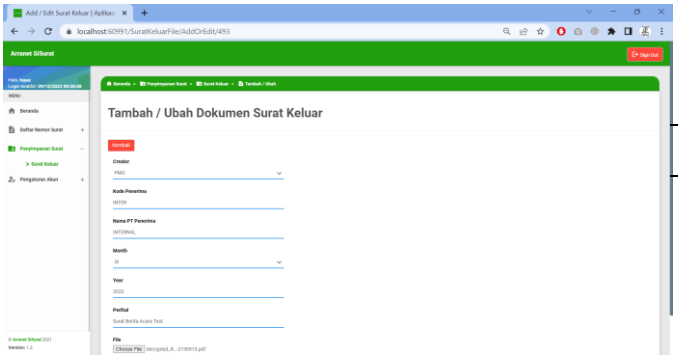
Gambar 12. Tampilan Halaman Tambah Nomor Surat

Gambar 12 Menjelaskan tentang tampilan tambah nomor surat.



Gambar 13. Tampilan Halaman Daftar Surat Tersimpan

Gambar 13 Menjelaskan tentang tampilan daftar surat tersimpan.

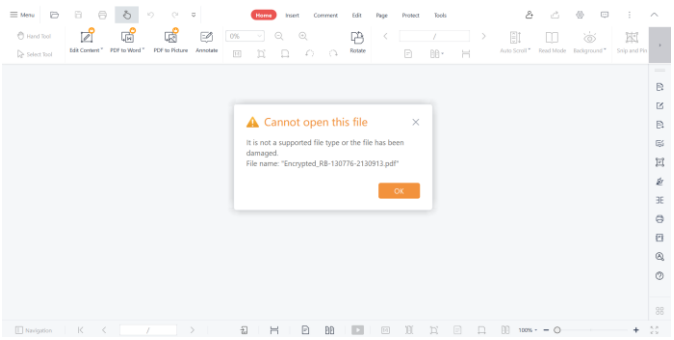


Gambar 14. Tampilan Halaman Penyimpanan Surat

Gambar 4 Menjelaskan tentang tampilan penyimpanan surat..

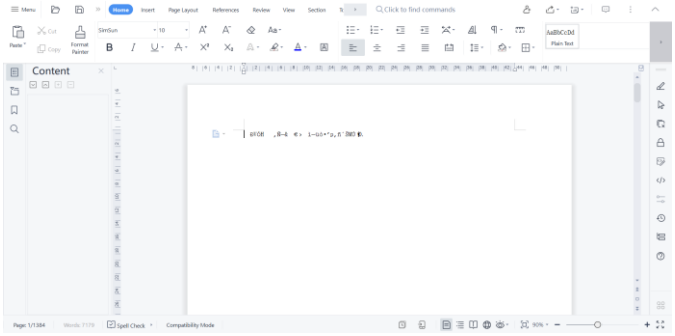
B. Hasil Enkripsi Dokumen

Dengan sistem yang telah diimplementasi diatas, enkripsi dokumen berhasil dilakukan.



Gambar 15. Hasil Enkripsi Dokumen Pdf

Gambar 15 Menjelaskan tentang tampilan dokumen yang terenkripsi.



Gambar 16. Hasil Enkripsi Dokumen Docx

Gambar 16 Menjelaskan tentang tampilan dokumen yang terenkripsi.

C. Hasil Pengujian Performa

TABEL I
HASIL PENGUJUAN PERFORMA

Panjang Kunci	Dokumen	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)
AES (256) & RSA (1024)	[210331] 001BA-UATIII-2021 Biller E-Samsat Jawa Timur.pdf	80	30
AES (256) & RSA (1024)	[210331] 002BA-UATIII-2021 Biller E-Money Mandiri.pdf	36	93
AES (256) & RSA (1024)	[210406] 002BA-ROIV-2021 Biller E-Samsat Jawa Timur.pdf	16	51
AES (256) & RSA (1024)	[210110] 011BA-ROI-2021 CA Arranetpay (Prepaid IM3).pdf	15	76
AES (256) & RSA (1024)	[210110] 002BA-ROI-2021 Incident Ticket #6189500.pdf	23	23
AES (256) & RSA (1024)	[210120] 003BA-TOI-2021 CA	17	10

Volume 9 Nomor 1, 2023, 1-7
ISSN: 2460-1799 P-ISSN: 1432-602743

MMBC (PBB DKI).pdf

IV. KESIMPULAN

Dari implementasi dan pengujian yang dilakukan, aplikasi berjalan sesuai dengan identifikasi kebutuhan. Gabungan kedua metode kriptografi memiliki peforma yang bagus.

Desain Aplikasi yang diajukan oleh penelitian ini masih belum sempurna dan dapat ditingkatkan dengan mengganti algoritma enkripsi yang serupa tetapi memiliki performa yang lebih baik.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada PT Arranet indonesia sejahtera yang menyediakan kebutuhan pengembangan ini dan didukung oleh Universitas Mercu Buana Meruya.

REFERENSI

[1] Kurniawan, D., Afyenni, R., & Hidayat, R. (2018). Implementasi Algoritma AES dalam Mengenkripsi Berkas Terintegrasi dengan Layanan Cloud Storage Berbasis Android. Seminar Nasional Sistem Informasi Dan Teknologi (SISFOTEK), (September), 237–245. Retrieved from https://seminar.iaii.or.id/index.php/SISFOTEK/article/view/84

[2] Farisi A., "Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone," https://doi.org/10.35957/jatisi.v4i2 .103, 2018.

[3] Prameshwari, A. and Sastra, N. (2018) " Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen " , Jurnal Eksplora Informatika, 8(1), pp. 52-58. doi: 10.30864/eksplora.v8i1.139.

[4] Fitriani, I. dan Utomo, A. B. (2020) "Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa", JISKA (Jurnal Informatika Sunan Kalijaga), 5(3), pp. 153–163. doi: 10.14421/jiska.2020.53-03.

[5] Nasution, R. and Triandi, B., 2020. IMPLEMENTASI METODE RSA DAN AES UNTUK MENGAMANKAN FILE WINRAR DAN ZIP.

[6] DM Meko. (2018) "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data", Jurnal Teknologi Terpadu Vol. 4, No. 1.

[7] Wahyudi, W., Hartama, D., Kirana, I., Sumarno, S. and 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, 2(1), pp.57-66.

[8] Tampubolon, A., (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks. Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), 20(1), p.38.

[9] Rizki, M. dan Farida Ariyani, P. (2021) "PENERAPAN KRIPTOGRAFI DENGAN MENGGUNAKAN ALGORITMA RSA UNTUK PENGAMANAN DATA BERBASIS DESKTOP PADA PT TRIAS MITRA JAYA MANUNGGAL", SKANIKA, 4(2), pp. 1-6. doi: 10.36080/skanika.v4i2.1991.

[10] Sutejo, S. (2021) "Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien", INTECOMS: Journal of Information Technology and Computer Science, 4(1), pp. 104 - 114. doi: https://doi.org/10.31539/intecoms.v4i1.2437.

[11] Ritonga, R., A'id, A. and Megayanti, A. (2021) "IMPLEMENTASI METODOLOGI SCRUM DALAM PENGEMBANGAN APLIKASI EREGITRASI VENDOR (STUDI KASUS : KRAKATAU IT)", Jurnal Sistem Informasi dan Informatika (Simika), 4(1), pp. 1-13. doi: 10.47080/simika.v4i1.1096.

[12] Kodar, A. (2017). Implementation of Steganography in Image Media Using Algorithm LSB (Least Significant Bit). International Research Journal of Computer Science, 4(8). https://doi.org/10.26562/irjcs.2017.aucs10081

[13] Tyagi, M., Manoria, M., & Mishra, B. (2019). Analysis and Implementation of AES and RSA for cloud. International Journal of Applied Engineering Research, 14(20), 3918. https://doi.org/10.37622/ijaer/14.20.2019.3918-3923v

[14] Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. In Procedia Computer Science (Vol. 78, pp. 617–624). Elsevier B.V. https://doi.org/10.1016/j.procs.2016.02.108

[15] Dr Asha Ambhaikar, Mr. A. G. (2021). AES AND RSA-BASED HYBRID ALGORITHMS FOR MESSAGE ENCRYPTION & DECRYPTION. INFORMATION TECHNOLOGY IN INDUSTRY, 9(1), 273–279. https://doi.org/10.17762/itii.v9i1.129