

Rancang Bangun Aplikasi Keamanan Data Ekspor Kayu Menggunakan Metode Affine Cipher Dan Rsa Berbasis Web

Design and Development of Timber Export Data Security Applications Using Web-Based Affine Cipher and Rsa Methods

Muhammad Fachrul Azmi^a, Charles Bronson Harahap^b

^{a,b}Informatika, Teknik Dan Ilmu Komputer, Universitas Potensi Utama
Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia – Medan
farolazmi@gmail.com¹, Charlesharahap07@gmail.com²

ABSTRAK

Kemajuan teknologi informasi muncul sebagai akibat dari perkembangan sistem keamanan yang cepat dan pesat. Disengaja atau tidak, teknologi informasi memberikan dampak yang signifikan pada banyak aspek kehidupan. Keamanan data tidak dapat dipisahkan dari berbagai aktivitas manusia yang memungkinkan terpeliharanya kerahasiaan informasi ini karena kemudahan transmisi informasi teknologi, namun pada kenyataannya, penipuan dan risiko terhadap data tetap ada, khususnya dalam ekspor kayu. Karena maraknya pencurian data, maka perlu dikembangkan aplikasi pengamanan data ekspor kayu yang menawarkan kerahasiaan data yang lebih terjamin. Selain itu, kurangnya keamanan terhadap kerahasiaan data ekspor kayu mengharuskan pengembangan aplikasi kriptografi untuk mengenkripsi data ekspor kayu.

Kata kunci : Ekspor kayu, keamanan data, metode RSA dan Affine cipher

ABSTRACT

Information technology advancements have emerged as a result of the security systems' quick and rapid development. Whether intentionally or not, information technology has a significant impact on many aspects of life. Data security cannot be isolated from many parts of human activities that enable the maintenance of this information's secrecy due to technology's ease of information transmission, but in reality, fraud and risks to data still exist, particularly in the export of timber. Due to the prevalence of data theft, it is necessary to develop a security application for timber export data that offers more secure data confidentiality. Additionally, the lack of security for the confidentiality of timber export data necessitates the development of a cryptographic application to encrypt timber export data.

Keywords: Wood export, data security, RSA method and Affine cipher

Info Artikel :

Disubmit: 1 Oktober 2022

Direview: 6 November 2022

Diterima : 11 Desember 2022

Copyright © 2023 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Perkembangan sistem keamanan memang sangat cepat dan pesat, hal ini menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari warna-warni kehidupan. Teknologi juga memudahkan untuk mengubah informasi sehingga keamanan data tidak lepas dari warna-warni aspek kondisi fana yang memungkinkan untuk menjaga kerahasiaan informasi tersebut, namun dalam praktiknya masih terdapat kecurangan dan jebakan terhadap data, khususnya dalam ekspor kayu. . Akibat dari maraknya pencurian data, diperlukan operasi pengamanan data impor kayu yang semakin mengamankan kerahasiaan data dan kurangnya pengamanan terhadap kerahasiaan data impor kayu memerlukan operasi kriptografi untuk mengenkripsi data impor kayu yang menyembunyikannya dapat diperkuat oleh sistem penguncian.

Ada banyak gaya pengamanan data yang dapat digunakan untuk membantu penipuan atau manipulasi data, salah satunya dengan menggunakan kriptografi atau cara penyamaran lainnya. Kriptografi adalah kebijaksanaan yang didasarkan pada cara yang baik untuk menangani keamanan informasi seperti kerahasiaan, integritas data, dan otentikasi realitas. Jadi pemahaman ultramodern tentang kriptografi tidak hanya berurusan dengan caching komunikasi melainkan serangkaian cara yang memberikan keamanan informasi.

RSA (Rivest Shamir Adleman) adalah salah satu algoritma kunci publik yang populer digunakan dan memang saat ini algoritma RSA masih dianggap aman dan Affine cipher adalah perpanjangan dari sandi Caesar, yang mengutip teks biasa dengan nilai dan menambahkannya dengan pergeseran.

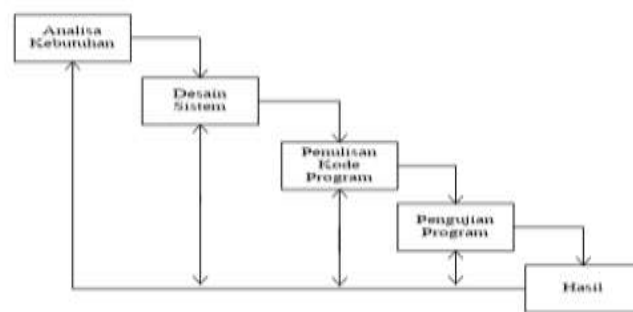
Penipuan dalam Keamanan Data Ekspor dapat diatasi dengan menggunakan gaya RSA dan Afiine Chipper secara terjemahan dan deskriptif.

Oleh karena itu diperlukan suatu sistem keamanan yang cocok untuk menjaga keamanan import data dari jebakan-jebakan lainnya yang dilakukan oleh pihak-pihak yang ugal-ugalan. Dengan menggunakan algoritma cipher RSA dan Affine, sistem akan meng-cipher data asli yang dimasukkan oleh stoner ke dalam ciphertext dengan menggunakan kunci, juga mentransfernya ke orang lain atau rekan kerja. Untuk memasukkan data asli, itu digambarkan sebagai plaintext menggunakan kunci juga oleh dermawan sehingga mentransfer informasi atau berolahraga informasi melalui keamanan algoritma cipher RSA dan Affine menjadi lebih mudah bagi perusahaan untuk memahami dalam menangani keamanan data impor.

2. METODE

Demikian penulis mengutip dari beberapa bacaan yang berkaitan dengan pengerjaan skripsi. Bacaan yang dikutip dapat berupa proposisi atau pendapat dari beberapa bacaan. Hal ini dimaksudkan untuk memberikan landasan teori yang kuat melalui buku-buku, jurnal-jurnal yang berkaitan dengan penulisan skripsi ini.

Dalam sistem eksplorasi ini digunakan cara-cara analisis, braket masalah, hingga masalah yang berkaitan dengan skripsi yang penulis buat. Cara yang ditempuh penulis untuk mencapai pretensi desain ditunjukkan pada Gambar 1, di bawah ini :



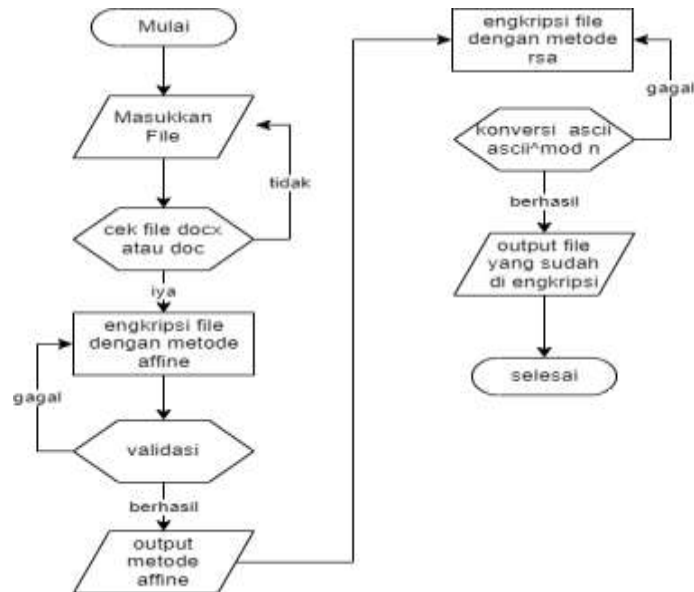
Gambar 1. Diagram *Waterfall*

3. HASIL DAN PEMBAHASAN

A. Flowchart

Jenis ilustrasi yang mewakili alur kerja suatu sistem, atau dapat mewakili algoritma yang menampilkan tahapan dalam bentuk simbol yang ditentukan. Dalam mendesain flowchart sebenarnya tidak memiliki

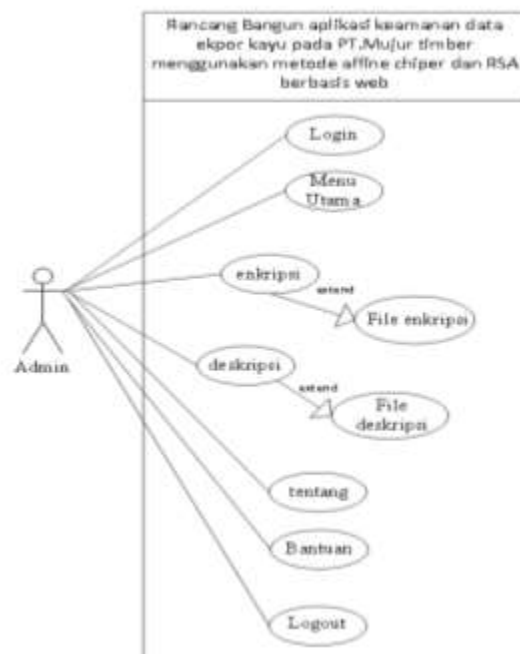
rumus tertentu, hanya saja flowchart memiliki simbol-simbol yang umum digunakan. Seperti yang telah dijelaskan tentang flowchart, fungsi utama dari flowchart adalah untuk menggambarkan, menyederhanakan rangkaian proses atau prosedur sehingga mudah dipahami dan mudah dilihat berdasarkan urutan jalan dalam suatu proses.



Gambar 2. Flowchart Sistem Aplikasi

B. Use Case Diagram

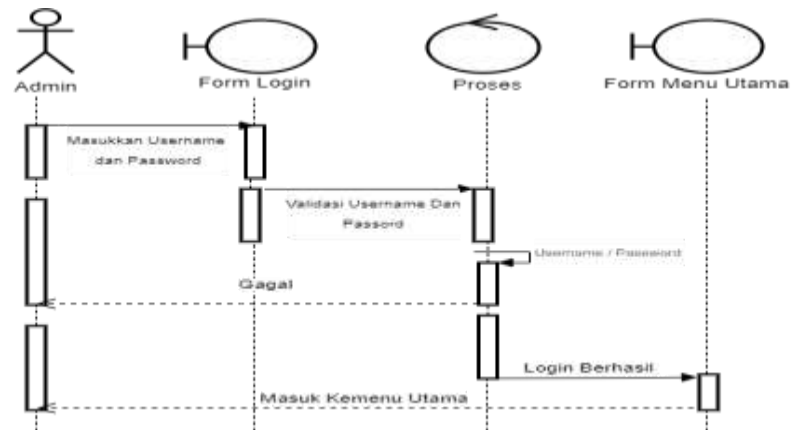
Geste dan tugas masing-masing elemen dan aktor yang terlibat dalam sistem yang akan dirancang akan digambarkan dalam bentuk ilustrasi use case yang bertujuan untuk memberikan gambaran umum sistem yang akan dirancang pada Gambar 3, sebagai berikut :



Gambar 3. Use Case Diagram

a) *Sequence Diagram Login*

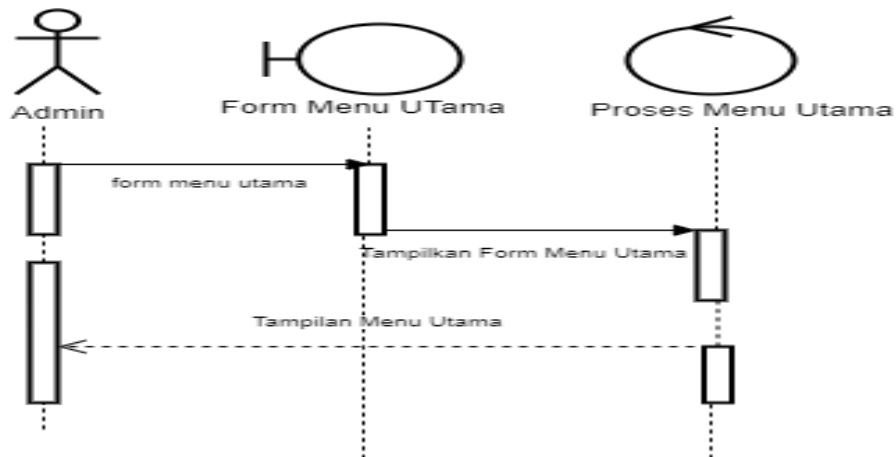
Serangkaian kerja melakukan *login* dapat dilihat pada Gambar 3. Dibawah ini.



Gambar 4. *Sequence Diagram Login*

b) *Sequence Diagram Menu Utama RSA Dan Affine Cipher*

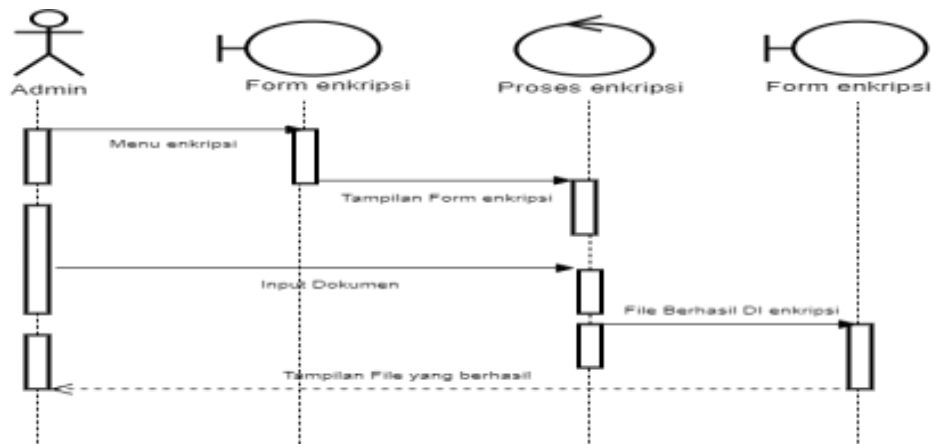
Serangkaian kerja melakukan Menu Utama RSA Dan Affine Cipher dapat dilihat pada Gambar 5. dibawah ini :



Gambar 5. *Sequence Diagram Menu Utama RSA Dan Affine Cipher*

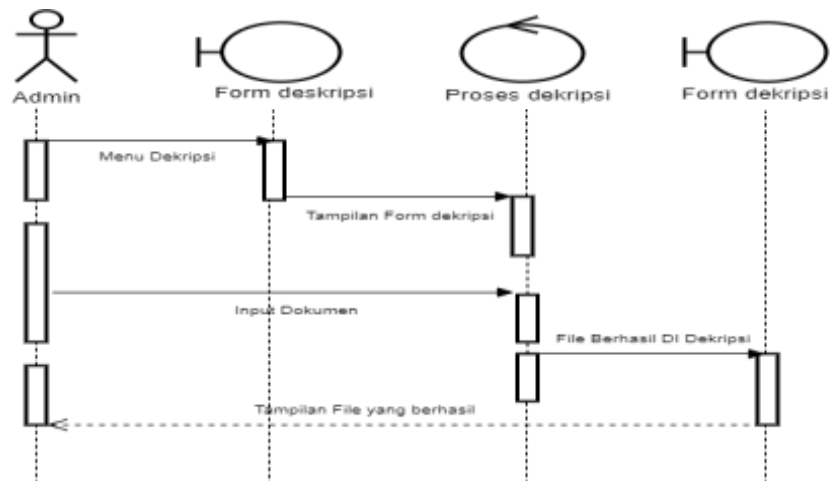
c) *Sequence Diagram Enkripsi RSA Dan Affine Cipher*

Serangkaian kerja melakukan enkripsi RSA Dan Affine Cipher dapat dilihat pada Gambar 6. dibawah ini.



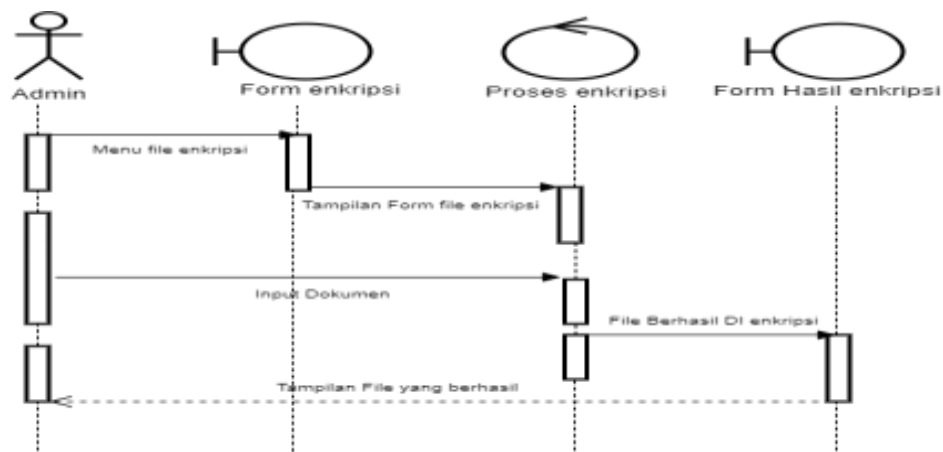
Gambar 6. Sequence Diagram Enkripsi RSA Dan Affine Cipher

- d) *Sequence Diagram Dekripsi Affine Cipher Dan RSA*
Serangkaian kerja melakukan dekripsi *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar 7. dibawah ini:



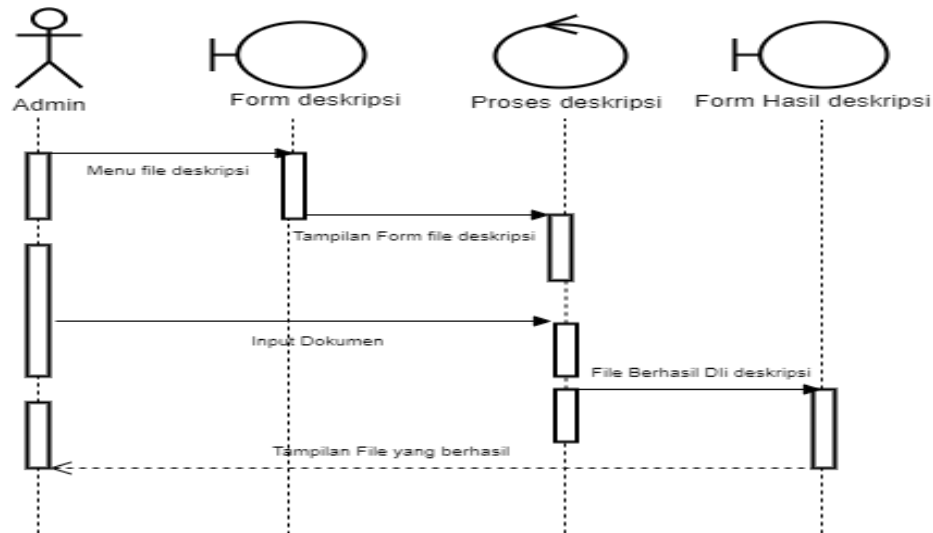
Gambar 7. Sequence Diagram Dekripsi Affine Cipher Dan RSA

- e) *Sequence Diagram Hasil Enkripsi Affine Cipher Dan RSA*
Serangkaian kerja melakukan Hasil Enkripsi *Affine Cipher* Dan *RSA* bisa dilihat pada Gambar 8. dibawah ini.



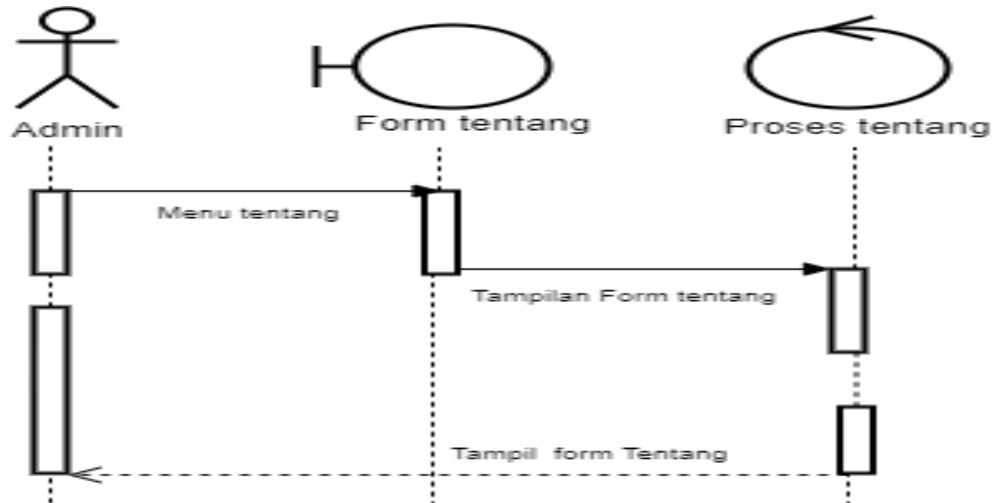
Gambar 8. Sequence Diagram Hasil Enkripsi Affine Cipher Dan RSA

- f) *Sequence Diagram Hasil Deskripsi Affine Cipher Dan RSA*
 Serangkaian kerja melakukan Hasil Deskripsi Affine Cipher Dan RSA dapat dilihat pada Gambar 9. dibawah ini.



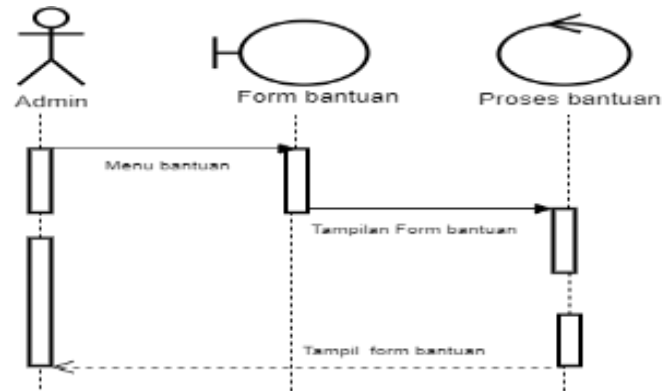
Gambar 9. Sequence Diagram Hasil Deskripsi Affine Cipher Dan RSA

- g) *Sequence Diagram Tentang Cipher Dan RSA*
 Serangkaian kerja melakukan Tentang Affine Cipher Dan RSA dapat dilihat pada Gambar III.19 dibawah ini.



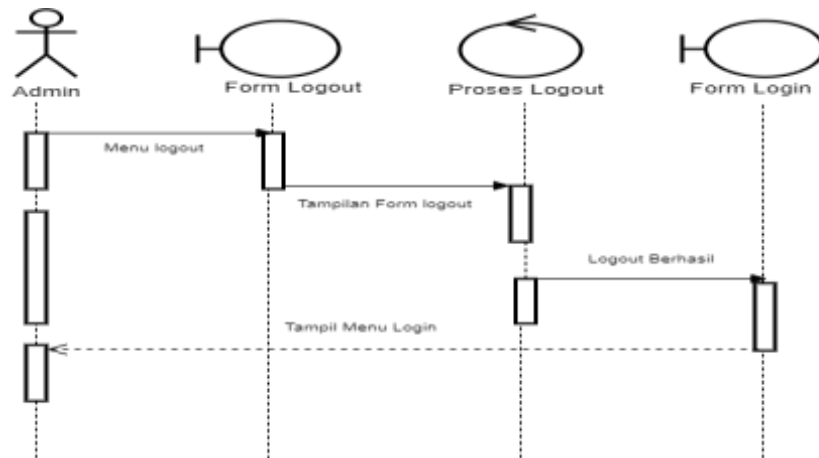
Gambar 10. Sequence Diagram Tentang Cipher Dan RSA

- h) *Sequence Diagram Bantuan Cipher Dan RSA*
 Serangkaian kerja melakukan Bantuan Affine Cipher Dan RSA dapat dilihat pada Gambar III.20 dibawah ini.



Gambar 11. Sequence Diagram Bantuan Cipher Dan RSA

- i) *Sequence Diagram Log Out*
Serangkaian kerja melakukan log out dapat dilihat pada Gambar III.21 dibawah ini.



Gambar 12. Sequence Diagram Log Out

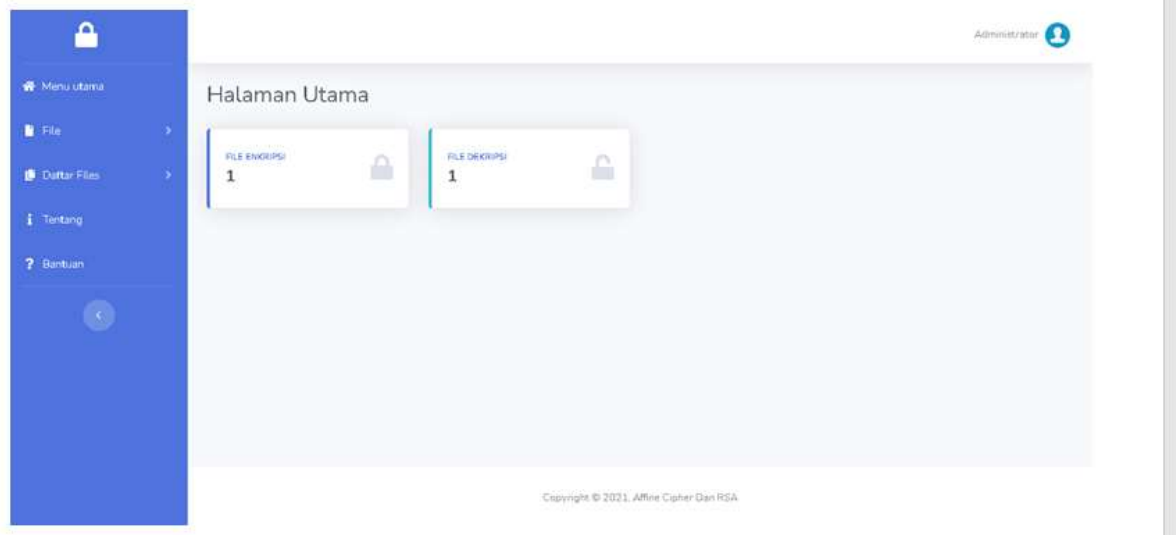
C. Tampilan Hasil

Tampilan ini merupakan halaman *login*. Halaman ini ber-is *username* dan *password* yang hanya bisa di-isi oleh *admin* saat mengakses aplikasi. Halaman ini dapat dilihat pada gambar 13. berikut ini:



Gambar 13. Tampilan Login

- a) Tampilan Halaman *Home*
Tampilan ini merupakan halaman *Dashboard*. Halaman ini merupakan tampilan halaman utama admin setelah melakukan login. Halaman ini berisikan laporan file enkripsi dan file deskripsi. Halaman ini dapat dilihat pada gambar 14. berikut ini:

Gambar 14. Tampilan Halaman *Home*

- b) Tampilan Halaman *File Enkripsi*
Tampilan ini merupakan Halaman-halaman File Enkripsi. Halaman ini berisi data Form Enkripsi Menggunakan Metode Caesar Chipser. Halaman ini admin bisa Memilih data yang akan di Enkripsi. Halaman ini dapat dilihat pada gambar 15. berikut ini:



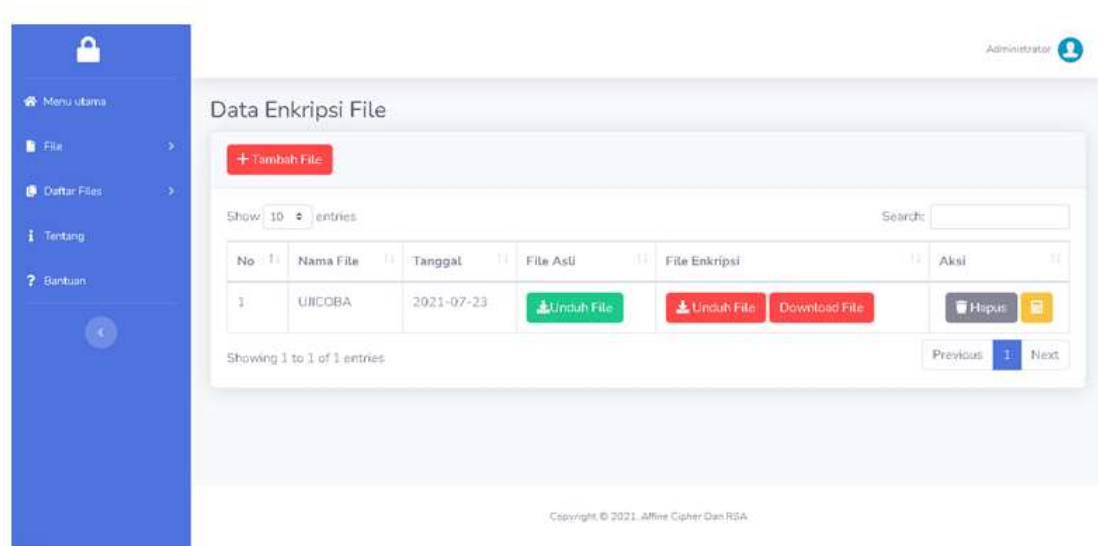
Gambar 15. Tampilan Halaman *File Enkripsi*

- c) Tampilan Halaman *File Deskripsi*
Tampilan ini merupakan halaman Halaman *File Deskripsi*. Halaman ini berisi data Form *Deskripsi Menggunakan Metode Caesar Cipher*. Halaman ini admin bisa Memilih data yang akan di Deskripsi. Halaman ini dapat dilihat pada gambar 16. berikut ini:

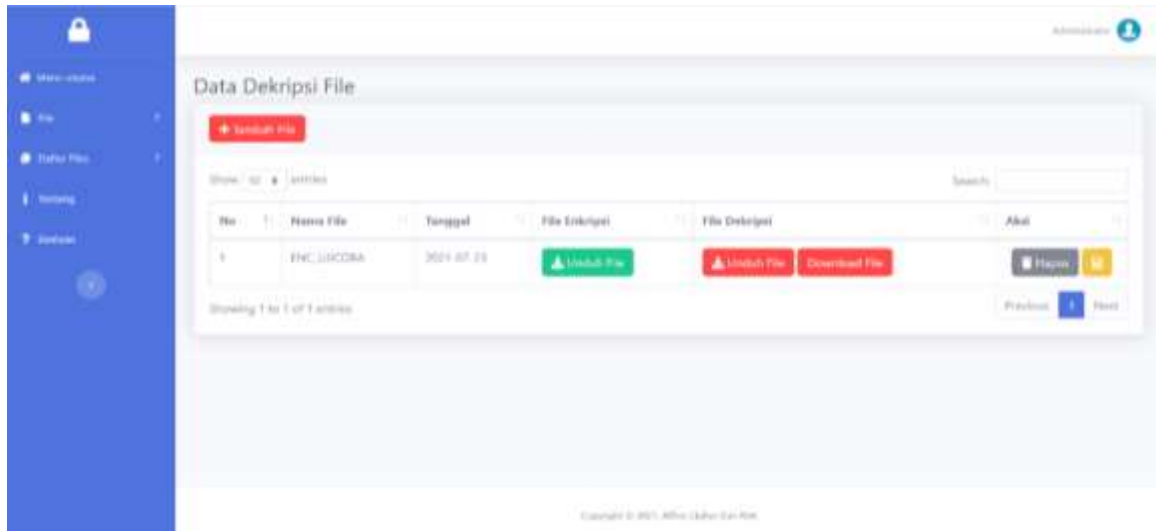


Gambar 16. Tampilan Halaman *File Deskripsi*

- d) Tampilan Halaman *Daftar File Enkripsi*
Tampilan ini merupakan halaman Daftar File Enkripsi. Halaman ini berisi Data Enkripsi File. Halaman ini admin bisa menambah, mengedit, menghapus, serta Mengunduh data File Enkripsi. Halaman ini dapat dilihat pada gambar 17. berikut ini:

Gambar 17. Tampilan Halaman *Daftar File Enkripsi*

- e) Tampilan Halaman *Daftar File Deskripsi*
 Tampilan ini merupakan halaman Daftar File Deskripsi. Halaman ini berisi Data Deskripsi File. Halaman ini admin bisa menambah, mengedit, menghapus, serta Mengunduh data File Deskripsi. Halaman ini dapat dilihat pada gambar 18. berikut ini:

Gambar 18. Tampilan Halaman *Daftar File Deskripsi*

D. Uji Coba Hasil

Uji coba terhadap aplikasi bertujuan untuk memastikan bahwa aplikasi sudah berada pada kondisi siap untuk digunakan, alat yang digunakan untuk melakukan pengujian aplikasi yaitu dengan menggunakan:

- a) Laptop dengan spesifikasi sebagai berikut:
 - a. *Processor Intel Core i3*

- b. *Memory* 4 GB
- c. *Harddisk* 500 GB
- d. *Operating System Windows* 10
- b) Perangkat lunak (*Software*) dengan spesifikasi sebagai berikut:
 - a. *MySQL*
 - b. *Sublime Text* 3
- c) Pengujian Aplikasi:
 - a. Tampilan Sistem
 - b. Informasi data yang dihasilkan oleh sistem.

E. Skenario Pengujian

Pada perancangan aplikasi, penulis menggunakan bahasa pemrograman PHP dan *database* MySQL. Pengujian aplikasi ini menggunakan *black box testing* seperti pada tabel berikut ini:

Tabel 1. Skenario Pengujian Admin (*Black Box Testing*)

Form Uji	Skenario Uji	Hasil yang diharapkan	Hasil Pengujian
Pengujian Login (Admin)			
Login	Memasukkan username dan password dengan benar	Sistem akan menerima akses login kemudian langsung menampilkan halaman admin	Valid
	Memasukkan Username dan Password dengan salah	Sistem akan menolak akses login dan akan muncul pesan pemberitahuan	Valid
Pengujian File Enkripsi (Admin)			
File Enkripsi	Komponen yang diuji adalah Textbox pada halaman File Enkripsi	Data yang diinput akan tampil pada halaman File Enkripsi	Valid
	Pengujian aksi Enkripsi File dengan mengklik tombol Enkripsi	Sistem akan Mengenkripsi File setelah di klik tombol Enkripsi	Valid
Pengujian File Deskripsi (Admin)			
File Deskripsi	Komponen yang diuji adalah Textbox pada halaman File Enkripsi	Data yang diinput akan tampil pada halaman data pertanyaan	Valid
	Pengujian aksi Deskripsi File dengan mengklik tombol Deskripsi	Sistem akan MengDeskripsi File setelah di klik tombol Deskripsi	Valid
Pengujian Data Enkripsi File (Admin)			
Data Enkripsi File	Komponen yang diuji adalah tambahFile pada halaman Data Enkripsi File	Data yang diinput akan tampil pada halaman Data Enkripsi File	Valid
	Pengujian aksi Unduh File dengan mengklik tombol Unduh File	Sistem akan Memproses File yang akan di Unduh	Valid

	Pengujian aksi hapus File dengan mengklik tombol hapus	Sistem akan menghapus File Enkripsi setelah di klik tombol hapus	<i>Valid</i>
	Pengujian Aksi Log Perhitungan uji coba Kombinasi Affine Cipher Dan RSA	Sistem akan Menampilkan Hasil Log Perhitungan uji coba Kombinasi Affine Cipher Dan RSA	<i>Valid</i>
Pengujian Data Deskripsi File (Admin)			
Data Deskripsi File	Komponen yang diuji adalah tambah File pada halaman Data Deskripsi File	Data yang diinput akan tampil pada halaman Data Deskripsi File	<i>Valid</i>
	Pengujian aksi Unduh File dengan mengklik tombol Unduh File	Sistem akan Memproses File yang akan di Unduh	<i>Valid</i>
	Pengujian aksi hapus File dengan mengklik tombol hapus	Sistem akan menghapus File Enkripsi setelah di klik tombol hapus	<i>Valid</i>
	Pengujian Aksi Log Perhitungan uji coba Kombinasi Affine Cipher Dan RSA	Sistem akan Menampilkan Hasil Log Perhitungan uji coba Kombinasi Affine Cipher Dan RSA	<i>Valid</i>

F. Kelebihan dan Kekurangan Aplikasi

Adapun beberapa kelebihan aplikasi yang penulis buat adalah sebagai berikut:

- Tampilan sistem yang menarik dan mudah dipahami.
- Data-data yang disimpan ada *database* dapat ditambah, diedit, dan dihapus langsung dari aplikasi web oleh *admin* tanpa mengubahnya dari *database*.
- Sistem yang dibuat dapat diakses dimana saja dengan menggunakan paket internet atau sistem yang dibuat adalah berbasis web.

Adapun beberapa kekurangan aplikasi yang penulis buat adalah sebagai berikut:

- Fitur dalam aplikasi masih terbatas, sehingga kedepannya dibutuhkan pengembangan aplikasi agar lebih menarik, efektif dan efisien.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama membuat aplikasi Keamanan Data Ekspor Kayu Pada Pt. Mujuur Timber Menggunakan Metode *Affine Cipher Dan RSA* Berbasis Web, maka dapat ditarik kesimpulan sebagai berikut:

- Dengan menggunakan sistem yang sudah terkomputerisasi bisa memudahkan perusahaan dalam menjaga kerahasiaan informasi dari data ekspor kayu dengan menerapkan algoritma *Affine Cipher dan RSA*.
- Dengan membangun sebuah aplikasi menggunakan metode *Algoritma Affine Cipher dan RSA* dalam Rancang Bangun Aplikasi Keamanan Data Ekspor Kayu Pada Pt. Mujuur Timber, diharapkan dapat membantu Pt. Mujuur Timber dari pencurian Data Ekspor Kayu.

- c) Dengan menerapkan metode *Algoritma Affine Cipher dan RSA* dalam Rancang Bangun Aplikasi Keamanan Data Ekspor Kayu Pada Pt. Mujur Timber, diharapkan dapat membantu Pt. Mujur Timber untuk menghasilkan laporan Keamanan Data Ekspor Kayu lebih tepat dan akurat.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada Universitas Potensi Utama yang telah memberikan kesempatan kepada penulis agar menyelesaikan karya ilmiah ini. Dan penulis berharap karya ilmiah ini dapat diambil ilmu dan manfaatnya.

REFERENSI

- [1] Fuad, R. N., & Winata, H. N. (2017). Aplikasi keamanan file audio wav (waveform) dengan terapan algoritma RSA. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, 1(2), 113-119.
- [2] Santoso, H., & Fakhri, M. F. M. (2018). Perancangan aplikasi keamanan file audio format wav (waveform) menggunakan algoritma RSA. *Algoritma: Jurnal Ilmu Komputer Dan Informatika*, 2(1).
- [3] Damanik, M. A., Nasution, S. D., & Buulolo, E. (2017). PENERAPAN ALGORITMA TRIPLE TRANSPOSITION VIGENERE CIPHER DAN ALGORITMA RSA DALAM KEAMANAN LOGIN. *Informasi dan Teknologi Ilmiah (INTI)*, 5(1), 76-80.
- [4] Prasetyo, Y., Triandi, B., & Hardianto, H. (2018). Perancangan Aplikasi Pengamanan File Teks dengan Skema Hybrid Menggunakan Algoritma Enigma dan Algoritma RSA. *IT (Informatic Technique) Journal*, 6(1), 46-55.
- [5] MANIK, M. A. F. (2021). PENERAPAN ALGORITMA RSA DAN AFFINE CIPHER DALAM KEAMANAN FILE MS WORD.
- [6] M. Ridwan, Z. Arifin, and Y. Yulianto, "Rancang Bangun E-Voting Dengan Menggunakan Keamanan Algoritma Rivest Shamir Adleman (RSA) Berbasis Web (Studi Kasus : Pemilihan Ketua Bem Fmipa)," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 11, no. 2, p. 22, 2016.
- [7] A. & N. Ardelia Nidya Agustina, "Pengamanan Dokumen Menggunakan Metode Rsa (Rivest Shamir Adleman) Berbasis Web," pp. 14–19, 2015.
- [8] F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.
- [9] Chandra, "Keamanan Data Dengan Metode Kriptografi Kunci Publik," *J. TIMES*, vol. 2, no. 2, pp. 11–15, 2016.
- [10] D. Email, A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk," vol. 3, no. 2, pp. 253–258, 2015.
- [11] D. Apdillah, H. F. Siregar, and H. Swanda, "Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP," vol. 2, no. 1, pp. 45–52, 2018.
- [12] M. Ridwan and Z. Arifin, "RANCANG BANGUN E-VOTING DENGAN MENGGUNAKAN KEAMANAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB (STUDI KASUS : PEMILIHAN KETUA BEM FMIPA)," vol. 11, no. 2, pp. 22–28, 2016.
- [13] A. N. Agustina, "PENGAMANAN DOKUMEN MENGGUNAKAN METODE RSA (RIVEST SHAMIR ADLEMAN) BERBASIS WEB," pp. 14–19, 2015.

- [14] Y. Suharya and H. Widia, "Implementasi Digital Signature Menggunakan Algoritma Kriptografi RSA Untuk Pengamanan Data Di Smk Wirakarya 1 Ciparay," J. Inform., vol. 07, no. 01, pp. 20–29, 2020.
- [15] I. Rifky, "KOMBINASI ALGORITMA RC5 BLOCK CIPHER DAN ALGORITMA REBALANCED RSA DALAM PENGAMANAN PESAN INSTAN," Komb. Algoritm. RC5 BLOCK CIPHER DAN Algoritm. REBALANCED RSA DALAM PENGAMANAN PESAN INSTAN, vol. 1, no. 3, pp. 82–91, 2017.