JAKIR (Jurnal Komputer dan Informatika)
p-ISSN: 3089-2643, e-ISSN: 3089-2643
Volume 2 Number 1 | Juni 2025 | Hal. 31-43
DOI: https://doi.org/10.52188/jakir.v2i1.1085

Implementasi Enkripsi Algoritma ECC (Elliptic Curve Cryptography) untuk Keamanan Data Sistem Administrasi Disposisi Surat Berbasis Website

Rafianto[1], Abdul Kohar[2], Dicky Andika Sulaeman[3]
[1-3]Department of Informatics Engineering, Universitas Nahdlatul Ulama Cirebon, Indonesia

Article Info

Article history:

Keywords:

Sistem Administrasi
Disposisi Surat
Pemantauan Surat
Algoritma Enkripsi

ABSTRAK

Disposisi surat adalah proses pengelolaan dan pendistribusian surat di sebuah instansi yang mencakup penerimaan surat, penentuan tindakan yang diperlukan, serta pengalihan surat kepada pihak yang bertanggung jawab untuk melakukan tindakan yang bersangkutan. Semua surat yang diedarkan harus dikelola dengan baik, tindakan yang diambil harus ditetapkan dengan tepat, dan balasan harus diberikan pada waktu yang tepat. Di Universitas Nahdlatul Ulama Cirebon masih terdapat beberapa kendala dan permasalahan terkait sistem disposisi surat yang saat ini diterapkan. Surat yang dikirim sering kali tertunda atau tidak terkirim seperti seharusnya. Selain itu, posisi surat yang telah dikirim tidak dapat terlacak dengan baik. Bahkan surat yang diarsipkan terkadang menjadi hilang. Juga perlu adanya pengintegrasian dengan teknologi yang semakin berkembang saat ini, terutama dalam hal efektivitas dan efisiensi sistem. Penelitian ini bertujuan untuk membangun sistem administrasi disposisi surat dengan menggunakan media teknologi informasi online berbasis website dan mengimplementasikan algoritma enkripsi untuk meningkatkan keamanan sistem. Metode pengembangan yang digunakan yaitu metode RUP (Rational Unified Process) yang dilakukan dengan pendekatan sistematis, dimulai dari tahap inception, tahap elaboration, tahap construction, dan tahap transition. Pengujian dilakukan dengan melakukan uji test case pada halaman pembuatan surat hingga proses pengarsipan surat. Hasil pengujian menyatakan bahwa sistem administrasi disposisi surat yang dibangun ini mencapai hasil sesuai dengan yang diharapkan.

Corresponding Author:

Rafianto,
Informatics Engeenering Department, Faculty of Computer, Universitas Nahdlatul Ulama Cirebon
Jl. Sisingamangaraja No.33 Panjunan, Lemah Wungkuk - Kota Cirebon. 45112
Email: rafianto@gmail.com

1. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi membawa dampak yang besar terhadap kehidupan masyarakat saat ini. Berkat adanya teknologi, banyak orang mulai beralih dari sistem manual menjadi otomatis. Perkembangan ilmu pengetahuan dan teknologi juga cenderung dikaitkan dengan komputer yang tujuannya untuk memudahkan tugas manusia dalam memperoleh informasi (Yusman & Harahap, 2020). Disposisi surat merupakan tanggapan atau instruksi yang diberikan oleh atasan kepada bawahannya untuk segera ditindaklanjuti (PT. Integra Inovasi Indonesia, 2021). Disposisi surat adalah proses pengelolaan dan pendistribusian surat di sebuah instansi. Hal ini mencakup penerimaan surat, penentuan tindakan yang perlu diambil, serta pengalihan surat kepada pihak yang bertanggung jawab

untuk menyelesaikan tindakan yang dimaksud. Disposisi membantu memastikan bahwa setiap surat yang diedarkan dikelola dengan baik, tindakan yang perlu diambil ditentukan dengan tepat, dan respons yang diberikan tepat waktu.

Namun sistem disposisi surat yang saat ini diterapkan di Universitas Nahdlatul Ulama Cirebon masih terdapat beberapa kendala dan masalah. Surat yang telah diajukan sering kali mengalami keterlambatan atau bahkan tidak tersampaikan seperti yang seharusnya, yang mana ini akan menghambat proses administrasi dalam Universitas Nahdlatul Ulama Cirebon. Selain itu, posisi surat yang telah dikirim tidak bisa dilihat untuk mengetahui progres penyampaian surat disposisi. Surat yang telah sampai di tujuan akan diarsipkan. Namun, dalam pengarsipan juga masih memiliki masalah yaitu hilangnya surat-surat yang telah diterima sebelumnya.

Selain itu, perlu adanya peningkatan dalam proses administrasi disposisi surat dan mengintegrasikannya dengan teknologi yang semakin berkembang saat ini, terutama dalam sisi keamanan data pada sistem. Serangan siber dapat menyebabkan penurunan kinerja perangkat dan jaringan, pencurian data sensitif, kerusakan reputasi, dan bahkan hilangnya kepercayaan terhadap suatu organisasi (Latif & Firdaus, 2024).

Tujuan pada penelitian ini ialah membangun sistem administrasi disposisi surat berbasis *website* dengan fitur menyampaikan surat, memantau progres penyampaian surat hingga diterima oleh pihak yang berkepentingan serta melakukan pengarsipan surat dengan baik, dan menerapkan algoritma enkripsi sebagai metode pengamanan data pada sistem.

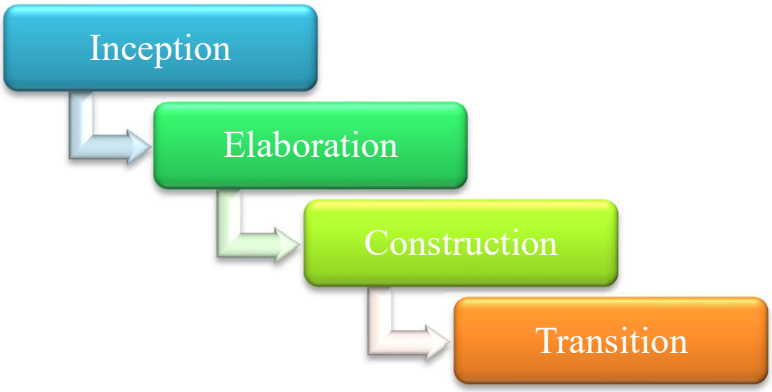
Beberapa penelitian terkait sistem administrasi disposisi surat adalah Perancangan Sistem Informasi Disposisi Surat Berbasis Web pada Kantor Badan Narkotika Nasional Kabupaten Deli Serdang (Alda & Nasution, 2023). Metode yang digunakan pada penelitian ini adalah metode *waterfall* dengan pengumpulan data observasi dan wawancara. Penelitian ini bertujuan untuk meningkatkan efisiensi dan efektivitas dalam mengelola surat masuk dan disposisi surat. Hasil akhir penelitian ini menghasilkan sistem informasi disposisi surat berbasis web.

Penelitian berikutnya terkait algoritma ECC adalah Pengamanan *Portable Document Format* (PDF) Menggunakan Algoritma Kriptografi Eliptik (Taopan, Boru, & Fanggidae, 2022). Penelitian ini bertujuan untuk menerapkan pengamanan PDF menggunakan algoritma ECC untuk mengamankan dokumen dari orang-orang yang tidak berwenang. Hasil dari penelitian ini menjelaskan bahwa algoritma ECC menggunakan panjang kunci yang lebih pendek namun memiliki tingkat keamanan yang sama jika dibandingkan dengan algoritma RSA.

Perbedaan penelitian terdahulu dengan penelitian ini adalah dalam merancang dan membangun sistem administrasi disposisi surat juga menerapkan algoritma ECC (*Elliptic Curve Cryptography*) untuk melakukan enkripsi dan dekripsi data yang ada pada sistem administrasi disposisi surat.

2. METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan kualitatif dengan pengumpulan data diperoleh melalui studi literatur, observasi, dan wawancara. Metode pengembangan sistem yang digunakan adalah metode RUP (*Rational Unified Process*) yang dilakukan dengan pendekatan sistematis, dimulai dari tahap *inception*, tahap *elaboration*, tahap *construction*, dan tahap *transition*.



Gambar 1 - Tahapan Metode RUP

a. Tahap Inception

Tahap *inception* dilakukan dengan memodelkan proses bisnis yang dibutuhkan (*business modeling*) dan mendefinisikan kebutuhan sistem yang akan dibuat (*requirement*).

b. Tahap Elaboration

Tahap *elaboration* dilakukan dengan menganalisis, membuat desain sistem, dan melakukan implementasi sistem yang fokus pada purwarupa sistem (*prototype*).

c. Tahap Construction

Tahap *construction* dilakukan dengan implementasi dan pengujian sistem yang fokus terhadap implementasi perangkat lunak pada kode program.

d. Tahap Transition

Tahap *transition* dilakukan dengan proses *deployment* atau instalasi sistem agar dapat dimengerti dan digunakan oleh *user*.

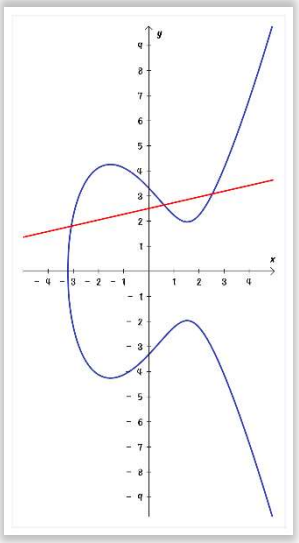
A. Kriptografi

Kriptografi adalah ilmu dan teknologi menjaga keamanan pesan dengan mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, dan keaslian data (Qadafi, 2019).

Dalam dunia kriptografi terdapat dua tahap, yaitu enkripsi dan dekripsi. Proses enkripsi mengubah teks asli menjadi susunan karakter atau simbol yang tidak dapat dipahami oleh manusia. Proses ini dapat menghasilkan sebuah pesan yang struktur karakternya berbeda dari teks aslinya. Sedangkan proses dekripsi merupakan kebalikan dari proses enkripsi, proses dekripsi mengembalikan pesan yang telah diubah menjadi bentuk yang dapat dipahami oleh manusia (Alfirdaus, et al., 2023).

B. Algoritma ECC (*Elliptic Curve Cryptography*)

Elliptic Curve Cryptography (ECC) adalah salah satu pendekatan algoritma kriptografi kunci publik berdasarkan pada struktur aljabar dari kurva elips pada daerah berhingga. Penggunaan kurva elips dalam kriptografi dicetuskan oleh Neal Koblitz dan Victor S. Miller pada tahun 1985. Kurva elips juga digunakan pada beberapa algoritma pemfaktoran integer yang juga memiliki aplikasinya dalam kriptografi, seperti *Lenstra Elliptic Curve Factorization*. Algoritma kunci publik berdasarkan pada variasi perhitungan matematis yang terbilang sangat sulit dipecahkan tanpa pengetahuan tertentu mengenai bagaimana perhitungan tersebut dibuat (Damanik P. S., 2019).



Gambar 2 - Bentuk Kurva Elips

Kurva elips dapat ditulis dengan menggunakan perhitungan matematis sebagai berikut.

$$y^2 = x^3 + ax + b \ (mod\ p)$$

Kriptografi kunci asimetris mengharuskan nilai parameter yang digunakan ditentukan terlebih dahulu dan disepakati oleh pihak yang berkomunikasi. Parameter yang digunakan pada ECC adalah nilai a dan

b, bilangan prima p dari persamaan kurva elips bidang berhingga, dan titik pembangkitan G yang dipilih dari kurva elips.

Pendekatan enkripsi menggunakan ECC ini dapat dijelaskan dengan menggunakan studi kasus. Misalnya, Aldi ingin menerima pesan terenkripsi dari Budi.

a. Pembuatan Kunci Privat dan Publik

Budi menghasilkan kunci privat n_B dengan memilih nomor acak antara nilai $[1, p-1]$. Budi menggunakan kunci privat untuk menghasilkan kunci publik $P_B = n_B \times G$.

b. Enkripsi

Pesan yang akan dikirim misalnya pesan m. Aldi mengkodekan pesan m ke titik P_m pada kurva elips. Kemudian pilihlah bilangan acak k yang nilainya antara $[1, p-1]$. Aldi menghasilkan teks sandi $C_m = \{(k \times G), (P_m + k \times P_B)\}$. Di sini, G adalah titik pembangkitan dan P_B adalah kunci publik Budi.

c. Deskripsi

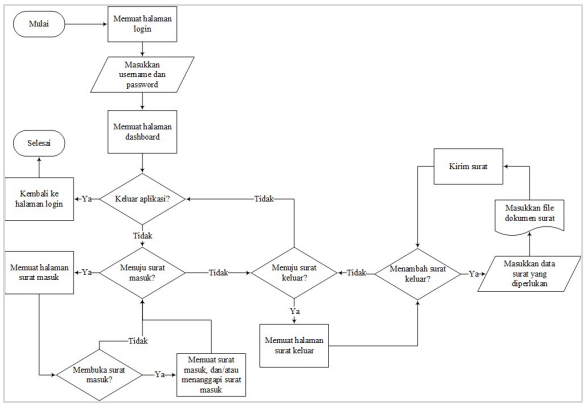
Untuk melakukan deskripsi *ciphertext* C_m, pertama-tama Budi mengalikan titik pertama *ciphertext* dengan kunci pribadinya n_B, lalu mengurangi titik kedua *ciphertext* dari hasil perkaliannya.

$$P_m + k \times n \times P_B - n_B(k \times G) = P_m + k(n_B \times G) - n_B(k \times G) = P_m$$

Budi kemudian menerjemahkan Pm ke dalam pesan asli m.

3. HASIL DAN IMPLEMENTASI

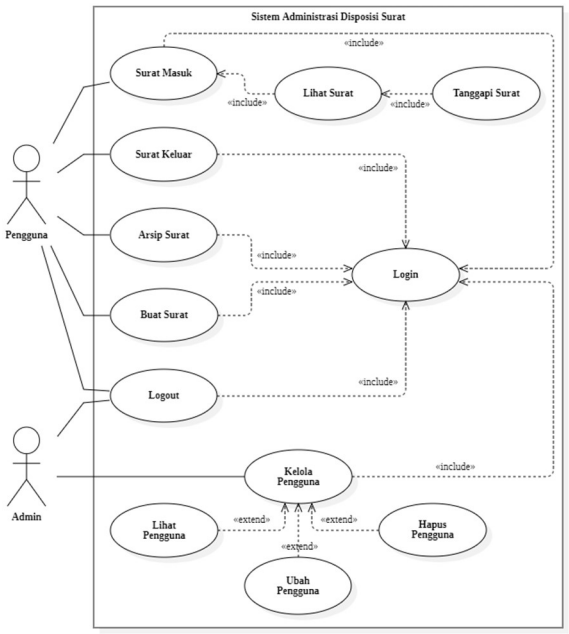
A. Analisis Sistem



Gambar 3 - Flowchart Sistem Administrasi Disposisi Surat

Flowchart dimulai dengan memuat halaman *login*, kemudian pengguna harus mengisi *username* dan *password* yang dimiliki untuk bisa masuk ke dalam sistem administrasi disposisi surat. Setalah pengguna berhasil masuk, sistem akan menampilkan halaman *dashboard* yang merupakan ringkasan daftar dari surat yang dikirim atau diterima. Pada halaman surat masuk, pengguna dapat menanggapi surat yang diterimanya kemudian ditindaklanjuti kepada pengguna lain. Apabila pengguna telah selesai menggunakan sistem administrasi disposisi surat, pengguna dapat melakukan *logout*.

B. *Use Case Diagram*



Gambar 4 - Use Case Diagram Sistem Administrasi Disposisi Surat

Berikut merupakan deskripsi *actor* dari *use case diagram* di atas adalah sebagai berikut:

Tabel 1 - Deskripsi Actor Use Case Diagram

No.	***Actor***	**Deskripsi**
1.	Pengguna	Pengguna dapat mengakses halaman *dashboard*, surat masuk, surat keluar, dan arsip surat setelah melakukan *login* menggunakan akun pengguna.
2.	Admin	Admin dapat mengakses halaman *dashboard* dan kelola pengguna setelah *login* menggunakan akun admin.

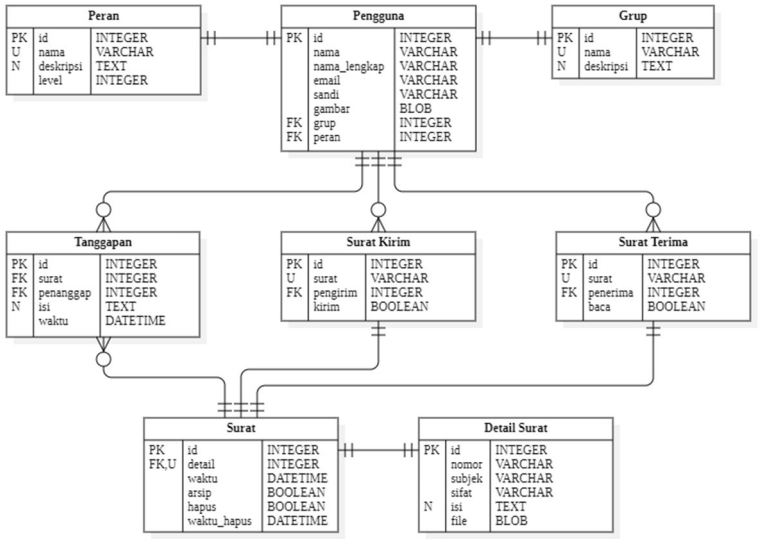
Berikut merupakan deskripsi *system* dari *use case diagram* di atas adalah sebagai berikut:

Tabel 2 - Deskripsi System Use Case Diagram

No.	***System***	**Deskripsi**
1.	*Login*	Fungsi ini digunakan sistem untuk pintu masuk dan verifikasi pengguna/admin yang akan menggunakan sistem administrasi disposisi surat.
2.	Surat Masuk	Fungsi ini digunakan sistem untuk menampilkan halaman berisi surat-surat yang diterima oleh pengguna.
3.	Lihat Surat	Fungsi ini digunakan sistem untuk menampilkan halaman berisi surat yang dipilih dan untuk melihat isi surat.
4.	Tanggapi Surat	Fungsi ini digunakan sistem untuk menampilkan halaman berisi formulir untuk menanggapi surat yang diterima oleh pengguna.
5.	Surat Keluar	Fungsi ini digunakan sistem untuk menampilkan halaman berisi surat-surat yang dikirim dari pengguna.
6.	Arsip Surat	Fungsi ini digunakan sistem untuk menampilkan halaman berisi surat-surat yang diarsipkan dan untuk mengelola pengarsipan surat.

7.	Buat Surat	Fungsi ini digunakan sistem untuk menampilkan halaman berisi formulir untuk mengirim surat kepada pengguna lain.
8.	Kelola Pengguna	Fungsi ini digunakan sistem untuk menampilkan halaman berisi pengguna-pengguna di dalam sistem administrasi disposisi surat dan untuk mengelola pengguna.
9.	Tambah Pengguna	Fungsi ini digunakan sistem untuk menampilkan halaman penambahan pengguna.
10.	Ubah Pengguna	Fungsi ini digunakan sistem untuk menampilkan halaman pengubahan pengguna.
11.	Hapus Pengguna	Fungsi ini digunakan sistem untuk menampilkan halaman penghapusan pengguna.
12.	Dekripsi	Fungsi ini digunakan sistem untuk melakukan dekripsi surat sebelum ditampilkan kepada pengguna.
13.	Enkripsi	Fungsi ini digunakan sistem untuk melakukan enkripsi surat sebelum dikirim kepada pengguna lain.
14.	*Logout*	Fungsi ini digunakan sistem untuk mengakhiri sesi pengguna/admin yang sedang digunakan.

C. *Entity Relationship Diagram*



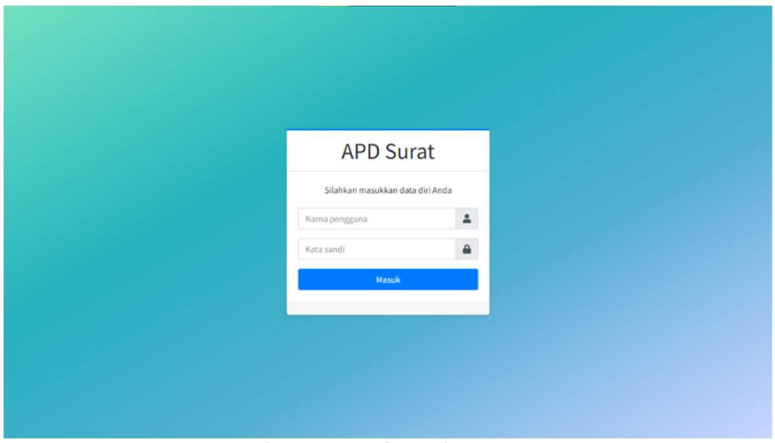
Gambar 5 - Entity Relationship Diagram Sistem Administrasi Disposisi Surat

Terdapat beberapa tabel yang ada di dalam *database* pada pembangunan sistem administrasi disposisi surat ini yang saling terhubung dengan masing-masing *primary key* pada setiap tabel. Pada tabel yang terkait dengan surat seperti tabel detail surat akan digunakan sebagai tempat penyimpanan hasil enkripsi dari sistem administrasi ini.

D. Rancangan *User Interface*

D.1. Tampilan Halaman *Login*

Pada halaman *login* ditampilkan sebuah formulir yang harus diisi untuk melakukan verifikasi data pengguna yang akan menggunakan sistem administrasi disposisi surat ini. Isian yang harus diisi berupa *username* dan *password*. Apabila *username* dan *password* sesuai dengan yang tersimpan dalam sistem, maka pengguna akan diarahkan ke halaman *dashboard*.



Gambar 6 - Tampilan Halaman Login

D.2. Tampilan Halaman *Dashboard*

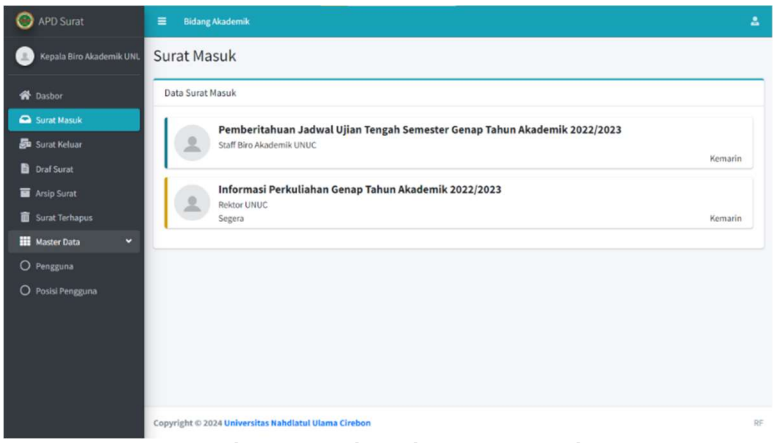
Pada halaman *dashboard* ditampilkan ringkasan jumlah dari daftar surat yang dimiliki pengguna. Daftar surat pengguna dikategorikan ke dalam 4 (empat) kategori, yaitu surat masuk, surat keluar, arsip surat, dan surat terhapus. Apabila masing-masing tombol ditekan akan ditampilkan ke halaman yang sesuai dengan tombol yang ditekan tersebut.

Pada bagian atas halaman ditampilkan bar yang menampilkan nama grup pengguna, profil pengguna, dan juga terdapat tombol *logout*. Pada bagian sisi samping kiri juga terdapat menu navigasi yang dapat dipilih untuk pergi ke halaman lain. Halaman yang dapat diakses tergantung dari hak akses yang dimiliki oleh pengguna.

Gambar 7 - Tampilan Halaman Dashboard

D.3. Tampilan Halaman Surat Masuk

Pada halaman surat masuk ditampilkan daftar keseluruhan surat yang diterima dari pengguna lain kepada pengguna yang sedang digunakan. Setiap surat dapat ditekan untuk melihat detail dari surat tersebut, pengguna akan diarahkan ke halaman detail surat.



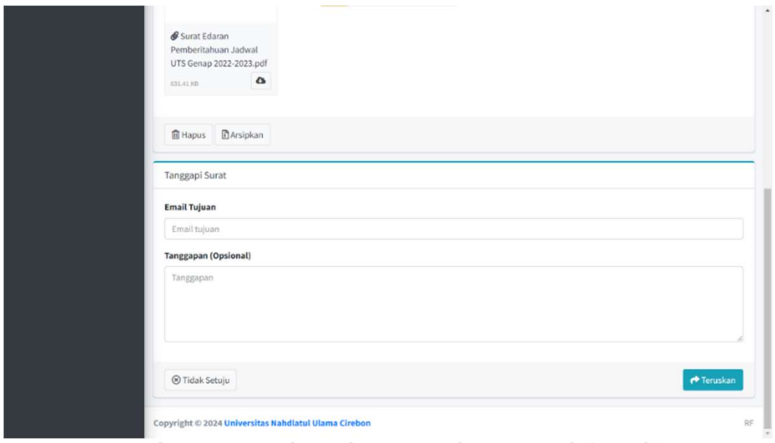
Gambar 8 - Tampilan Halaman Surat Masuk

D.4. Tampilan Halaman Detail Surat Masuk

Pada halaman detail surat masuk ditampilkan detail dari surat yang diterima oleh pengguna dari pengguna lainnya. Detail surat yang ditampilkan berupa nomor surat, alamat email pengirim surat, alamat email penerima surat, waktu surat tersebut dikirimkan, informasi tambahan dari pengirim surat, dan juga file surat yang dilampirkan.

Gambar 9 - Tampilan Halaman Detail Surat Masuk (Atas)

Pada bagian bawah dari halaman detail surat masuk ditampilkan formulir tanggapan yang dapat diisi. Tanggapan dapat berupa komentar, pesan, atau arahan yang dapat dikirim kepada pengirim surat atau kepada pengguna lainnya. Tanggapan yang diteruskan akan dikirim kepada alamat email tujuan yang diisi pada formulir tanggapan. Sedangkan, tanggapan yang tidak disetujui akan dikirim kembali kepada pengirim surat.

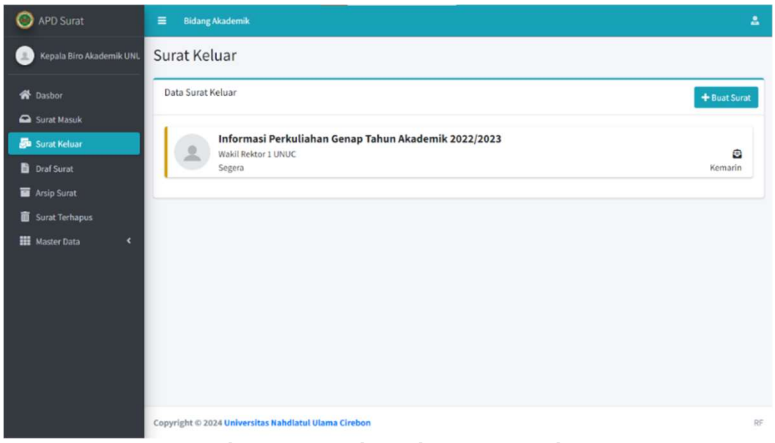


Gambar 10 - Tampilan Halaman Detail Surat Masuk (Bawah)

D.5. Tampilan Halaman Surat Keluar

Pada halaman surat keluar ditampilkan daftar keseluruhan surat yang dikirim pengguna kepada pengguna lainnya. Pada setiap surat akan ditampilkan status terbaca apabila penerima surat sudah membuka surat yang dikirim atau menanggapi surat tersebut. Setiap surat dapat ditekan untuk melihat detail dari surat tersebut, pengguna akan diarahkan ke halaman detail surat.

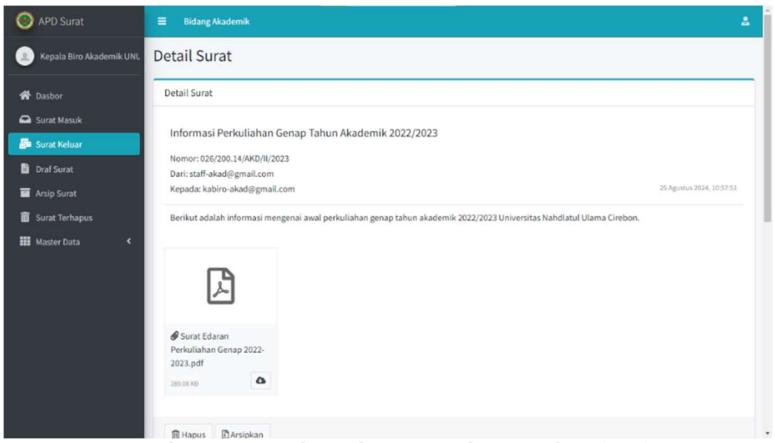
Pada halaman ini juga ditampilkan tombol buat surat untuk membuat dan mengirim surat kepada pengguna lainnya. Apabila pengguna menekan tombol ini, pengguna akan diarahkan ke halaman buat surat.



Gambar 11 - Tampilan Halaman Surat Keluar

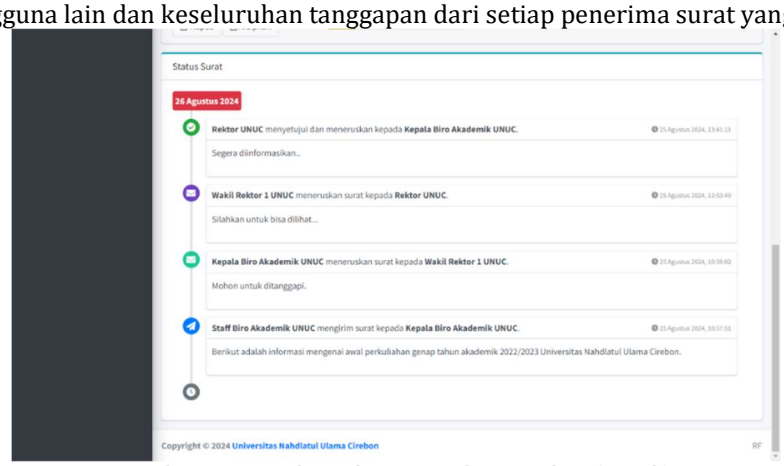
D.6. Tampilan Halaman Detail Surat Keluar

Pada halaman detail surat keluar ditampilkan detail dari surat yang dikirim oleh pengguna kepada pengguna lainnya. Detail surat yang ditampilkan berupa nomor surat, alamat email pengirim surat, alamat email penerima surat, waktu surat tersebut dikirimkan, informasi tambahan dari pengirim surat, dan juga file surat yang dilampirkan.



Gambar 12 - Tampilan Halaman Detail Surat Keluar (Atas)

Pada bagian bawah dari halaman detail surat keluar ditampilkan status surat yang dikirim kepada pengguna lain dan keseluruhan tanggapan dari setiap penerima surat yang diteruskan.



Gambar 13 - Tampilan Halaman Detail Surat Keluar (Bawah)

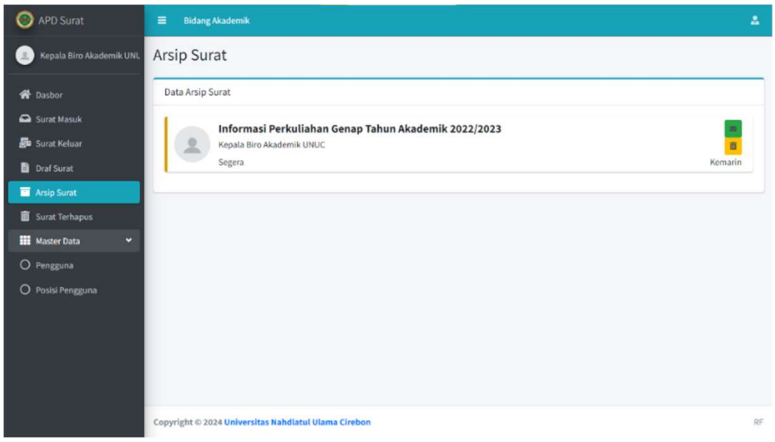
D.7. Tampilan Halaman Buat Surat

Pada halaman buat surat ditampilkan formulir untuk membuat dan mengirim surat kepada pengguna lainnya. Formulir yang harus diisi berupa alamat email tujuan, nomor surat, subjek atau perihal surat, deskripsi atau informasi tambahan yang bersifat opsional, dan juga isian untuk mengunggah file surat. Apabila semua isian sudah terisi, pengguna dapat menekan tombol kirim dan mengirimkan surat kepada pengguna lainnya.

Gambar 14 - Tampilan Halaman Buat Surat

D.8. Tampilan Halaman Arsip Surat

Pada halaman arsip surat ditampilkan daftar keseluruhan surat yang diarsipkan, baik dari kategori surat masuk maupun surat keluar. Di halaman ini, detail surat masih dapat dilihat namun penerima surat tidak dapat menanggapi surat dan pengirim surat tidak bisa melihat status posisi surat saat ini.



Gambar 15 - Tampilan Halaman Arsip Surat

E. Analisis Algoritma

Kriptografi kurva elips merupakan suatu metode kriptografi yang melakukan proses enkripsi dan deskripsi dengan menggunakan titik-titik pada kurva elips sebagai kuncinya.

E.1. Proses Pembangkitan Kunci

Proses pembangkitan kunci menggunakan algoritma ECC dilakukan dengan langkah sebagai berikut:

a. Menentukan bentuk persamaan kurva eliptik

Persamaan kurva eliptik secara umum dijabarkan dengan persamaan:

$$y^2 = x^3 + ax + b \ (mod\ p)$$

Untuk membentuk persamaan kurva eliptik, maka dibutuhkan parameter koefisien a (bilangan bulat), konstanta b (bilangan bulat), dan modulus p (bilangan prima) dengan ketentuan nilai a dan b adalah $4a^3 + 27b^2 \neq 0 \ (mod\ p)$. Pada penelitian ini, sebagai batasan masalah ditetapkan nilai $a = 2$, $b = 2$, dan $p = 17$. Sehingga persamaan kurva eliptik yang akan digunakan adalah sebagai berikut:

$$y^2 = x^3 + 2x + 2 \ (mod\ 17) \ \cdots\cdots \ (1)$$

b. Menentukan titik pembangkitan G di atas kurva eliptik

Dalam penentuan titik pembangkitan G harus diketahui terlebih dahulu titik-titik yang dapat digunakan sebagai titik pembangkitan di atas kurva eliptik yang telah ditentukan pada persamaan (1). Titik-titik ini dicari dengan melakukan substitusi nilai x dan y ke dalam persamaan (1) dengan nilai $F_p = \{x | 0 \leq x \leq p - 1\}$. Berdasarkan perhitungan titik-titik pada kurva eliptik yang dihasilkan dari persamaan (1), maka diambil satu titik sebagai titik pembangkitan G yang bukan merupakan titik *infinity* $O(0, 0)$ yaitu $G(3, 1)$.

c. Membuat kunci privat untuk A dan B

Pemilihan kunci privat ditentukan secara acak di mana nilai kunci privat harus merupakan elemen-elemen bidang hingga $F_p = \{x | 2 \leq x \leq p - 1\}$. Pada penelitian ini, kunci privat yang dipilih untuk A adalah $A_{priv} = 3$ dan kunci privat untuk B adalah $B_{priv} = 8$.

d. Menghitung kunci publik untuk A dan B

Perhitungan kunci publik didasarkan pada persamaan $K_{pub} = K_{priv} \times G$ dengan G merupakan titik pembangkitan kunci. Sehingga diperoleh kunci publik untuk A adalah:

$$A_{pub} = A_{priv} \times G \ \cdots\cdots (2)$$

$$A_{pub} = 3 \times (3, 1) = (0, 11)$$

Sedangkan kunci publik untuk B adalah sebagai berikut:

$$B_{pub} = B_{priv} \times G \cdots\cdots (3)$$
$$B_{pub} = 8 \times (3,1) = (16,4)$$

E.2. Proses Enkripsi

Proses enkripsi pesan dilakukan oleh A dengan menggunakan kunci publik B yang kemudian akan dikirim kepada B. Adapun proses enkripsi ini dilakukan dengan langkah sebagai berikut:

a. Membuat kunci bersama antara A dan B

Kunci bersama digunakan untuk mengacak kunci untuk melakukan enkripsi pesan. Kunci bersama dapat dihitung dengan menggunakan rumus seperti pembangkitan kunci publik dengan menggunakan konstanta k pada perkaliannya. Kunci bersama untuk enkripsi pesan dari A ke B dengan nilai $k = 5$ adalah sebagai berikut:

$$K_{enk} = k \times G \cdots\cdots (4)$$
$$K_{enk} = 5 \times (3,1) = (5,1)$$

b. Melakukan enkripsi pesan

Ambil contoh pesan yang akan dikirimkan adalah $M = (9,16)$, untuk proses enkripsi dilakukan dengan persamaan berikut:

$$M_C = M + k \times B_{pub} \cdots\cdots (5)$$
$$M_C = (9,16) + 5 \times (16,4) = (16,4)$$

c. Mengirim pesan kepada B

Susun kunci bersama dan pesan yang telah dienkripsi sebelum dikirim kepada B. Penyusunan dapat berbentuk seperti berikut:

$$(K_{enk}, M_c) = \big((5,1),(16,4)\big)$$

E.3. Proses Dekripsi

Proses dekripsi pesan dilakukan oleh B dengan menggunakan kunci privat B. Adapun proses dekripsi ini dilakukan dengan persamaan sebagai berikut:

$$M = M_C - B_{priv} \times K_{enk} \cdots\cdots (6)$$
$$M = (16,4) - 8 \times (5,1) = (9,16)$$

Berdasarkan perhitungan di atas, pesan asli dapat diterima dan terbaca dengan hasil $M = (9,16)$.

4. KESIMPULAN

Berdasarkan penelitian dan pengujian yang dilakukan, dapat diambil kesimpulan bahwa:

1. Sistem administrasi disposisi surat berbasis *website* dapat dibangun dan dapat mengirim surat dengan cepat tanpa perlu menunggu jeda waktu dalam proses pengirimannya.
2. Sistem administrasi disposisi surat berbasis *website* dapat digunakan untuk memantau progres penyampaian dan posisi surat yang sedang dikeluarkan atau diajukan.
3. Sistem administrasi disposisi surat berbasis *website* dapat melakukan proses pengarsipan dengan aman.

Sistem administrasi disposisi surat berbasis *website* dapat menjadi solusi yang efektif dan dapat meningkatkan keamanan data pada sistem dengan menerapkan algoritma enkripsi.

DAFTAR PUSTAKA

Alda, M., & Nasution, V. A. (2023, Desember 5). Perancangan Sistem Informasi Disposisi Surat Berbasis Web pada Kantor Badan Narkotika Nasional Kabupaten Deli Serdang. *Jurnal Pendidikan Tambusai, VII*(3), 27716-27724. doi:https://doi.org/10.31004/jptam.v7i3.11146

Alfirdaus, M. H., Tahir, M., Dewanti, N. E., Ardianto, R., Azurah, N. N., & Cahyono, N. F. (2023, Mei 15). Perancangan Aplikasi Enkripsi Deskripsi Mengunakan Metode Caesar Chiper Berbasis Web. *Jurnal Teknik Mesin, Industri, Elektro dan Informatika, II*(2), 64-76. doi:https://doi.org/10.55606/jtmei.v2i2.1628

Damanik, P. S. (2019). Implementasi Algoritma Elliptic Curve Cryptography (ECC) Untuk Penyandian Pesan Pada Aplikasi Chatting Client ServerBerbasis Desktop. *Jurnal Riset Komputer (JURIKOM)*, 395-400.

Latif, N., & Firdaus, A. (2024, Juni 24). *'Hacker' retas pusat data nasional Indonesia, minta tebusan Rp131 miliar*. Diambil kembali dari Benar News: https://www.benarnews.org/indonesian/berita/hacker-pusat-data-nasional-tebusan-131-miliar-06242024112554.html

PT. Integra Inovasi Indonesia. (2021, Desember 28). *Kesulitan Melacak Status Disposisi Surat? Begini Solusinya*. Diambil kembali dari Integra Indonesia: https://www.integraindonesia.co.id/6958/kesulitan-melacak-status-disposisi-surat-begini-solusinya/

Qadafi, K. M. (2019). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA. *Seminar Nasional Sistem Informasi dan Teknik Informatika*, (hal. 219-228). Pontianak. Diambil kembali dari https://ejurnal.dipanegara.ac.id/index.php/sensitif/article/view/547

Rahmawati, D., Kumaladewi, N., & Sugiarti, Y. (2018, Mei 1). Sistem Informasi Disposisi Surat Berbasis Android. *Applied Information Systems and Management, I*(1), 45-50. doi:https://doi.org/10.15408/aism.v1i1.8671

Taopan, G. I., Boru, M., & Fanggidae, A. (2022, Maret 19). Pengamanan Portable Document Format (PDF) Menggunakan Algoritma Kriptografi Eliptik. *Jurnal Komputer dan Informatika, X*(1), 47-54. doi:https://dx.doi.org/10.35508/jicon.v10i1.5296

Yusman, Y., & Harahap, S. P. (2020, Januari 8). Implementasi Website Alumni pada SMP PGRI 1 Padang. *Community Engangement & Emergence, I*(1), 27-29. doi:https://doi.org/10.37385/ceej.v1i1.44