

**IMPLEMENTASI ENKRIPSI ALGORITMA ECC (ELLIPTIC CURVE
CRYPTOGRAPHY) UNTUK KEAMANAN DATA SISTEM
ADMINISTRASI DISPOSISI SURAT
BERBASIS WEBSITE**

(Studi Kasus Universitas Nahdlatul Ulama Cirebon)

Skripsi ini diajukan sebagai salah satu syarat
untuk memperoleh gelar Sarjana Komputer.



OLEH:

RAFIANTO

NIM: 0402201045

FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS NAHDLATUL ULAMA CIREBON

2024 M / 1446 H



UNIVERSITAS NAHDLATUL ULAMA CIREBON
LEMBAR PENGESAHAN STATUS SKRIPSI

JUDUL : IMPLEMENTASI ENKRIPSI ALGORITMA ECC (ELLIPTIC CURVE CRYPTOGRAPHY) UNTUK KEAMANAN DATA SISTEM ADMINISTRASI DISPOSISI SURAT BERBASIS WEBSITE

SAYA : RAFIANTO

NIM : 0402201045

Mengizinkan skripsi Sarjana Komputer ini disimpan di perpustakaan Universitas Nahdlatul Ulama Cirebon dengan syarat-syarat kegunaan sebagai berikut:

1. Skripsi adalah hak milik Universitas Nahdlatul Ulama Cirebon.
2. Perpustakaan Universitas Nahdlatul Ulama Cirebon dibenarkan membuat salinan untuk referensi saja.
3. Perpustakaan juga dibenarkan membuat salinan skripsi ini sebagai bahan pertukaran antara institusi pendidikan tinggi.
4. Berikan tanda ✓ sesuai dengan kategori skripsi:
 - ☐ Sangat rahasia (Mengandung isi tentang keselamatan atau kepentingan negara Indonesia)
 - ☐ Rahasia (Mengandung isi tentang kerahasiaan dari sesuatu badan/organisasi di mana penelitian skripsi ini dikerjakan)
 - ☒ Biasa

Disahkan oleh:

Dicky Andika Sulaeman, M.Kom.

Tanggal: 12 September 2024

Abdul Kohar, M.Kom.

Tanggal: 12 September 2024



UNIVERSITAS NAHDLATUL ULAMA CIREBON

LEMBAR PERNYATAAN PENULIS

JUDUL : IMPLEMENTASI ENKRIPSI ALGORITMA ECC (ELLIPTIC CURVE CRYPTOGRAPHY) UNTUK KEAMANAN DATA SISTEM ADMINISTRASI DISPOSISI SURAT BERBASIS WEBSITE

SAYA : RAFIANTO

NIM : 0402201045

“Saya menyatakan dan bertanggungjawab dengan sebenarnya bahwa skripsi ini adalah hasil karya saya sendiri kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya. Jika pada waktu selanjutnya ada pihak lain yang mengklaim bahwa skripsi ini sebagai karyanya, yang disertai dengan bukti-bukti yang cukup, maka saya bersedia untuk membatalkan gelar Sarjana Komputer saya beserta segala hak dan kewajiban yang melekat pada gelar tersebut”.

Cirebon, 22 Agustus 2024



RAFIANTO

NIM: 0402201045



UNIVERSITAS NAHDLATUL ULAMA CIREBON

LEMBAR PERSETUJUAN SKRIPSI

JUDUL : IMPLEMENTASI ENKRIPSI ALGORITMA ECC (ELLIPTIC CURVE CRYPTOGRAPHY) UNTUK KEAMANAN DATA SISTEM ADMINISTRASI DISPOSISI SURAT BERBASIS WEBSITE

SAYA : RAFIANTO

NIM : 0402201045

Skrripsi ini telah diperiksa dan disetujui,
Cirebon, 22 Agustus 2024

Pembimbing I

Dicky Andika Sulaeman, M.Kom.
NIDN. 0409069402

Pembimbing II

Abdul Kohar, M.Kom.
NIDN. 0412068704

Ketua Program Studi

Dicky Andika Sulaeman, M.Kom.
NIDN. 0409069402



UNIVERSITAS NAHDLATUL ULAMA CIREBON

LEMBAR PENGESAHAN SKRIPSI

JUDUL : IMPLEMENTASI ENKRIPSI ALGORITMA ECC (ELLIPTIC CURVE CRYPTOGRAPHY) UNTUK KEAMANAN DATA SISTEM ADMINISTRASI DISPOSISI SURAT BERBASIS WEBSITE

SAYA : RAFIANTO

NIM : 0402201045

Skripsi ini telah diujikan dan dipertahankan di hadapan Dewan Penguji pada Sidang Skripsi tanggal 29 Agustus 2024 menurut pandangan kami, Skripsi ini memadai untuk penganugerahan gelar Sarjana Komputer (S.Kom.).

	Tanggal	Tanda Tangan
Pembimbing I, <u>Dicky Andika Sulaeman, M. Kom.</u> NIDN. 0409069402	12-09-2024	
Pembimbing II, <u>Abdul Kohar, M.Kom.</u> NIDN. 0412068704	12-09-2024	
Penguji I, <u>Rosidin, M.Kom.</u> NIDN. 0415028303	10-09-2024	
Penguji II, <u>Sukarsa, M.Kom.</u> NIDN. 0418117605	09-09-2024	

Mengetahui,
Dekan Fakultas Ilmu Komputer
Universitas Nahdlatul Ulama Cirebon

Rosidin, M.Kom.
NIDN. 0415028303

ABSTRACT

Mail disposition is the process of managing and distributing mail in an agency that includes receiving the mail, determining the necessary action, and transferring the mail to the party responsible for taking the action. All letters circulated must be properly managed, actions taken must be determined appropriately, and replies must be given in a timely manner.

At the University of Nahdlatul Ulama Cirebon there are still several obstacles and problems related to the letter disposition system currently implemented. Letters sent are often delayed or not sent as they should. In addition, the position of letters that have been sent cannot be tracked properly. Even archived letters sometimes get lost. It is also necessary to integrate with today's growing technology, especially in terms of system effectiveness and efficiency.

This research aims to build a letter disposition administration system using website-based online information technology media and implement encryption algorithms to improve system security. The development method used is the RUP (Rational Unified Process) method which is carried out with a systematic approach, starting from the inception stage, elaboration stage, construction stage, and transition stage.

Testing is done by conducting test cases on the letter creation page to the letter filing process. The test results state that the letter disposition administration system that was built achieved the results as expected.

Keywords: *Administration System, Letter Disposition, Letter Monitoring, Encryption Algorithm*

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.

Kata Kunci: Sistem Administrasi, Disposisi Surat, Pemantauan Surat, Algoritma Enkripsi

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Allah SWT., karena atas rahmat dan karunia-Nya sehingga dalam penyusunan skripsi ini penulis dapat menyelesaikan tanpa mengalami hambatan yang berarti.

Tersusunnya skripsi ini merupakan hasil peran serta, dukungan, dan bimbingan dari berbagai pemangku kepentingan, baik secara spiritual maupun material. Oleh karena itu, penulis memanjatkan doa kepada Allah SWT. pada kesempatan berharga ini, semoga Allah SWT. memberikan balasan kepada Bapak, Ibu, serta rekan-rekan yang telah memberikan dukungan dan bantuan kepada penulis.

Tidak lupa juga penulis mengucapkan terima kasih dan penghargaan yang sedalam-dalamnya kepada:

1. Bapak Dr. Agus Sugiarto, S.H., M.H., M.M., selaku Rektor Universitas Nahdlatul Ulama (UNU) Cirebon.
2. Bapak Rosidin, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Nahdlatul Ulama (UNU) Cirebon.
3. Bapak Dicky Andika Sulaeman, M.Kom., selaku Ketua Program Studi Teknik Informatika sekaligus menjadi Dosen Pembimbing I.
4. Bapak Abdul Kohar, M.Kom., selaku Dosen Pembimbing II.
5. Ibu Neneng Euis Susanti, selaku Narasumber Staf Rektorat Universitas Nahdlatul Ulama (UNU) Cirebon.
6. Bapak Prasetyo Adi Wibowo, S.T., M.T., selaku Narasumber Kepala Biro Kemahasiswaan Universitas Nahdlatul Ulama (UNU) Cirebon.
7. Dosen-dosen Fakultas Ilmu Komputer Universitas Nahdlatul Ulama (UNU) Cirebon.
8. Terima kasih terhadap kedua orang tua yang selalu mendoakan, mendukung, memberi semangat dan pengarahan hingga dapat berada pada titik ini.

9. Teman-teman semua yang telah memberikan pandangan dan wawasan kepada penulis dalam rangka menyelesaikan skripsi ini.

Penulis juga menyampaikan terima kasih kepada semua pihak yang terlibat walaupun tidak dapat disebutkan satu per satu, yang telah banyak memberikan dukungan luar biasa kepada penulis sehingga penulisan skripsi ini dapat terselesaikan, semoga Allah SWT. membalas dengan imbalan yang berlipat ganda. Amiin.

Segala rintangan dan hambatan yang dialami penulis selama penyusunan skripsi ini tidak membuat penulis berputus asa dan putus harapan. Penulis mengharapkan kritik dan saran yang bersifat membangun demi kemanfaatan skripsi ini.

Akhir kata penulis mohon maaf apabila masih banyak kekurangan dalam penyusunan laporan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi semua pihak yang memerlukan. Aamiin.

Cirebon, 30 Juli 2024

Penulis,

DAFTAR ISI

LEMBAR PENGESAHAN STATUS SKRIPSI	ii
LEMBAR PERNYATAAN PENULIS.....	iii
LEMBAR PERSETUJUAN SKRIPSI.....	iv
LEMBAR PENGESAHAN SKRIPSI.....	v
<i>ABSTRACT</i>	vi
ABSTRAK	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xv
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Identifikasi Masalah	3
1.3. Rumusan Masalah.....	3
1.4. Tujuan Penelitian.....	4
1.5. Batasan Masalah.....	4
1.6. Manfaat Penelitian.....	5
1.7. Metode Penelitian	5
1.8. Sistematika Penulisan	7
1.9. Kerangka Berpikir	8
BAB II LANDASAN TEORI	10
2.1. Keterkaitan Penelitian dengan Ayat Suci Al-Qur'an	10
2.2. Tinjauan Pustaka.....	11
2.3. Dasar Teori	22
2.3.1. Kriptografi.....	22
2.3.2. Algoritma ECC.....	24
2.3.3. Administrasi Surat.....	25

2.3.4. Disposisi Surat	25
2.3.5. Sistem Informasi	25
2.3.6. <i>Website</i>	25
2.3.7. <i>Black Box</i>	26
2.4. <i>Tools</i> Perancangan, Pengembangan Sistem, dan Bahasa Pemrograman.....	27
2.4.1. Perancangan Sistem	27
2.4.2. Pengembangan Sistem	37
2.4.3. Bahasa Pemrograman.....	38
BAB III ANALISIS DAN PERANCANGAN SISTEM	40
3.1. Analisis Kebutuhan Sistem.....	40
3.1.1. Tempat dan Waktu Penelitian.....	40
3.1.2. Analisis Masalah.....	40
3.1.3. Sistem Berjalan	41
3.1.4. Sistem yang Dibangun	41
3.1.5. Kebutuhan Sistem	41
3.1.6. Analisis Algoritma	43
3.2. Desain Perancangan Sistem.....	45
3.2.1. Desain Sistem.....	45
3.2.2. <i>Database</i>	65
3.2.3. <i>Mockup Interface</i>	66
3.2.4. Perancangan Pengujian	71
BAB IV IMPLEMENTASI PENGEMBANGAN DAN PENGUJIAN SISTEM.....	78
4.1. Implementasi	78
4.1.1. Implementasi <i>Database</i>	78
4.1.2. Implementasi <i>Interface</i>	79
4.1.3. Implementasi Algoritma ECC.....	88
4.2. Pengujian	88
4.2.1. Pengujian <i>Interface</i>	88
4.2.2. Pengujian Algoritma ECC.....	106
BAB V KESIMPULAN DAN SARAN.....	109

5.1. Kesimpulan.....	109
5.2. Saran.....	109
DAFTAR PUSTAKA	110

DAFTAR GAMBAR

Gambar 1 - Alur Metode RUP	6
Gambar 2 - Kerangka Berpikir.....	8
Gambar 3 - Contoh Pengujian Black Box.....	27
Gambar 4 - Logo Microsoft Visio.....	27
Gambar 5 - Logo StarUML.....	29
Gambar 6 - Contoh Use Case Diagram.....	33
Gambar 7 - Contoh Activity Diagram.....	36
Gambar 8 - Project Timeline.....	40
Gambar 9 - Flowchart Aplikasi.....	45
Gambar 10 - Use Case Diagram Sistem Administrasi Disposisi Surat.....	46
Gambar 11 - Activity Diagram Login.....	48
Gambar 12 - Activity Diagram Surat Masuk	50
Gambar 13 - Activity Diagram Lihat Surat.....	51
Gambar 14 - Activity Diagram Dekripsi Surat	52
Gambar 15 - Activity Diagram Tanggapi Surat.....	53
Gambar 16 - Activity Diagram Surat Keluar	54
Gambar 17 - Activity Diagram Arsip Surat	55
Gambar 18 - Activity Diagram Buat Surat	56
Gambar 19 - Activity Diagram Enkripsi.....	57
Gambar 20 - Activity Diagram Kelola Pengguna	58
Gambar 21 - Activity Diagram Tambah Pengguna.....	59
Gambar 22 - Activity Diagram Ubah Pengguna	61
Gambar 23 - Activity Diagram Hapus Pengguna	62
Gambar 24 - Activity Diagram Logout.....	64
Gambar 25 - Entity Relationship Diagram.....	65
Gambar 26 - Wireframe Login.....	66
Gambar 27 - Wireframe Dashboard.....	66
Gambar 28 - Wireframe Surat Masuk.....	67

Gambar 29 - Wireframe Detail Surat Masuk	67
Gambar 30 - Wireframe Surat Keluar	68
Gambar 31 - Wireframe Detail Surat Keluar	69
Gambar 32 - Wireframe Tambah Surat.....	69
Gambar 33 - Wireframe Arsip Surat.....	70
Gambar 34 - Wireframe Surat Terhapus.....	70
Gambar 35 - Database System	78
Gambar 36 - Interface Halaman Login	79
Gambar 37 - Interface Halaman Dashboard Admin	80
Gambar 38 - Interface Halaman Dashboard User	81
Gambar 39 - Interface Halaman Surat Masuk.....	81
Gambar 40 - Interface Halaman Detail Surat Masuk (Atas).....	82
Gambar 41 - Interface Halaman Detail Surat Masuk (Bawah).....	82
Gambar 42 - Interface Halaman Surat Keluar.....	83
Gambar 43 - Interface Halaman Detail Surat Keluar (Atas).....	84
Gambar 44 - Interface Halaman Detail Surat Keluar (Bawah).....	85
Gambar 45 - Interface Halaman Buat Surat	85
Gambar 46 - Interface Halaman Arsip Surat.....	86
Gambar 47 - Interface Halaman Data Pengguna.....	87
Gambar 48 - Interface Halaman Tambah Pengguna	87
Gambar 49 - Interface Halaman Data Pengguna Terenkripsi	88
Gambar 50 - Hasil Enkripsi.....	108
Gambar 51 - Hasil Dekripsi	108

DAFTAR TABEL

Tabel 1 - Studi Literatur.....	11
Tabel 2 - Simbol Use Case Diagram.....	32
Tabel 3 - Simbol Activity Diagram.....	35
Tabel 4 - Deskripsi Actor Use Case.....	46
Tabel 5 - Deskripsi System Use Case	47
Tabel 6 - Skenario Black Box - Login	71
Tabel 7 - Skenario Black Box - Dashboard	72
Tabel 8 - Skenario Black Box - Surat Masuk	72
Tabel 9 - Skenario Black Box - Lihat Surat.....	72
Tabel 10 - Skenario Black Box - Tanggapi Surat	73
Tabel 11 - Skenario Black Box - Surat Keluar	74
Tabel 12 - Skenario Black Box - Arsip Surat	74
Tabel 13 - Skenario Black Box - Buat Surat.....	74
Tabel 14 - Skenario Black Box - Kelola Pengguna	75
Tabel 15 - Skenario Black Box - Logout	77
Tabel 16 - Pengujian Skenario Black Box - Login	89
Tabel 17 - Pengujian Skenario Black Box - Dashboard	91
Tabel 18 - Pengujian Skenario Black Box - Surat Masuk	93
Tabel 19 - Pengujian Skenario Black Box - Lihat Surat.....	94
Tabel 20 - Pengujian Skenario Black Box - Tanggapi Surat	95
Tabel 21 - Pengujian Skenario Black Box - Surat Keluar	97
Tabel 22 - Pengujian Skenario Black Box - Arsip Surat	98
Tabel 23 - Pengujian Skenario Black Box - Buat Surat.....	99
Tabel 24 - Pengujian Skenario Black Box - Kelola Pengguna	101
Tabel 25 - Pengujian Skenario Black Box - Logout	105
Tabel 26 - Pengujian Algoritma ECC	107

BAB I

PENDAHULUAN

1.1. Latar Belakang

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).

Pada pemerintahan, surat adalah sarana komunikasi yang tertulis untuk menyampaikan pesan dan informasi dari masyarakat kepada dunia usaha dan pihak berwenang (Yusuf, Muin, & Nisrawati, Rancang Bangun Aplikasi Disposisi Persuratan Berbasis Mobile Apps, 2022). Dengan berkembangnya teknologi informasi secara umum saat ini, aktivitas dan proses surat-menyurat yang sebelumnya dilakukan secara manual, kini beralih memanfaatkan teknologi informasi yang ada dengan menggunakan surat elektronik atau email. Menurut Kamus Besar Bahasa Indonesia dalam konteks administrasi dan kepegawaian, disposisi adalah pendapat seorang pejabat mengenai urusan yang termuat dalam suatu surat dinas, yang langsung dituliskan pada surat yang bersangkutan atau pada lembar khusus (Badan Pengembangan dan Pembinaan Bahasa, 2023).

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 merupakan salah satu media pemberitahuan informasi yang penting bagi suatu instansi universitas (Rahmawati, Kumaladewi, & Sugiarti, 2018). Hal ini akan membantu memastikan bahwa setiap surat yang diedarkan dikelola dengan

baik, tindakan yang perlu diambil ditentukan dengan tepat, dan respons yang diberikan tepat waktu.

Namun, berdasarkan hasil observasi dan wawancara pada rektorat dan biro kemahasiswaan di Universitas Nahdlatul Ulama Cirebon pada tanggal 25-26 Februari 2024, masih terdapat beberapa kendala dan masalah terkait sistem disposisi surat yang saat ini diterapkan di Universitas Nahdlatul Ulama Cirebon. Menurut bapak Prasetyo Adi Wibowo, S.T., M.T., 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. Seperti yang diketahui bahwa tidak lama ini terdapat kasus pencurian data pada Pusat Data Nasional (PDN) yang mengakibatkan hilangnya data-data penting seperti informasi data pribadi warga, data ekonomi, hingga data pendidikan yang terjadi pada bulan Juni 2024. Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa terdapat 401 juta serangan siber yang terjadi pada tahun 2023 saja. Serangan ini dapat menyebabkan penurunan kinerja perangkat dan jaringan, pencurian data sensitif, kerusakan reputasi, dan bahkan hilangnya kepercayaan terhadap suatu organisasi (Latif & Firdaus, 2024).

Berdasarkan latar belakang yang telah dijelaskan, penulis tertarik untuk melakukan penelitian di Universitas Nahdlatul Ulama Cirebon dengan tema “Implementasi Enkripsi Algoritma ECC (*Elliptic Curve Cryptography*) untuk Keamanan Data Sistem Administrasi Disposisi Surat Berbasis *Website*”.

1.2. Identifikasi Masalah

Berdasarkan latar belakang masalah di atas, berikut identifikasi permasalahan yang diperoleh penulis di antaranya:

1. Surat yang telah dikeluarkan atau diajukan sering kali mengalami keterlambatan, bahkan tidak tersampaikan kepada atasan seperti seharusnya.
2. Surat yang telah dikeluarkan atau diajukan tidak dapat dipantau progres penyampaian dan tidak diketahui keberadaannya.
3. Hilangnya surat-surat yang telah diarsipkan.
4. Perlu adanya integrasi dengan sistem informasi, terutama dalam keefektifan dan keamanan data pada sistem.

1.3. Rumusan Masalah

Berdasarkan identifikasi permasalahan yang telah dipaparkan sebelumnya, terdapat beberapa rumusan masalah yang dapat dirumuskan oleh penulis, di antaranya sebagai berikut:

1. Bagaimana membangun sistem yang dapat menyampaikan surat tanpa jeda waktu pada saat pengiriman surat?
2. Bagaimana sistem yang dibangun dapat memantau progres penyampaian surat setelah surat dikeluarkan atau diajukan?
3. Bagaimana membangun sistem yang dapat melakukan pengarsipan surat dan menyimpan surat dengan aman?
4. Bagaimana membangun sistem dengan integrasi sistem informasi sehingga dapat meningkatkan keefektifan dan utamanya keamanan data pada sistem dengan menerapkan algoritma enkripsi?

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan di atas, berikut ini adalah tujuan penelitian dengan tema “Implementasi Enkripsi Algoritma ECC (*Elliptic Curve Cryptography*) untuk Keamanan Data Sistem Administrasi Disposisi Surat Berbasis *Website*”, di antaranya sebagai berikut:

1. Untuk mengetahui cara membangun sistem administrasi berbasis *website* yang dapat menyampaikan surat tanpa jeda waktu pada proses pengiriman surat.
2. Untuk mengetahui cara membangun sistem administrasi berbasis *website* yang dapat memantau progres penyampaian surat hingga diterima oleh pihak yang berkepentingan.
3. Untuk mengetahui cara membangun sistem administrasi berbasis *website* yang dapat melakukan pengarsipan surat dengan baik.
4. Untuk mengetahui cara membangun sistem administrasi berbasis *website* dengan menggunakan teknologi sistem informasi *online* dan menerapkan algoritma enkripsi sebagai metode pengamanan data pada sistem.

1.5. Batasan Masalah

✓ Ruang Lingkup Penelitian

Penelitian ini hanya dilakukan di Universitas Nahdlatul Ulama Cirebon pada bagian biro dan fakultas. Penelitian hanya tertuju pada sistem administrasi disposisi surat di lingkungan internal kampus dan belum melibatkan lingkungan eksternal di luar Universitas Nahdlatul Ulama Cirebon.

✓ Fitur Sistem Administrasi

Sistem administrasi yang akan dibangun mencakup pengelolaan surat masuk, surat keluar, pemantauan surat, dan pengarsipan surat.

✓ Penerapan Algoritma Enkripsi

Algoritma enkripsi yang digunakan menggunakan algoritma ECC (*Elliptic Curve Cryptography*) dengan memanfaatkan kunci publik dan kunci privat. Algoritma enkripsi digunakan untuk mengunci data *file* surat yang diedarkan melalui sistem yang akan dibangun.

1.6. Manfaat Penelitian

Manfaat penelitian ini dapat diuraikan sebagai berikut:

1. Diharapkan dapat meningkatkan keefektifan dan menjadi solusi yang tepat atas kendala yang dihadapi saat ini di lingkungan Universitas Nahdlatul Ulama Cirebon.
2. Diharapkan dapat memberikan pengetahuan dan wawasan baru kepada masyarakat luas maupun penelitian yang akan datang terkait sistem administrasi disposisi surat dan implementasi keamanan data.

1.7. Metode Penelitian

1.7.1. Pengumpulan Data

Metode pengumpulan data pada penelitian ini yaitu studi literatur, observasi, dan wawancara. Metode penelitian ini menggunakan pendekatan kualitatif dalam pengumpulan dan pengolahan data penelitian.

- Studi Literatur

Data yang dikumpulkan melalui studi literatur ini berupa analisis jurnal-jurnal yang berkaitan dengan tema dan topik penelitian. Studi literatur juga berguna agar penulis dapat memiliki gambaran mengenai penelitian yang akan dilakukan dari penelitian lain yang serupa dan telah dilakukan.

- Observasi

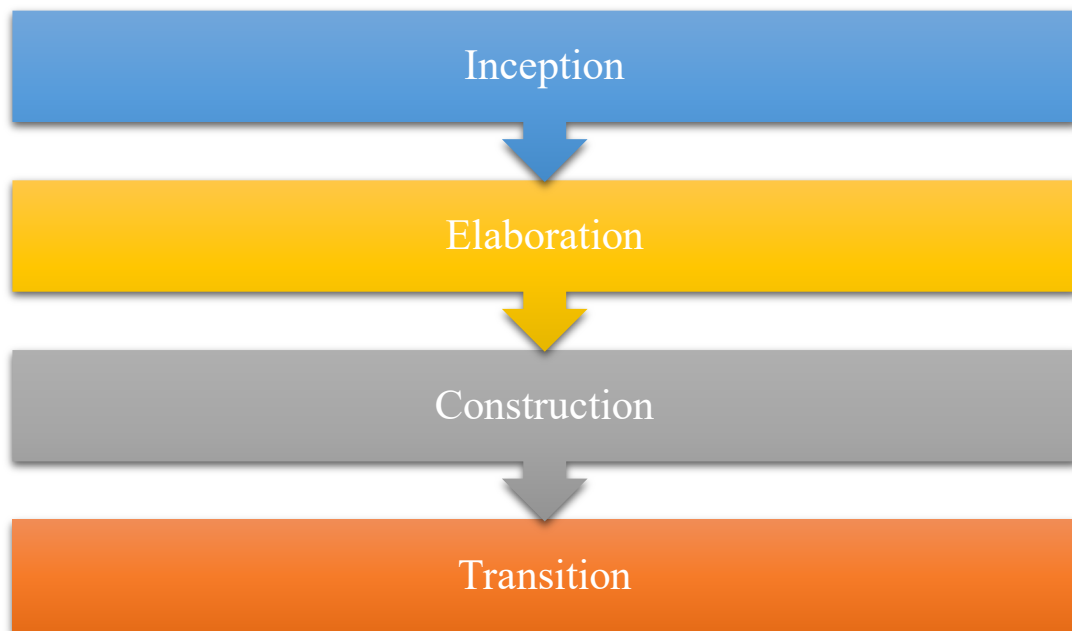
Observasi dilakukan dengan mengunjungi tempat penelitian dan mengamati proses administrasi yang dilakukan. Observasi berguna agar penulis memiliki gambaran mengenai perancangan sistem yang baik dan dapat menjadi solusi yang efektif bagi pengguna.

- Wawancara

Wawancara dilakukan kepada kepala biro kemahasiswaan dan staf rektorat. Wawancara ini dilakukan dengan tujuan agar penulis dapat memahami permasalahan yang sering dialami pada saat melakukan administrasi disposisi surat.

1.7.2. Metode Pengembangan Perangkat Lunak

Metode pengembangan yang digunakan pada penelitian ini adalah metode RUP (*Rational Unified Process*). Metode ini dilakukan dengan pendekatan yang sistematis, dimulai dari tahap *inception*, tahap *elaboration*, tahap *construction*, dan tahap *transition*.



Gambar 1 - Alur Metode RUP

Berikut penjabaran setiap tahap menurut

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*.

1.8. Sistematika Penulisan

Penulisan laporan penelitian ini tersusun atas 5 (lima) bab dan di dalamnya terdapat sub-sub yang akan membahas dan memberikan penjelasan yang lebih terperinci. Berikut ini sistematika penulisan pada laporan penelitian ini di antaranya sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi tentang Latar Belakang, Identifikasi Masalah, Rumusan Masalah, Tujuan Penelitian, Batasan Masalah, Manfaat Penelitian, Metode Penelitian, Sistematika Penulisan, Kerangka Berpikir.

BAB II LANDASAN TEORI

Pada bab ini berisi tentang Keterkaitan Penelitian dengan Ayat Suci Al-Qur'an, Tinjauan Pustaka, Dasar Teori Penelitian, serta Tools Perancangan dan Pengembangan Sistem.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini berisi tentang Penjelasan mengenai sistem administrasi surat yang saat ini berjalan, Perancangan sistem aplikasi yang akan dibangun.

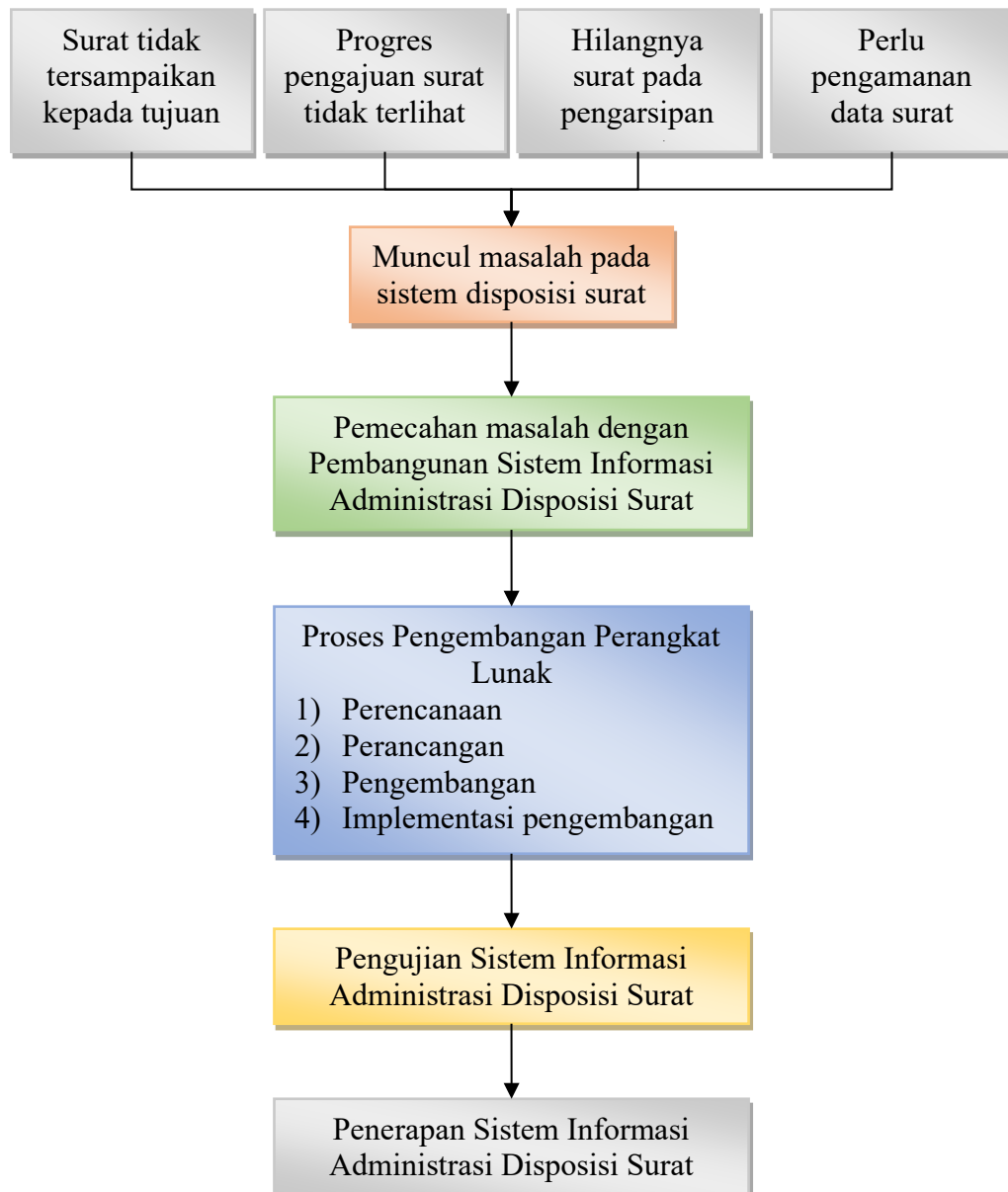
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini berisi tentang Implementasi perancangan sistem berdasarkan perancangan yang telah dibuat, Pengujian terhadap sistem yang dibangun.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dan saran dari penulis mengenai penelitian ini.

1.9. Kerangka Berpikir



Gambar 2 - Kerangka Berpikir

Disposisi surat adalah proses pengelolaan dan pendistribusian surat di sebuah instansi yang melibatkan penerimaan surat, penentuan tindakan yang perlu diambil, serta pengalihan surat kepada pihak yang bertanggung jawab untuk menyelesaikan tindakan yang dimaksud. Penyampaian disposisi surat perlu ditindaklanjuti dengan cepat. Namun dalam penerapannya di Universitas Nahdlatul Ulama Cirebon, ditemukannya beberapa permasalahan yang menyebabkan penyampaian disposisi surat ini menjadi terhambat.

Permasalahan yang muncul berupa tidak adanya kejelasan mengenai status surat yang telah disampaikan, dan juga dalam pengarsipan surat yang masih bersifat konvensional menyebabkan rentannya kehilangan data surat yang telah diterima. Sehingga perlu adanya sistem administrasi disposisi surat yang lebih efektif dan dapat diakses pada kondisi apa pun. Sistem administrasi juga perlu mempertimbangkan keamanan datanya agar berkas surat yang diedarkan dapat terlindungi dari akses yang tidak diperbolehkan.

Sistem administrasi yang akan dibangun hanya ditujukan di lingkungan internal Universitas Nahdlatul Ulama Cirebon. Fitur dari sistem yang dibangun mencakup pengelolaan surat masuk, surat keluar, pemantauan surat, dan pengarsipan surat.

Sistem administrasi disposisi surat akan diimplementasikan dan diuji di lingkungan Universitas Nahdlatul Ulama Cirebon. Hasil dari pengimplementasian ini diharapkan dapat meningkatkan keefektifan dalam administrasi disposisi surat.

BAB II

LANDASAN TEORI

2.1. Keterkaitan Penelitian dengan Ayat Suci Al-Qur'an

Diambil dari jurnal berjudul “Sistem Pengenalan dan Penerjemahan Al-Qur'an Surah Al-Waqi'ah melalui Suara Menggunakan Transformasi Sumudu” (Ula, Risawandi, & Rosdian, 2019), Al-Qur'an menurut bahasa berarti bacaan atau yang dibaca. Menurut istilah, Al-Qur'an adalah wahyu Allah SWT. yang diturunkan kepada Nabi Muhammad SAW. melalui malaikat Jibril sebagai petunjuk bagi umat manusia. Pengertian surah ditinjau dari sisi etimologi adalah manzilah atau kedudukan. Surah secara terminologi berarti sejumlah ayat Al-Qur'an yang mempunyai permulaan dan kesudahan. Secara bahasa, ayat dapat diartikan sebagai mukjizat, tanda atau alamat, pelajaran atau peringatan, suatu hal yang menakjubkan, kelompok atau kumpulan, dan bukti. Secara istilah ayat diartikan sebagai sejumlah kalam Allah SWT. yang terdapat dalam suatu surat Al-Qur'an.

Sebagai umat Islam, Al-Qur'an merupakan pedoman dalam menjalani kehidupan di dunia. Agama Islam tidak hanya mengatur hubungan antara manusia dengan Allah SWT., namun juga hubungan antara semua makhluk hidup ciptaan Allah SWT. Sebagai ajaran yang bersifat universal, Islam meyakini bahwa perlindungan data pribadi adalah tujuan syariat yang harus diwujudkan. Dalam surah An-Nur ayat 27, Allah SWT. berfirman:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ
لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

“Wahai orang-orang yang beriman, janganlah memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Demikian itu lebih baik bagimu agar kamu mengambil pelajaran.” (QS. An-Nur [24]: 27)

Sistem jaringan keamanan yang mencegah akses tidak sah dari jaringan pribadi di masa modern disebut *firewall*. Sistem ini mirip dengan kisah Raja Zulkarnain dalam surat Al-Kahfi ayat 96.

أَتُونِي زُبَرَ الْحَدِيدِ حَتَّى إِذَا سَاوَى بَيْنَ الصَّدَفَيْنِ قَالَ انْفُخُوا حَتَّى إِذَا جَعَلَهُ نَارًا قَالَ أَتُونِي أُفْرِغَ عَلَيْهِ قِطْرًا

“Berilah aku potongan-potongan besi.” Hingga ketika (potongan besi) itu telah (terpasang) sama rata dengan kedua (puncak) gunung itu, dia (Zulqarnain) berkata, “Tiuplah (api itu).” Ketika (besi) itu sudah menjadi (merah seperti) api, dia pun berkata, “Berilah aku tembaga (yang mendidih) agar kutuangkan ke atasnya (besi panas itu).” (QS. Al-Kahfi [18]:96)

Zulkarnain diminta oleh sekelompok masyarakat untuk membangun tembok besi yang dilapisi api dan tembaga untuk melindungi mereka dari serangan Ya'juj dan Majuj yang merusak.

2.2. Tinjauan Pustaka

Dalam penulisan skripsi ini, peneliti menggali informasi dari beberapa penelitian sebelumnya sebagai referensi dan bahan perbandingan dengan menggunakan pendekatan studi literatur. Beberapa jurnal yang menjadi referensi dan bahan perbandingan penulis di antaranya sebagai berikut:

Tabel 1 - Studi Literatur

1.	Judul Penelitian	Perancangan Sistem Informasi Disposisi Surat Berbasis Web pada Kantor Badan Narkotika Nasional Kabupaten Deli Serdang
	Metode Penelitian	a. Metode kualitatif dengan observasi dan wawancara. b. Metode pengembangan <i>Waterfall</i> .
	Tujuan Penelitian	➤ Untuk meningkatkan efisiensi dan efektivitas dalam mengelola surat masuk dan disposisi surat. ➤ Untuk membuat perancangan sistem informasi disposisi surat berbasis web pada Kantor Badan Narkotika Nasional (BNN) Kabupaten Deli Serdang.
	Data Penelitian	a. <i>Flowchart</i> admin <i>input</i> surat masuk b. <i>Flowchart</i> user

		c. Rancangan UI • Halaman <i>login</i> • Halaman <i>dashboard</i> admin • Halaman surat masuk • Halaman disposisi • Halaman sifat surat • Halaman <i>user</i> • Halaman <i>dashboard user</i>
--	--	--

		• Halaman surat masuk <i>user</i> • Halaman disposisi masuk
	Kesimpulan	✓ Perancangan dan implementasi Sistem Informasi Disposisi Surat Berbasis Web pada Kantor Badan Narkotika Nasional (BNN) Kabupaten Deli Serdang dapat menjadi solusi efektif dalam mengatasi kendala-kendala yang muncul selama proses pengelolaan surat disposisi secara manual. ✓ Implementasi teknologi informasi dalam proses persuratan diharapkan dapat mengoptimalkan penggunaan sumber daya.
2.	Judul Penelitian	Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris dalam Meningkatkan Keamanan Sistem Informasi
	Metode Penelitian	Pendekatan yang digunakan adalah studi pustaka.
	Tujuan Penelitian	➤ Untuk melakukan analisis perbandingan antara algoritma kriptografi simetris dan asimetris dalam upaya meningkatkan keamanan sistem informasi.
	Data Penelitian	a. Algoritma yang digunakan pada jenis kriptografi simetris adalah RC-5, sedangkan pada jenis kriptografi asimetris tidak disebutkan dengan jelas. b. Pada jenis simetris, data yang digunakan adalah 3 (tiga) berkas *.txt yang berbeda ukuran. Sedangkan pada jenis asimetris menggunakan 3 (tiga) berkas *.txt, 2 (dua) berkas *.jpg, dan 5 (lima) berkas *.doc yang saling berbeda ukuran.
	Kesimpulan	✓ Metode simetris memiliki kecepatan dan efisiensi yang tinggi. Sedangkan, metode asimetris biasanya lebih lambat karena memerlukan sumber daya komputasi yang besar.

		✓ Metode simetris memiliki risiko keamanan jika kunci rahasia jatuh ke tangan yang salah. Sedangkan metode asimetris dikenal dengan tingkat keamanannya yang lebih tinggi karena melibatkan kunci publik dan kunci pribadi yang berbeda. ✓ Metode simetris memiliki kendala dalam hal skalabilitas jika banyak pihak perlu berkomunikasi dengan kunci simetris yang berbeda. Sedangkan metode asimetris lebih skalabel dalam hal berbagi kunci publik dengan banyak pihak. ✓ Metode simetris sering digunakan dalam skenario di mana kecepatan dan efisiensi menjadi faktor utama. Sedangkan metode asimetris umumnya digunakan dalam skenario di mana keamanan menjadi faktor yang sangat penting. ✓ Disarankan untuk memperdalam integrasi metode kriptografi hibrid. Tantangan utamanya adalah menjaga waktu komputasi yang efisien sambil menjaga tingkat keamanan yang tinggi.
3.	Judul Penelitian	Penerapan Algoritma AES (<i>Advanced Encryption Standart</i>) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi
	Metode Penelitian	a. Studi literatur b. Analisa data c. Perancangan dan pembuatan sistem d. Uji coba sistem
	Tujuan Penelitian	➤ Untuk merancang suatu aplikasi yang dapat mengamankan data agar tidak dapat digunakan oleh orang lain yang tidak memiliki izin.

	Data Penelitian	a. Algoritma yang digunakan adalah AES (<i>Advanced Encryption Standard</i>). b. Data yang digunakan adalah 20 (dua puluh) <i>file</i> dengan ukuran di bawah 2 MB.
	Kesimpulan	✓ Dilakukan pengujian enkripsi dan dekripsi terhadap 20 (dua puluh) <i>file</i> dengan ukuran di bawah 2 MB. ✓ Persentase kenaikan ukuran <i>file</i> sekitar 0,038% sampai dengan 2,086%. ✓ Rata-rata waktu proses enkripsi yaitu 12,769 ms dan rata-rata waktu proses dekripsi yaitu 18,075 ms. ✓ Disarankan menggunakan dua algoritma pada proses enkripsi dan dekripsi, misalnya dengan menggunakan dua algoritma simetris atau kombinasi antara algoritma asimetris dan simetris.
4.	Judul Penelitian	Analisis Performa dari Algoritma Kriptografi RSA dan ElGamal dalam Enkripsi dan Dekripsi Pesan
	Metode Penelitian	Dilakukan uji coba performa antara algoritma RSA dan ElGamal dalam melakukan proses enkripsi dan dekripsi.
	Tujuan Penelitian	➤ Untuk menganalisis performa dari kedua algoritma kriptografi RSA dan ElGamal.
	Data Penelitian	a. Algoritma yang digunakan adalah RSA (<i>Rivest-Shamir-Adleman</i>) dan ElGamal. b. Data yang digunakan adalah sebuah teks “Uvuvwevwevwe Onyetemevwe Ngubwemubwem Osas” dengan panjang 42 (empat puluh dua) karakter.
	Kesimpulan	✓ Algoritma RSA mempunyai <i>CPU time</i> dengan total 4,96 ms, sedangkan ElGamal mempunyai <i>CPU time</i> dengan total 7,29 ms, menunjukkan algoritma RSA lebih cepat daripada ElGamal.

		✓ Hasil kalkulasi <i>peak memory</i> , algoritma RSA dan ElGamal memiliki hasil yang sama dan mendapatkan <i>peak memory</i> sebesar 184,16 MiB.
5.	Judul Penelitian	Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA
	Metode Penelitian	a. Studi literatur b. Desain percobaan c. Pemodelan sistem d. Perancangan aplikasi e. Data uji coba
	Tujuan Penelitian	➤ Untuk melakukan perancangan dan implementasi enkripsi data menggunakan algoritma RSA dan algoritma AES.
	Data Penelitian	a. Algoritma yang digunakan adalah AES (<i>Advanced Encryption Standard</i>) dan RSA (<i>Rivest-Shamir-Adleman</i>). b. Data yang digunakan adalah teks “Bukan Pesan Rahasia” (19 karakter), “ini pesan rahasia” (17 karakter), “adityahermawan.my.id” (20 karakter), “Okeaditya988” (12 karakter), “Universitas Teknologi Yogyakarta” (32 karakter).
	Kesimpulan	✓ Pembangkitan kunci RSA yang ideal digunakan yaitu 2048 bit dengan waktu pembuatan sekitar 495,56 ms. ✓ Proses enkripsi menggunakan RSA membutuhkan waktu rata-rata 7,428 ms dan proses enkripsi menggunakan AES membutuhkan waktu rata-rata 4,365 ms. ✓ Proses dekripsi menggunakan RSA membutuhkan waktu rata-rata 54,068 ms dan proses dekripsi

		menggunakan AES membutuhkan waktu rata-rata 2,753 ms. ✓ Disarankan meningkatkan keamanan dengan menerapkan metode kombinasi yang lebih kompleks dari AES dan RSA.
6.	Judul Penelitian	Pengamanan <i>Portable Document Format</i> (PDF) Menggunakan Algoritma Kriptografi Eliptik
	Metode Penelitian	Metode penelitian tidak disebutkan dengan jelas.
	Tujuan Penelitian	➤ Untuk menerapkan pengamanan PDF menggunakan algoritma ECC untuk mengamankan dokumen dari orang-orang yang tidak berwenang.
	Data Penelitian	a. Algoritma yang digunakan adalah ECC (<i>Elliptic Curve Cryptography</i>). b. Data yang digunakan terdiri dari 4 jenis ukuran <i>file</i> PDF (<i>Portable Document Format</i>) yaitu 1 KB - 2 MB, 2 MB - 4 MB, 4 MB - 6 MB dan lebih dari 6MB. Masing-masing ukuran <i>file</i> tersebut memiliki 3 <i>file</i>, yang mana masing-masing <i>file</i> tersebut diuji sebanyak 3 kali percobaan.
	Kesimpulan	✓ Algoritma ECC menggunakan panjang kunci yang lebih pendek namun memiliki tingkat keamanan yang sama jika dibandingkan dengan algoritma RSA. ✓ Penerapan algoritma ECC dalam melakukan pengamanan terhadap <i>file</i> PDF dapat dilakukan dengan baik yaitu dengan nilai korelasi yang dominan terhadap kelas yang sangat rendah yaitu (0,00-0,199) dengan persentase $\pm 53,33\%$ dari 360 percobaan. ✓ Dibutuhkan sebuah teknik baru, sehingga tidak semua parameter penggunaan ECC ini harus diingat.

	✓ Dibutuhkan sebuah algoritma yang mampu memilih dengan pasti parameter-parameter yang akan menghasilkan korelasi yang selalu mendekati 0. ✓ Disarankan dapat mengamankan <i>file</i> Microsoft Office, Word, Excel, dan jenis dokumen elektronik lainnya.
--	---

Penelitian dengan judul “Perancangan Sistem Informasi Disposisi Surat Berbasis Web pada Kantor Badan Narkotika Nasional Kabupaten Deli Serdang” oleh (Alda & Nasution, 2023) menjelaskan mengenai fungsi disposisi surat dan perancangan sistem informasi disposisi surat. Disposisi memiliki beberapa fungsi, yaitu 1.) Mempertegas arahan yang harus dilakukan seseorang; 2.) Mengatur alur kerja suatu instansi atau organisasi; 3.) Meningkatkan efektivitas dan efisiensi dalam pelaksanaan tugas; 4.) Menjaga kerahasiaan informasi yang terkandung dalam surat. Penelitian ini bertujuan untuk meningkatkan efisiensi dan efektivitas dalam mengelola surat masuk dan disposisi surat. Penulis menggunakan penelitian ini untuk memberikan informasi dan wawasan kepada penulis mengenai perancangan sistem informasi yang akan dibangun.

Penelitian dengan judul “Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris dalam Meningkatkan Keamanan Sistem Informasi” oleh (Arif & Nurokhman, 2022) menjelaskan mengenai perbandingan metode kriptografi simetris dan asimetris. Algoritma yang digunakan pada penelitian ini yaitu algoritma RC-5 untuk metode kriptografi simetris, sedangkan untuk metode asimetris tidak dijelaskan secara langsung terkait algoritma yang digunakan. Penelitian ini bertujuan untuk melakukan analisis perbandingan antara algoritma kriptografi simetris dan asimetris dalam upaya meningkatkan keamanan sistem informasi. Data yang digunakan dalam penelitian ini ialah 10 berkas *.txt untuk pengujian metode simetris, sedangkan untuk metode asimetris menggunakan 3 berkas *.txt, 2 berkas *.jpg, dan 5 berkas *.doc yang saling berbeda ukurannya. Penelitian ini menyarankan untuk memperdalam integrasi metode kriptografi hibrid, berdasarkan hasil penelitian sebagai berikut:

- a. Metode simetris memiliki kecepatan dan efisiensi yang tinggi. Sedangkan, metode asimetris biasanya lebih lambat karena memerlukan sumber daya komputasi yang besar.
- b. Metode simetris memiliki risiko keamanan jika kunci rahasia jatuh ke tangan yang salah. Sedangkan metode asimetris dikenal dengan tingkat keamanannya yang lebih tinggi karena melibatkan kunci publik dan kunci pribadi yang berbeda.
- c. Metode simetris memiliki kendala dalam hal skalabilitas jika banyak pihak perlu berkomunikasi dengan kunci simetris yang berbeda. Sedangkan metode asimetris lebih skalabel dalam hal berbagi kunci publik dengan banyak pihak.
- d. Metode simetris sering digunakan dalam skenario di mana kecepatan dan efisiensi menjadi faktor utama. Sedangkan metode asimetris umumnya digunakan dalam skenario di mana keamanan menjadi faktor yang sangat penting.

Penelitian selanjutnya dengan judul “Penerapan Algoritma AES (*Advanced Encryption Standard*) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi” oleh (Ignasius & Sakti, 2022) menjelaskan mengenai penerapan algoritma AES (*Advanced Encryption Standard*) 128 untuk mengenkripsi dokumen. Tujuan dari penelitian ini ialah untuk merancang suatu aplikasi yang dapat mengamankan data agar tidak dapat digunakan oleh orang lain yang tidak memiliki izin. Dari penelitian ini juga penulis mendapatkan informasi mengenai algoritma AES. Berdasarkan hasil uji coba pada 20 *file* dengan ukuran di bawah 2 MB, persentase kenaikan ukuran *file* sekitar 0,038% sampai dengan 2,086%. Waktu yang dibutuhkan untuk mengenkripsi dokumen menggunakan algoritma AES yakni sekitar 12,769 ms, sedangkan untuk mendekripsi dokumen membutuhkan waktu sekitar 18,075 ms. Penelitian ini menyarankan untuk menggunakan dua algoritma pada proses enkripsi dan dekripsi, misalnya dengan menggunakan dua algoritma simetris atau kombinasi antara algoritma asimetris dan simetris.

Penelitian berikutnya dengan judul “Analisis Performa dari Algoritma Kriptografi RSA dan ElGamal dalam Enkripsi dan Dekripsi Pesan” oleh (Fajrin, Benedict, & Kusuma, 2023) menjelaskan mengenai analisis performa dari dua algoritma asimetris yaitu RSA dan ElGamal. Penelitian ini bertujuan untuk menganalisis performa dari kedua algoritma kriptografi RSA dan ElGamal sehingga dilakukan uji coba performa antara algoritma RSA dan ElGamal dalam melakukan proses enkripsi dan dekripsi. Data yang digunakan pada penelitian ini berupa pesan dengan teks “Uvuvwevwevwe Onyetemevwe Ngubwemubwem Osas”. Hasil dari penelitian ini yaitu:

- a. Algoritma RSA mempunyai *CPU time* dengan total 4,96 ms, sedangkan ElGamal mempunyai *CPU time* dengan total 7,29 ms, menunjukkan algoritma RSA lebih cepat daripada ElGamal.
- b. Hasil kalkulasi *peak memory*, algoritma RSA dan ElGamal memiliki hasil yang sama dan mendapatkan *peak memory* sebesar 184,16 MiB.

Selanjutnya adalah penelitian dengan judul “Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA” oleh (Hermawan & Ujjianto, 2021) menjelaskan penelitian mengenai implementasi enkripsi dengan menggunakan kombinasi algoritma AES dan RSA. Tujuan dari penelitian ini ialah untuk melakukan perancangan dan implementasi enkripsi data menggunakan algoritma AES dan RSA serta mengetahui kecepatan kedua algoritma yang digunakan dalam proses enkripsi maupun dekripsi. Penulis mendapatkan informasi dari hasil penelitian ini yaitu sebagai berikut:

- a. Pembangkitan kunci RSA yang ideal digunakan yaitu 2048 bit dengan waktu pembuatan sekitar 495,56 ms.
- b. Proses enkripsi menggunakan RSA membutuhkan waktu rata-rata 7,428 ms dan proses enkripsi menggunakan AES membutuhkan waktu rata-rata 4,365 ms.
- c. Proses dekripsi menggunakan RSA membutuhkan waktu rata-rata 54,068 ms dan proses dekripsi menggunakan AES membutuhkan waktu rata-rata 2,753 ms.

Penelitian terakhir berjudul “Pengamanan *Portable Document Format* (PDF) Menggunakan Algoritma Kriptografi Eliptik” oleh (Taopan, Boru, & Fanggidae, 2022) menjelaskan implementasi algoritma ECC (*Elliptic Curve Cryptography*). Tujuan dari penelitian ini adalah untuk menerapkan pengamanan PDF menggunakan algoritma ECC untuk mengamankan dokumen dari orang-orang yang tidak berwenang. Berdasarkan penelitian ini, pengujian dilakukan terhadap sejumlah *file*. Terdapat 4 jenis ukuran *file* PDF yang dienkripsi, yaitu 1KB-2MB, 2MB-4MB, 4MB-6MB dan lebih dari 6MB. Masing-masing ukuran *file* tersebut memiliki 3 *file*, yang mana masing-masing *file* tersebut diuji sebanyak 3 kali percobaan. Sehingga terdapat 360 percobaan. Hasil yang diperoleh dari penelitian ini adalah sebagai berikut:

- a. Algoritma ECC menggunakan panjang kunci yang lebih pendek namun memiliki tingkat keamanan yang sama jika dibandingkan dengan algoritma RSA.
- b. Penerapan algoritma ECC dalam melakukan pengamanan terhadap *file* PDF dapat dilakukan dengan baik yaitu dengan nilai korelasi yang dominan terhadap kelas yang sangat rendah yaitu (0,00-0,199) dengan persentase $\pm 53,33\%$ dari 360 percobaan, artinya bahwa hasil enkripsi *file* memiliki tingkat kemiripan yang rendah (dalam artian baik) jika dibandingkan dengan *file* yang belum dienkripsi.

Berdasarkan studi literatur yang telah diteliti dari sumber-sumber di atas dan juga sumber-sumber yang tidak dapat disebutkan semuanya, penulis memutuskan untuk membuat sistem aplikasi berbasis web yang mudah diakses oleh perangkat teknologi (*smartphone* maupun *desktop*) selama perangkat tersebut memiliki akses internet. Selain itu, penulis mengambil algoritma enkripsi ECC (*Elliptic Curve Cryptography*) sebagai algoritma keamanan data yang memanfaatkan kunci publik dan kunci privat terhadap dokumen-dokumen surat yang akan digunakan melalui aplikasi ini.

2.3. Dasar Teori

2.3.1. Kriptografi

Kriptografi berasal dari kata Yunani “*kryptos*” yang berarti “tersembunyi” dan “*graphene*” yang berarti “tulisan”. Kriptografi adalah ilmu yang mempelajari teknik-teknik perlindungan informasi, termasuk menjaga kerahasiaan data, integritas data, dan validitas data. Enkripsi tidak hanya menyembunyikan pesan, tetapi juga memastikan bahwa pesan sampai ke penerima secara utuh dan benar dari sumber yang sah (otentikasi) dan integritas pesan terjamin (integritas data juga ditujukan).

Qadafi (2019) dalam jurnal prosidingnya menyampaikan bahwa 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. Enkripsi dimaksudkan untuk melindungi informasi sensitif, integritas data, autentikasi, dan non-penyangkalan yang dikirimkan melalui jaringan internet agar tidak dilihat atau digunakan oleh orang lain atau pihak yang tidak berwenang.

Teknik kriptografi memiliki beberapa tujuan utama dalam mengamankan data informasi di antaranya:

a. Kerahasiaan

Tujuan enkripsi adalah untuk memastikan bahwa hanya pihak tertentu yang berwenang yang dapat mengakses informasi melalui pesan email, dan proses enkripsi hanya dapat dibaca oleh penerima yang memiliki kunci dekripsi.

b. Integritas Data

Enkripsi memastikan bahwa informasi tidak diubah atau dimanipulasi selama proses pengiriman atau disimpan di tujuan. Enkripsi ini memastikan bahwa data sampai ke penerima dalam keadaan benar yang sama, tidak diubah.

c. Autentikasi

Kriptografi berfungsi untuk menjamin autentikasi sumber informasi. Kriptografi khususnya sertifikat digital, berperan penting dalam menjamin keaslian sumber informasi. Sertifikat digital adalah dokumen elektronik yang menghubungkan identitas pemilik kunci publik dengan otoritas sertifikasi (CA atau *Certification Authority*) terpercaya. Otoritas sertifikat bertanggung jawab untuk memverifikasi identitas pemilik kunci publik sebelum menerbitkan sertifikat digital. Informasi dalam sertifikat digital seperti nama, alamat email, dan tanggal kedaluwarsa sertifikat dapat digunakan untuk memverifikasi identitas pengirim pesan atau dokumen elektronik.

d. *Non-Rejection*

Tujuan keempat adalah *non-rejection*, atau biasa disebut dengan *anti-rejection*. Ini adalah tindakan yang diperlukan untuk mencegah pengirim menolak memberikan informasi. Enkripsi mencegah informasi dikirim atau ditandatangani oleh pihak yang tidak berwenang. Tanda tangan digital juga dapat digunakan untuk memastikan tidak ada penolakan bahwa pesan dikirim oleh pihak yang ditentukan.

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).

Secara umum, kriptografi dibagi menjadi dua jenis: kriptografi simetris dan kriptografi asimetris. Kriptografi simetris menggunakan kunci privat yang sama untuk melakukan proses enkripsi (*encrypting*) dan dekripsi (*decrypting*) pesan. Contohnya adalah algoritma *Data Encryption Standard* (DES) atau *Advanced Encryption Standard* (AES) yang banyak digunakan.

Jenis kriptografi yang kedua adalah kriptografi asimetris. Kriptografi asimetris menggunakan dua kunci berbeda yaitu kunci publik untuk melakukan enkripsi dan kunci privat untuk melakukan dekripsi. Kunci publik dapat dibagikan secara bebas, namun kunci privat tetap dirahasiakan. Hanya kunci privat terkait yang dapat digunakan untuk mendekode pesan yang dienkripsi dengan kunci publik. Enkripsi asimetris umumnya mengacu pada sistem yang menggunakan algoritma enkripsi modern. Enkripsi asimetris dianggap lebih aman dibandingkan enkripsi simetris karena tidak memerlukan kunci privat untuk didistribusikan dengan aman. Contoh algoritma kriptografi asimetris yang terkenal adalah algoritma *Rivest-Shamir-Adleman* (RSA). Kelebihan kriptografi asimetris adalah menggunakan algoritma matematika dan komputer serta lebih modern, sehingga informasi tidak mudah diuraikan.

Ada satu lagi jenis kriptografi yang lebih modern yaitu kriptografi hibrid. Kriptografi hibrid memanfaatkan sifat unik kriptografi kunci publik untuk bertukar informasi sensitif melalui saluran yang tidak terpercaya dengan efisiensi kriptografi simetris. Enkripsi ini menciptakan solusi perlindungan data *end-to-end* yang praktis. Enkripsi hibrid umumnya digunakan dalam protokol transfer data web seperti *Transport Layer Security* (TLS). Saat terhubung ke situs web yang menggunakan HTTPS (HTTP aman menggunakan TLS), browser menegosiasikan algoritma enkripsi yang melindungi koneksi penggunaannya. Algoritma ini mencakup pertukaran kunci, enkripsi simetris, dan algoritma tanda tangan digital.

2.3.2. Algoritma ECC

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).

2.3.3. Administrasi Surat

Administrasi merupakan proses pencatatan atau pengumpulan data dan laporan yang berkaitan dengan surat-menyurat dan kearsipan sehingga dapat memberikan kontribusi dalam penyelesaian permasalahan dalam pengelolaan, pelaksanaan, pengarahan atau pengorganisasian seluruh kegiatan untuk mencapai tujuan (Akion, 2024).

2.3.4. Disposisi Surat

Disposisi surat adalah tata cara atau prosedur pengelolaan surat yang dibuat dan disetujui oleh pimpinan suatu perusahaan atau instansi yang berhak dalam mengurus segala persetujuan surat-menyurat pada perusahaan atau instansi yang dipimpinnya. Prosedur ini diketahui oleh pimpinan perusahaan dan harus dilaksanakan dengan sebaik-baiknya agar surat-surat dikelola sesuai dengan konsep surat pada perusahaan atau instansi tersebut (Herpendi, Fathurrahmani, & Hafidz, 2022).

2.3.5. Sistem Informasi

Sistem dapat didefinisikan dengan pendekatan prosedural dan pendekatan komponen. Dengan pendekatan prosedural, sistem dapat didefinisikan sebagai kumpulan prosedur dengan tujuan tertentu (Oktaviani, Rodianto, Noviana, & Nawassyarif, 2020).

2.3.6. Website

Website atau situs dapat diartikan sebagai kumpulan halaman yang menampilkan data teks, data gambar diam atau bergerak, data animasi, suara, video dan segala kombinasi baik yang bersifat statis maupun dinamis yang masing-masing terhubung membentuk suatu rangkaian bangunan yang saling berhubungan (Oktaviani, Rodianto, Noviana, & Nawassyarif, 2020).

2.3.7. *Black Box*

Pengujian sistem adalah proses menjalankan sistem perangkat lunak untuk menentukan apakah sistem memenuhi spesifikasi sistem dan beroperasi di lingkungan yang dimaksudkan. Pengujian sering kali melibatkan penemuan *bug*, cacat program, dan kesalahan dalam program yang menyebabkan kesalahan saat sistem perangkat lunak dijalankan. Pengujian meliputi pengujian setiap proses dan kesalahan apa saja yang mungkin terjadi pada setiap proses.

Pengujian sistem yang digunakan dalam penelitian ini adalah teknik pengujian *black box* atau biasa disebut pengujian struktural, yang memerlukan pengetahuan teknis terperinci tentang sistem. Pengujian *black box* merupakan suatu metode pengujian perangkat lunak dan berbagai aplikasi untuk melihat apakah berfungsi dengan benar dan optimal. Pengujian *black box* mengevaluasi fungsionalitas suatu aplikasi tanpa mengetahui struktur internal atau detail implementasinya.

Penguji berinteraksi dengan aplikasi hanya melalui antarmuka pengguna, dengan fokus pada masukan, keluaran, dan perilaku yang diharapkan. Pengujian *black box* membantu memvalidasi aplikasi terhadap persyaratan pengguna dan memastikan bahwa semua fungsi berfungsi sesuai harapan.

Penulis mengambil contoh pengujian dengan teknik *black box* yang berasal dari jurnal berjudul “Rancang Bangun Aplikasi Disposisi Persuratan Berbasis Mobile Apps” (Yusuf, Muin, & Nisrawati, Rancang Bangun Aplikasi Disposisi Persuratan Berbasis Mobile Apps, 2022). Dalam jurnal ini, pengujian dilakukan dengan membuat tabel skenario kasus dengan data masukan, hasil yang diharapkan, dan hasil pengujian.

Kasus dan Hasil Uji Coba		
Data Masukan	Yang Diharapkan	Status
Username dan Password salah	Menampilkan informasi	[√] Sukses
	Username atau Password Salah	[] Gagal
Username dan Password benar	Menampilkan halaman sesuai	[√] Sukses
	dengan user yang login	[] Gagal

Gambar 3 - Contoh Pengujian Black Box

2.4. Tools Perancangan, Pengembangan Sistem, dan Bahasa Pemrograman

2.4.1. Perancangan Sistem

2.4.1.1. Microsoft Visio



Gambar 4 - Logo Microsoft Visio

Microsoft Office Visio atau biasa disebut dengan Microsoft Visio, merupakan sebuah perangkat lunak komputer yang biasa digunakan untuk membuat diagram, diagram alur, *brainstorming*, dan skema jaringan. Selain Word, Excel dan PowerPoint, Microsoft Office juga menyertakan Microsoft Visio. Perangkat lunak ini menggunakan grafik vektor untuk membuat diagram (Bintara, 2023).

Microsoft Visio pertama kali diperkenalkan pada tahun 1992 dan dikembangkan oleh Visio Corporation. Namun pada tahun 2000, perangkat lunak ini diakuisisi oleh Microsoft. Setelah itu, Microsoft Visio dapat dibedakan menjadi tiga edisi, yaitu *Standart*, *Professional*, dan *Online* yang masing-masing memiliki fitur, kapabilitas, serta harga yang berbeda-beda.

Berikut beberapa fungsi serta manfaat yang pengguna dapatkan dari Microsoft Visio, di antaranya sebagai berikut:

1) Membuat diagram profesional

Banyaknya fitur yang disediakan Microsoft Visio memungkinkan pengguna dapat membuat diagram dengan cepat, efisien, dan profesional. Terlebih didukung dengan beragam *template* menarik untuk semua jenis diagram yang diinginkan.

2) Mudahnya menampilkan informasi terperinci

Pengguna juga dapat mendokumentasikan alur kerja atau proses dengan mudah. Dalam hal ini, dapat meningkatkan kejelasan informasi dan mengidentifikasi peluang penyempurnaan. Atau bahkan dengan pemetaan diagram, pengguna dapat memecahkan masalah dan membuat keputusan yang tepat.

3) Meningkatkan kinerja

Yang terakhir dapat meningkatkan kinerja pengguna karena pengguna dapat dengan mudah menyelesaikan diagram hanya dengan beberapa klik saja. Selain itu, terdapat fitur kolaborasi yang memungkinkan pengguna dapat menggabungkan ide dan wawasan ke dalam satu lembar kerja yang sama. Dalam hal ini tentunya akan dapat mempercepat pekerjaan serta meningkatkan kinerja. Artinya pengguna dapat

memanfaatkan waktu kerja secara efisien dan tidak membuang waktu secara percuma.

Microsoft Visio menghadirkan berbagai fitur-fitur yang menarik. Terlebih pengguna akan diberikan kemudahan dalam membuat berbagai jenis diagram secara profesional. Berikut beberapa fitur yang terdapat dalam Microsoft Visio, yaitu:

- ❖ *Auto Connect*. Fitur ini memungkinkan pengguna untuk menghubungkan *shape* baru dengan *shape* yang ada pada halaman gambar secara otomatis.
- ❖ *Data Graphic*. Fitur yang dapat memvisualisasikan data yang terdapat di dalam *shape* tertentu.
- ❖ *Data Link*. Berfungsi untuk memudahkan dalam menghubungkan diagram dengan sumber data, sumber data dengan *shape data*, serta mengatur hubungan tersebut.
- ❖ *Themes*. Mengubah tampilan diagram supaya lebih menarik untuk dilihat.
- ❖ *Visualizer Data*. Ubah data peta proses Microsoft Excel menjadi Diagram Visio.

2.4.1.2. StarUML



Gambar 5 - Logo StarUML

StarUML merupakan perangkat lunak pemodelan yang mendukung UML (*Unified Modeling Language*). StarUML didasarkan pada UML versi 1.4 dan menyediakan notasi-notasi UML versi 2.0 serta 11 (sebelas) tipe diagram berbeda. StarUML sangat mudah beradaptasi terhadap lingkungan pengguna dan memiliki ekstensibilitas yang tinggi dalam hal fungsionalitasnya. StarUML tergolong perangkat lunak pemodelan yang masih baru karena dirilis pada tahun 2005. Berbagai fitur baru telah ditambahkan untuk memperluas fungsionalitas perangkat lunak ini (Mubarok, Purnomo, & Noor, 2019).

UML (*Unified Modeling Language*) adalah bahasa pemodelan visual yang digunakan untuk merancang dan memodelkan sistem perangkat lunak. UML mencakup notasi grafis yang digunakan untuk mewakili berbagai aspek dari sistem, seperti struktur sistem, perilaku sistem, interaksi antar objek, dan lingkungan di mana sistem beroperasi. UML terdiri dari berbagai diagram yang masing-masing mewakili aspek tertentu dari sistem. Beberapa diagram *Unified Modeling Language* yang paling umum digunakan meliputi *class diagram*, *activity diagram*, dan lain-lain (Faulina, 2023).

Diagram UML adalah notasi grafis yang digunakan dalam *Unified Modeling Language* untuk merepresentasikan aspek tertentu dari sistem perangkat lunak. Berikut adalah beberapa jenis diagram UML yang umum digunakan di antaranya:

a. *Use Case Diagram*

Use case diagram digunakan untuk mewakili kasus penggunaan suatu sistem, termasuk kebutuhan dan persyaratan pengguna. Diagram ini menunjukkan bagaimana pengguna menggunakan sistem dalam situasi tertentu. *Use case diagram* membantu para pengembang untuk memahami kebutuhan dan persyaratan pengguna serta memastikan bahwa sistem memenuhi kebutuhan tersebut (Faulina, 2023).

Sehingga *use case diagram* dapat dikatakan sebagai suatu metode yang merepresentasikan hubungan antara pengguna suatu sistem dengan sistem itu sendiri yang hasilnya berupa skema sederhana untuk memudahkan pengguna dalam membaca dan memahami informasi yang diberikan. *Use case diagram* terbentuk dari skenario yang berkaitan dengan kegunaan sistem yang diilustrasikan dengan sebuah *use case*. Setiap skenario menggambarkan serangkaian aktivitas yang dapat dimulai oleh pengguna sistem yang disebut *actor*.

Fungsi dari *use case diagram* yaitu:

- Berguna memperlihatkan proses aktivitas secara urut dalam sistem.
- Mampu menggambarkan proses bisnis, bahkan menampilkan urutan aktivitas pada sebuah proses.
- Sebagai *bridge* atau jembatan antara pembuat dengan konsumen untuk mendeskripsikan sebuah sistem.

Manfaat dari *use case diagram* di antaranya:

- Menggunakannya sebagai kebutuhan verifikasi.
- Menjadi gambaran *interface* dari sebuah sistem karena setiap sistem yang dibangun haruslah memiliki *interface*.
- Mengidentifikasi siapa saja orang yang dapat berinteraksi dengan sistem, serta apa yang dapat dilakukan oleh sistem.
- Memberikan kepastian mengenai kebutuhan sistem, sehingga tidak membingungkan.
- Memudahkan proses komunikasi antara domain *expert* dan *end user*.

Komponen yang ada pada *use case diagram* yaitu sebagai berikut:

1) *System*

Sebuah sistem digambarkan ke dalam bentuk persegi. Fungsinya untuk membatasi *use case* dengan interaksi dari luar sistem. Sistem pada umumnya diberikan label yang sesuai.

Namun, umumnya sistem ini tidaklah diberi gambar karena tidak terlalu memberikan makna pada sebuah diagram.

2) *Actor*

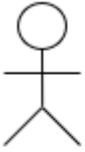
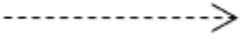
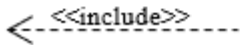
Fungsi *Actor* menjelaskan siapa yang berinteraksi dengan sistem. *Actor* akan memberikan informasi kepada sistem, serta menerima informasi dari sistem. *Actor* tidak memberikan kontrol terhadap sistem, namun hanya memberikan gambaran mengenai hubungannya dengan sistem.

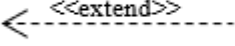
3) *Use Case*

Use case adalah komponen gambaran fungsional dalam sebuah sistem. Sehingga konsumen maupun pembuat saling mengenal dan mengerti mengenai alur sistem yang akan dibuat.

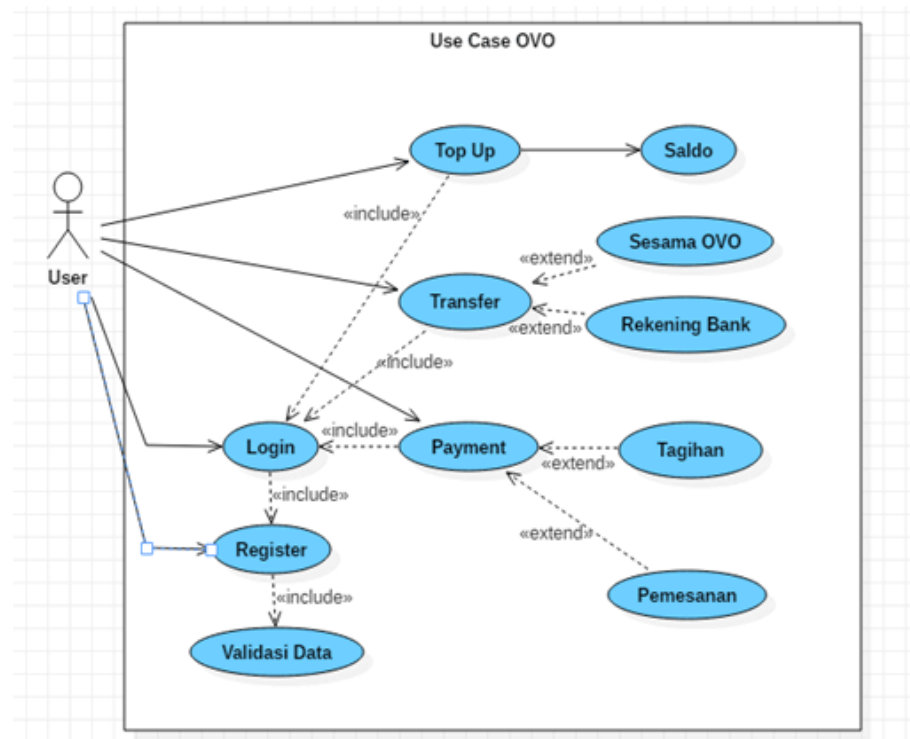
Simbol-simbol yang dapat digunakan pada *use case diagram* di antaranya sebagai berikut:

Tabel 2 - Simbol Use Case Diagram

Simbol	Keterangan
	<i>Actor</i> , mewakili peran orang, sistem yang lain, atau alat ketika berkomunikasi dengan <i>use case</i> .
	<i>Use case</i> , abstraksi dan interaksi antara sistem dan <i>actor</i> .
	<i>Association</i> , abstraksi dari penghubung antara <i>actor</i> dengan <i>use case</i> .
	Generalisasi, menunjukkan spesialisasi <i>actor</i> untuk dapat berpartisipasi dengan <i>use case</i> .
	Menunjukkan bahwa suatu <i>use case</i> seluruhnya merupakan fungsionalitas dari <i>use case</i> lainnya.

	Menunjukkan bahwa suatu <i>use case</i> merupakan tambahan dari <i>use case</i> lainnya jika suatu kondisi terpenuhi.
---	---

Berikut contoh dari *use case diagram* diambil dari situs Dicoding Blog (Dicoding Intern, 2021):



Gambar 6 - Contoh Use Case Diagram

OVO adalah aplikasi pintar yang memberikan kemudahan dalam bertransaksi (OVO Cash), serta berfungsi untuk mengumpulkan poin di banyak tempat (OVO Points). Gambar di atas merupakan contoh *use case diagram* pada OVO, adapun penjelasannya sebagai berikut ini:

- 1) *User*: Orang yang dapat mengakses atau menggunakan aplikasi OVO, mulai dari *login* ke aplikasi hingga melakukan aksi terhadap aplikasi seperti *top up* saldo, transfer, dan *payment*.
- 2) *Register*: Register merupakan langkah pertama yang dilakukan *user* ketika ia tidak mempunyai akses pada aplikasi OVO. Mendaftarkan data diri ke dalam aplikasi agar dikenali.

- 3) *Login*: Setelah mendapatkan akun, *user* harus melakukan *login* agar dapat mengakses berbagai fitur aplikasi OVO.
- 4) *Top Up*: Suatu kegiatan yang dilakukan *user* untuk mengisi ulang saldo OVO. Terdapat 2 pilihan alternatif untuk melakukan *top up* saldo, yaitu melalui ATM dan internet *banking*.
- 5) *Transfer*: Transfer berfungsi untuk mengirim atau membagikan saldo dalam aplikasi OVO ke pengguna lain, baik sesama OVO atau ke rekening tertentu.
- 6) *Payment*: Ketika *user* memilih menu *payment*, maka *user* dapat melakukan pembayaran lewat aplikasi.

b. *Activity Diagram*

Activity diagram digunakan untuk mewakili alur kerja dalam suatu sistem, termasuk tindakan dan keadaan yang terjadi selama proses dijalankan. Diagram ini menunjukkan aktivitas dan tindakan yang harus dilakukan sistem saat menjalankan suatu proses. *Activity diagram* membantu pengembang untuk memahami alur kerja suatu sistem dan mengidentifikasi masalah atau kesalahan dalam prosesnya (Faulina, 2023).

Activity diagram, dalam bahasa Indonesia diagram aktivitas, yaitu diagram yang dapat digunakan untuk memodelkan proses-proses yang terjadi dalam suatu sistem. Alur proses dari suatu sistem digambarkan secara vertikal. *Activity diagram* merupakan pengembangan dari *Use Case* yang memiliki alur aktivitas.

Tujuan dari *activity diagram* yaitu:

- Menjelaskan urutan aktivitas dalam suatu proses.
- Di dalam dunia bisnis biasanya digunakan untuk modeling (memperlihatkan urutan proses bisnis).
- Mudah dalam memahami proses yang ada dalam sistem secara keseluruhan.

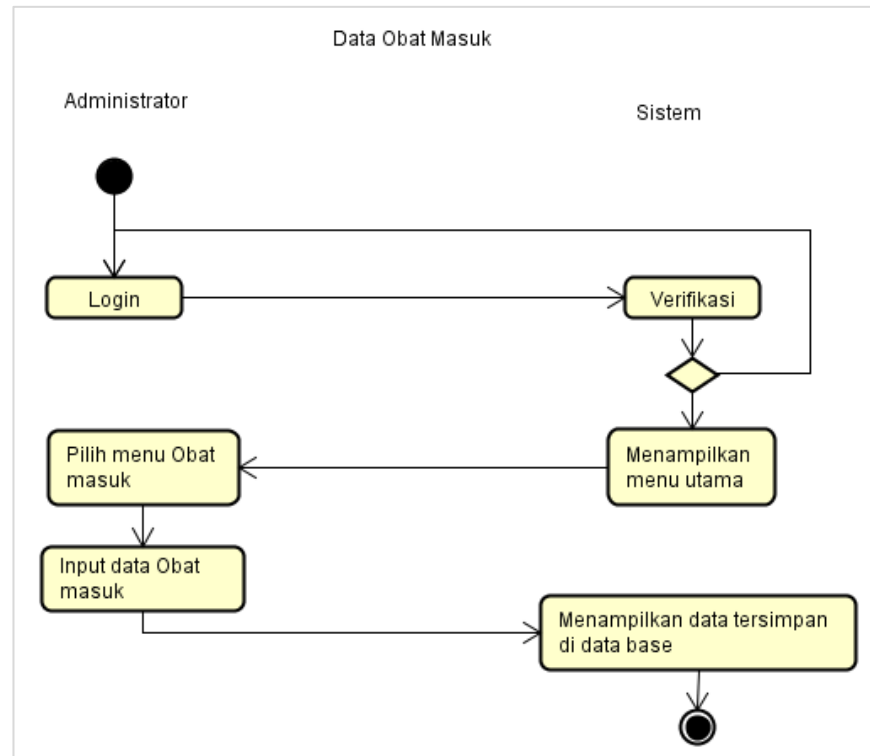
- Merupakan metode perancangan yang terstruktur, mirip dengan *Flowchart* maupun *Data Flow Diagram* (DFD).
- Mengetahui aktivitas aktor/pengguna berdasarkan *use case*/diagram yang dibuat sebelumnya.

Komponen dan simbol-simbol yang dapat digunakan pada *activity diagram*, di antaranya sebagai berikut:

Tabel 3 - Simbol Activity Diagram

Simbol	Nama	Keterangan
	Status Awal	Sebuah diagram aktivitas memiliki sebuah status awal.
	Aktivitas	Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja.
	Percabangan / <i>Decision</i>	Percabangan di mana ada pilihan aktivitas yang lebih dari satu.
	Penggabungan / <i>Join</i>	Penggabungan di mana ada lebih dari satu aktivitas lalu digabungkan menjadi satu.
	Status Akhir	Status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki sebuah status akhir.
	<i>Swimlane</i>	<i>Swimlane</i> memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang terjadi.

Berikut merupakan contoh dari *activity diagram* diambil dari situs Dicoding Blog (Dicoding Intern, 2023):



Gambar 7 - Contoh Activity Diagram

Adapun penjelasan dari contoh diagram di atas adalah:

- 1) Admin melakukan *login* ke sistem.
- 2) Sistem akan memverifikasi *username* dan *password* yang dimasukkan oleh admin. Jika kedua informasi ini benar, admin akan masuk ke menu utama. Jika *username* dan *password* yang dimasukkan salah, admin akan kembali ke halaman login.
- 3) Setelah berhasil masuk, admin memilih *input* data obat masuk.
- 4) Berikutnya, sistem akan menyimpan data ke *database* secara otomatis.

2.4.1.3. Balsamiq Wireframe

Balsamiq adalah sebuah perangkat lunak *prototyping* yang digunakan untuk membuat *wireframe* atau sketsa kasar dari antarmuka pengguna (*User Interface*) pada suatu aplikasi atau situs web. *Wireframe* adalah representasi visual sederhana dari tata letak dan elemen utama dalam suatu desain tanpa detail grafis yang mendalam. Balsamiq dirancang untuk membantu desainer, pengembang, dan pemangku kepentingan lainnya untuk dengan cepat membuat sketsa ide desain dan menguji fungsionalitas konsep sebelum mengembangkan versi final (UPT TIK, 2023).

2.4.2. Pengembangan Sistem

2.4.2.1. Visual Studio Code

VSCode merupakan singkatan dari Visual Studio Code, yaitu aplikasi *code editor* yang mendukung proses pengembangan sebuah aplikasi. *Software* ini dikembangkan oleh perusahaan teknologi raksasa terkenal Microsoft. Meskipun begitu, VSCode mendukung untuk dioperasikan pada perangkat selain Windows, seperti Linux dan Mac OS.

Code editor ini memungkinkan untuk membuat atau mengedit *source code* menggunakan berbagai bahasa pemrograman, seperti NodeJs, JavaScript, dan sebagainya. VSCode juga mendukung bahasa pemrograman lain seperti Python, Java, PHP, dan .NET. Hal ini memungkinkan sebab VSCode mempunyai ekosistem luas dengan banyak ekstensi (Santi, 2024).

2.4.2.2. XAMPP

XAMPP adalah *web server open source* yang berjalan pada sistem operasi lintas platform (Windows, Linux, Mac OS). Semua yang diperlukan untuk mengelola situs web tersedia di XAMPP seperti Apache, MySQL/MariaDB, PHP, dan Perl. Meski program di dalamnya

lengkap, XAMPP tetap menjadi web server yang sederhana dan ringan (Sari, Syahputra, Zaky, Sibuea, & Zakhir, 2022)

2.4.2.2.1. Apache Web Server

Apache adalah perangkat lunak web server gratis dan *open source* yang memungkinkan pengguna dapat mengunggah situs web ke internet. Server ini menjadi platform bagi 33% situs web di seluruh dunia dan secara resmi dikenal dengan nama Apache HTTP Server. Apache merupakan salah satu web server tertua dan terbaik, dirilis pertama kali pada tahun 1995 dan dikelola serta dikembangkan oleh Apache Software Foundation. (Uly, 2024)

2.4.2.2.2. MySQL Database

MySQL merupakan perangkat lunak RDBMS (*Relational Database Management System*) yang memungkinkan *database* dikelola dengan sangat cepat, dapat menampung data dalam jumlah yang sangat besar, dapat diakses oleh banyak pengguna (*multi-user*) dan dapat menjalankan proses secara sinkron atau bersamaan (*multi-threaded*) (Pratiwi, Wijaya, & Fajriyah, 2021).

2.4.3. Bahasa Pemrograman

2.4.3.1. PHP

PHP (*Personal Home Page*) adalah bahasa *scripting* yang dibundel dengan HTML yang berjalan di sisi server. Sebagian besar perintah PHP hanya berasal dari bahasa C, Java dan Perl dengan beberapa fungsi khusus PHP yang ditambahkan. Bahasa ini memungkinkan pengembang aplikasi web dapat dengan cepat dan mudah mengirimkan HTML yang dinamis dan interaktif yang dihasilkan server (Martani, M, & Ikhsan, 2022).

2.4.3.2. HTML

HTML merupakan bahasa yang digunakan untuk menggambarkan struktur halaman web. HTML berfungsi untuk mempublikasi dokumen *online*. Instruksi dasar dari HTML disebut *tag*. Sebuah *tag* dinyatakan dalam sebuah kurung siku (<>). *Tag* yang menargetkan dokumen atau bagian dokumen harus dibuat berpasangan. Terdiri dari *tag* pembuka dan *tag* penutup, di mana *tag* penutup menggunakan tambahan tanda garis miring (/) di awal nama *tag* (Sari, Syahputra, Zaky, Sibuea, & Zakhir, 2022).

2.4.3.3. CSS

CSS adalah bahasa untuk menampilkan halaman web seperti warna, *layout*, dan *font*. CSS memungkinkan pengembang web dapat membuat halaman web yang dapat beradaptasi dengan berbagai ukuran layar. CSS dapat dimasukkan ke dalam halaman HTML, namun biasanya dibuat terpisah dengan halaman HTML. Hal ini dimaksudkan untuk membantu menata halaman HTML dengan desain rancangan yang sama (Ramadhani, Sari, & Satria, 2023).

2.4.3.4. JavaScript

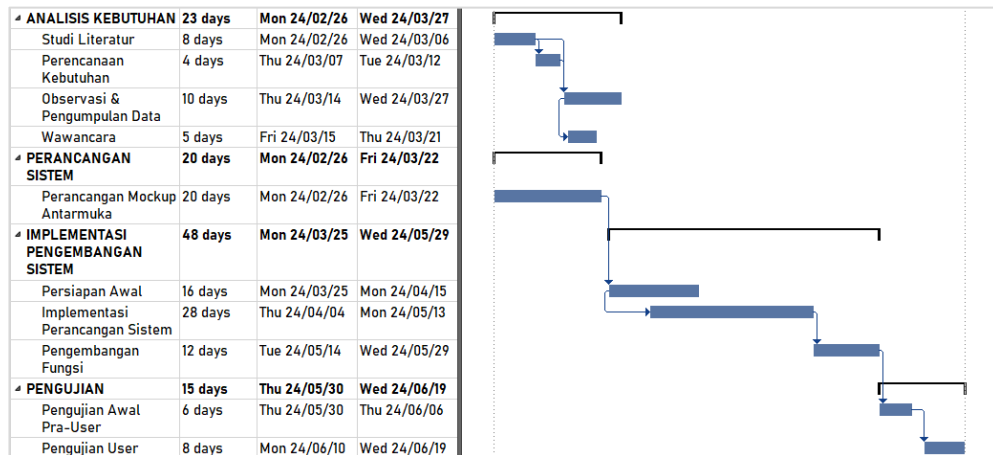
JavaScript adalah bahasa pemrograman yang dirancang untuk dijalankan pada web browser. JavaScript pertama kali dikembangkan pada web browser Netscape oleh Brenden Eich dengan nama Mocha, kemudian diubah menjadi Live-Script dan akhirnya menjadi JavaScript (Noviantoro, Silviana, Fitriani, & Permatasari, 2022).

BAB III

ANALISIS DAN PERANCANGAN SISTEM

3.1. Analisis Kebutuhan Sistem

3.1.1. Tempat dan Waktu Penelitian



Gambar 8 - Project Timeline

Penelitian dilakukan di lingkungan Universitas Nahdlatul Ulama Cirebon bagian rektorat dan biro kemahasiswaan. Penelitian dilakukan dimulai dari tanggal 26 Februari 2024.

3.1.2. Analisis Masalah

Analisis masalah adalah penguraian masalah-masalah pokok yang teridentifikasi sampai ke akar penyebabnya. Analisis masalah ini menjelaskan proses identifikasi masalah serta evaluasi mengenai sistem administrasi disposisi surat pada Universitas Nahdlatul Ulama Cirebon. Berdasarkan uraian pada latar belakang masalah pada penelitian ini terdapat permasalahan dalam melakukan disposisi surat, di antaranya sebagai berikut:

- Surat yang diajukan sering kali mengalami keterlambatan atau bahkan tidak tersampaikan.
- Posisi surat yang telah dikirim tidak bisa dilihat untuk mengetahui progres penyampaian surat disposisi.

- Dalam proses pengarsipan sering mengalami kehilangan surat yang telah diterima.
- Perlu adanya peningkatan dan pengintegrasian dengan teknologi pada sistem administrasi disposisi surat.

3.1.3. Sistem Berjalan

Proses administrasi disposisi surat pada Universitas Nahdlatul Ulama Cirebon saat ini belum menerapkan sistem dan aturan yang baku. Sistem yang saat ini digunakan merupakan tahap uji coba dikarenakan adanya pergantian kepemimpinan dan perubahan proses manajemen yang direncanakan akan lebih baik ke depannya. Menurut Neneng Euis Susanti sebagai staf rektorat, disposisi surat ini masih dalam tahap penyesuaian dan terus mengalami perbaikan dalam manajemen serta alur administrasi disposisi surat di Universitas Nahdlatul Ulama Cirebon.

3.1.4. Sistem yang Dibangun

Sistem yang akan dibangun pada penelitian ini berupa sistem informasi administrasi disposisi surat berbasis *website* dengan menggunakan bahasa pemrograman PHP versi 8 dan *framework* CodeIgniter versi 4. Fitur-fitur yang terdapat pada sistem informasi ini termasuk pengelolaan surat masuk, surat keluar, pemantauan posisi surat, dan pengarsipan surat.

3.1.5. Kebutuhan Sistem

Analisis kebutuhan untuk bisa mengimplementasikan algoritma kriptografi pada sistem administrasi disposisi surat terdiri dari Kebutuhan Fungsional dan Kebutuhan Non Fungsional. Berikut adalah uraian mengenai kebutuhan sistem administrasi disposisi surat di antaranya sebagai berikut:

a. Fungsional

Kebutuhan fungsional adalah kebutuhan yang berisi proses-proses apa saja/layanan apa saja yang nantinya harus disediakan oleh sistem, mencakup bagaimana sistem harus bereaksi pada *input* tertentu dan bagaimana perilaku sistem pada situasi tertentu. Kebutuhan fungsional

menggambarkan fungsionalitas atau layanan sistem dan bergantung pada tipe *software*, harapan pengguna dan tipe sistem di mana *software* digunakan. Secara fungsional, kebutuhan sistem untuk implementasi algoritma kriptografi pada sistem administrasi disposisi surat yaitu:

1) Sistem

Kebutuhan sistem untuk implementasi algoritma kriptografi pada sistem administrasi disposisi surat yaitu:

- a. Sistem dapat terhubung dengan jaringan internet.
- b. Sistem dapat meng-*input file* dokumen.
- c. Sistem dapat melakukan algoritma kriptografi enkripsi dan dekripsi pada teks maupun *file*.
- d. Sistem dapat menampilkan dokumen *plaintext*.
- e. Sistem dapat mengirim dan menerima pesan antar pengguna sistem.

2) Pengguna

Kebutuhan pengguna untuk menjalankan sistem administrasi disposisi surat dibagi atas beberapa kategori pengguna sebagai berikut:

a) Admin IT

- ✓ Dapat melakukan manajemen pengguna.
- ✓ Dapat melakukan manajemen kategori surat bawaan.

b) Pengguna

- ✓ Dapat melakukan manajemen kategori surat khusus.
- ✓ Dapat mengirimkan surat kepada pengguna lain.
- ✓ Dapat menanggapi surat yang telah diterima.
- ✓ Dapat melihat progres surat yang telah dikirim.
- ✓ Dapat melakukan manajemen arsip surat.

b. Non Fungsional

Kebutuhan non fungsional adalah kebutuhan yang menitikberatkan pada properti perilaku yang dimiliki oleh sistem. Kebutuhan fungsional juga sering disebut sebagai batasan layanan atau fungsi yang ditawarkan sistem seperti batasan waktu, batasan pengembangan proses, standarisasi, dan lain-lain. Secara non fungsional, kebutuhan sistem untuk implementasi algoritma kriptografi pada sistem administrasi disposisi surat yaitu:

1) Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan untuk membangun dan menjalankan sistem administrasi disposisi surat ini adalah laptop dengan spesifikasi sebagai berikut:

- ✓ Prosesor Intel Core i5
- ✓ RAM 8 GB
- ✓ ROM SSD 256 GB

2) Perangkat Lunak (*Software*)

Perangkat lunak yang digunakan pada penelitian ini untuk membangun sistem administrasi disposisi surat adalah sebagai berikut:

- ✓ OS (*Operation System*) Windows 10 Pro 64bit.
- ✓ Visual Studio Code IDE (*Integrated Development Environment*).
- ✓ XAMPP (*Cross-Platform*, Apache, MySQL, PHP, Perl).
- ✓ *Programming Language* PHP 8.2.
- ✓ Browser Google Chrome dan Mozilla Firefox

3.1.6. Analisis Algoritma

Algoritma kriptografi yang digunakan pada penelitian ini adalah algoritma ECC (*Elliptic Curve Cryptography*). *Elliptic Curve Cryptography* (ECC) adalah pendekatan algoritma kriptografi kunci publik berdasarkan struktur aljabar kurva elips dalam domain terbatas.

Penggunaan kurva elips dalam kriptografi ditemukan oleh Neil Koblitz dan Victor S. Miller pada tahun 1985. Kurva elips juga digunakan dalam beberapa algoritma faktorisasi bilangan bulat yang juga memiliki aplikasi dalam kriptografi, seperti *Lenstra Elliptic Curve Factorization*. Algoritma kunci publik didasarkan pada berbagai perhitungan matematis dan dianggap sangat sulit untuk diselesaikan tanpa pengetahuan tentang bagaimana perhitungan tersebut dilakukan (Damanik P. S., 2019).

Kurva elips dapat ditulis dengan menggunakan perhitungan matematis sebagai berikut.

$$y^2 = x^3 + ax + b$$

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.

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

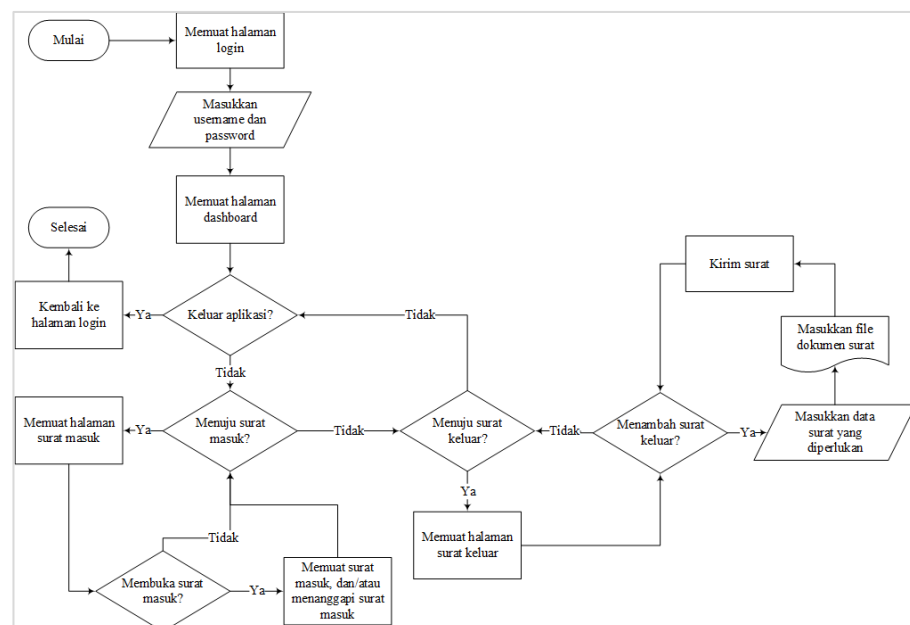
Budi kemudian menerjemahkan P_m ke dalam pesan asli m .

3.2. Desain Perancangan Sistem

Perancangan desain sistem menggunakan *tools* Micorosft Visio, StarUML, dan juga Balsamiq Wireframe.

3.2.1. Desain Sistem

a. *Flowchart Diagram*



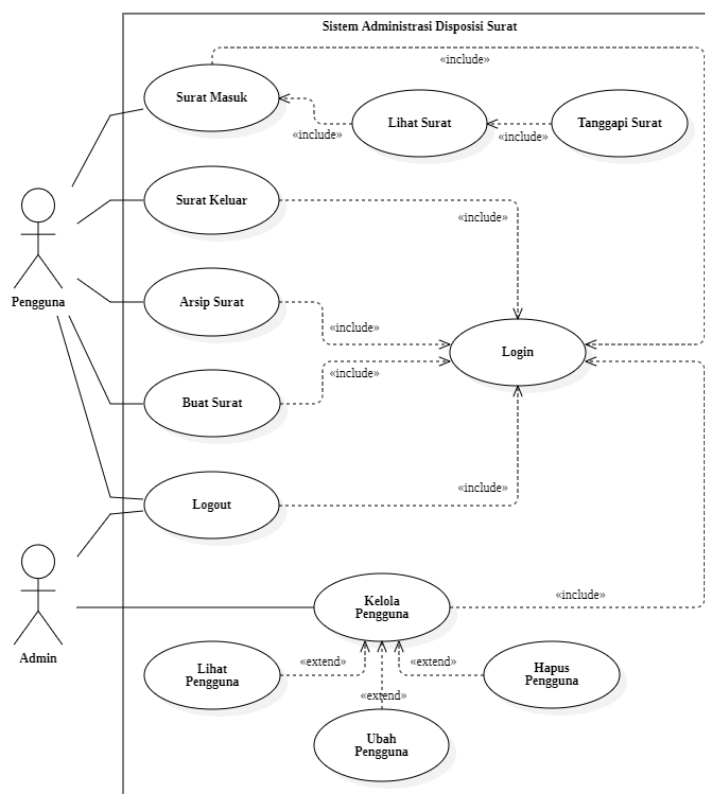
Gambar 9 - Flowchart Aplikasi

Flowchart dimulai dengan memuat halaman *login*, kemudian pengguna harus mengisi *username* dan *password* yang dimiliki untuk bisa masuk ke dalam sistem administrasi disposisi surat. Setelah 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*

Use case diagram pada sistem administrasi disposisi surat ini ditampilkan pada gambar sebagai berikut:



Gambar 10 - Use Case Diagram Sistem Administrasi Disposisi Surat

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

Tabel 4 - Deskripsi Actor Use Case

No.	Actor	Deskripsi
1.	Pengguna	Pengguna dapat mengakses halaman <i>dashboard</i> , surat masuk, surat keluar, dan arsip surat setelah melakukan <i>login</i> menggunakan akun pengguna.

2.	Admin	Admin dapat mengakses halaman <i>dashboard</i> dan kelola pengguna setelah <i>login</i> menggunakan akun admin.
----	-------	---

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

Tabel 5 - Deskripsi System Use Case

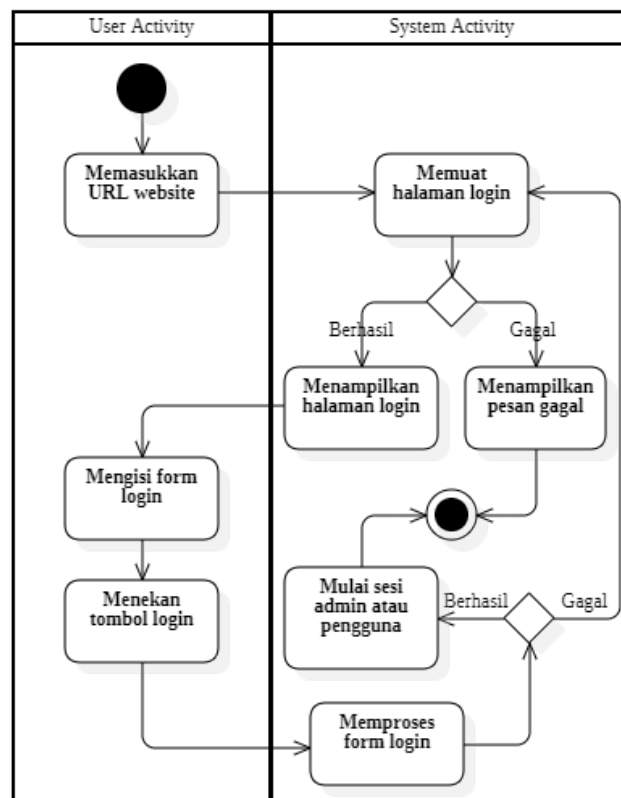
No.	System	Deskripsi
1.	Login	Fungsi ini digunakan sistem untuk pintu masuk dan verifikasi pengguna/admin yang akan menggunakan sistem administrasi disposisi surat.
2.	Surat Masuk	Fungsi ini digunakan sistem untuk menampilkan halaman berisi surat-surat yang diterima oleh pengguna.
3.	Lihat Surat	Fungsi 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 perubahan 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. *Activity Diagram*

Activity diagram pada sistem administrasi disposisi surat ini dijelaskan pada poin-poin berikut:

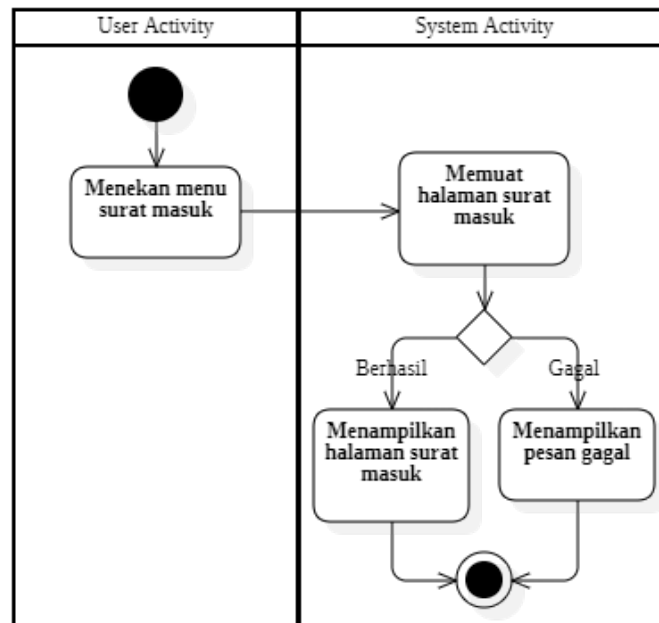
1) *Login*



Gambar 11 - Activity Diagram Login

- a) Admin/pengguna harus memasukkan alamat *website* untuk mengakses situs Sistem Administrasi Disposisi Surat.
- b) Setelah admin/pengguna memasukkan alamat *website*, sistem akan memuat halaman *login*.
- c) Apabila sistem berhasil memuat halaman *login*, maka sistem akan menampilkan halaman *login* kepada admin/pengguna (lanjut ke poin e).
- d) Apabila sistem gagal memuat halaman *login*, maka sistem akan menampilkan pesan gagal atau eror kepada admin/pengguna.
- e) Setelah halaman *login* berhasil ditampilkan, admin/pengguna harus mengisi *form* isian yang dibutuhkan.
- f) Admin/pengguna harus menekan tombol *login* untuk memverifikasi data yang diisi.
- g) Apabila proses verifikasi berhasil, maka sistem akan memulai sesi admin/pengguna.
- h) Apabila proses verifikasi gagal, maka sistem akan menampilkan pesan gagal atau eror.

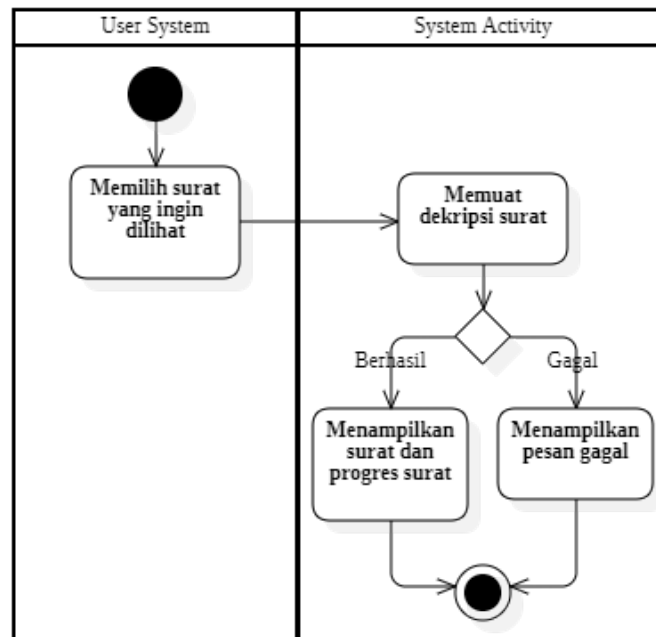
2) Surat Masuk



Gambar 12 - Activity Diagram Surat Masuk

- a) Pengguna harus menekan menu surat masuk untuk mengakses dan melihat daftar surat masuk.
- b) Setelah pengguna menekan menu surat masuk, sistem akan memuat halaman surat masuk.
- c) Apabila sistem berhasil memuat halaman surat masuk, maka sistem akan menampilkan halaman dan daftar surat masuk yang diterima oleh pengguna.
- d) Apabila sistem gagal memuat halaman surat masuk, maka sistem akan menampilkan pesan gagal atau error kepada pengguna.

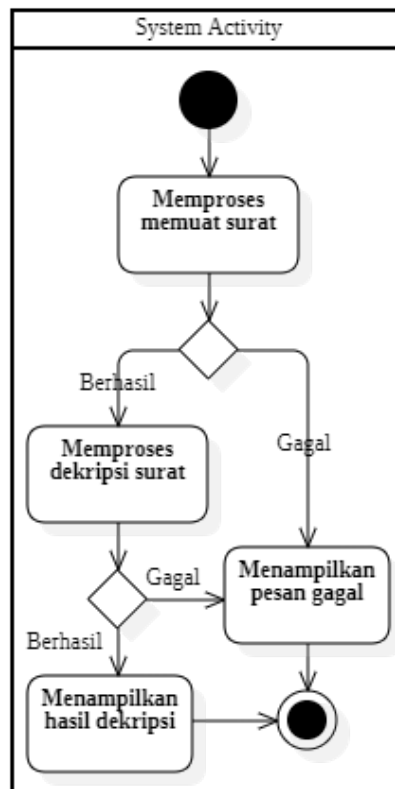
3) Lihat Surat



Gambar 13 - Activity Diagram Lihat Surat

- a) Pengguna harus memilih surat yang ada dalam daftar surat.
- b) Setelah pengguna memilih surat yang ingin dilihat, sistem akan memuat dan mendekripsikan isi surat.
- c) Apabila sistem berhasil memuat dan mendekripsikan isi surat, maka sistem akan menampilkan isi dan identitas surat kepada pengguna.
- d) Apabila sistem gagal memuat dan mendekripsikan isi surat, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.

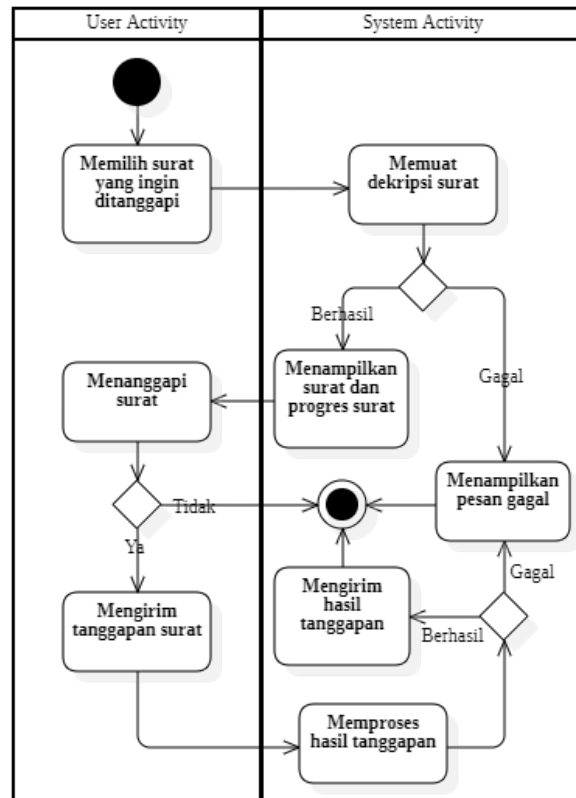
4) Dekripsi



Gambar 14 - Activity Diagram Dekripsi Surat

- a) Sistem akan memuat surat yang akan didekripsikan.
- b) Apabila sistem berhasil memuat surat, maka sistem akan memulai proses dekripsi surat (lanjut ke poin d).
- c) Apabila sistem gagal memuat surat, maka sistem akan menampilkan pesan gagal kepada pengguna.
- d) Pada proses dekripsi surat, apabila sistem berhasil melakukan proses dekripsi surat, maka sistem akan menampilkan surat dari hasil dekripsi.
- e) Apabila sistem gagal melakukan proses dekripsi surat, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.

5) Tanggapi Surat

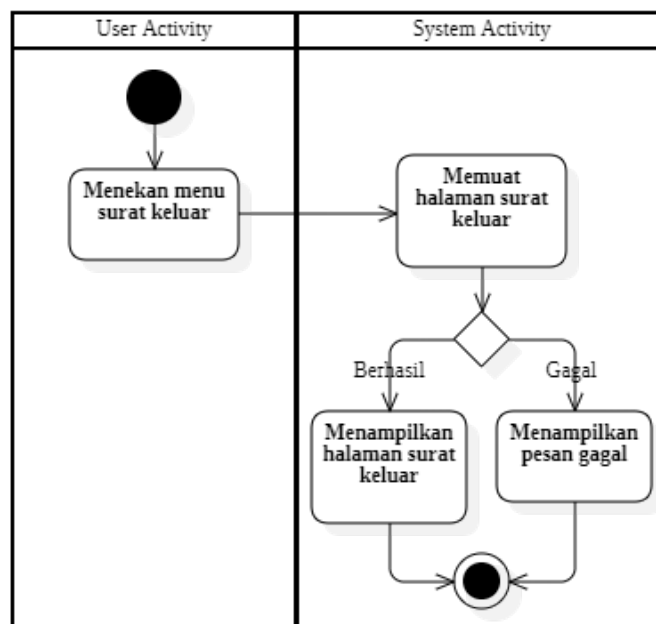


Gambar 15 - Activity Diagram Tanggapi Surat

- Pengguna harus memilih surat yang ada dalam daftar surat.
- Setelah pengguna memilih surat yang ingin ditanggapi, sistem akan melakukan proses dekripsi.
- Apabila sistem berhasil melakukan proses dekripsi, maka sistem akan menampilkan surat kepada pengguna (lanjut ke poin e).
- Apabila sistem gagal melakukan proses dekripsi, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.
- Setelah surat ditampilkan kepada pengguna, pengguna dapat menanggapi dan mengirim hasil tanggapan surat.

- f) Sistem akan memproses hasil tanggapan surat dari pengguna.
- g) Apabila sistem berhasil memproses hasil tanggapan surat, maka sistem akan menyimpan dan mengirim hasil tanggapan kepada pengirim surat.
- h) Apabila sistem gagal memproses hasil tanggapan surat, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.

6) Surat Keluar

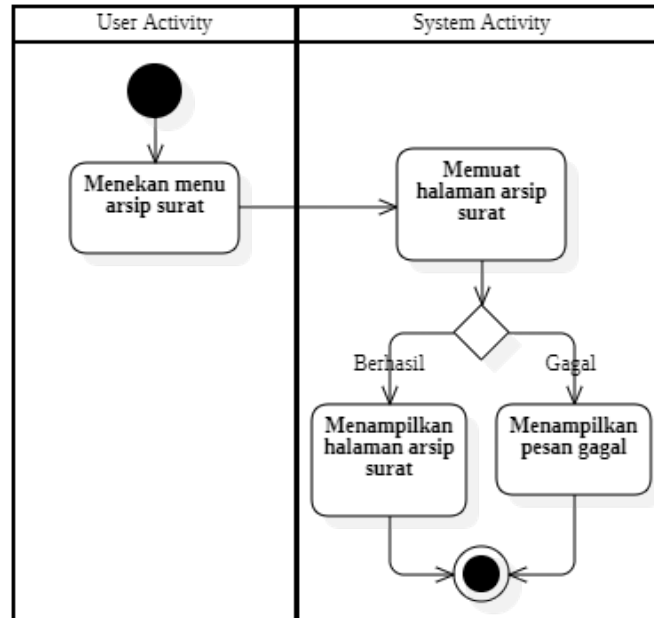


Gambar 16 - Activity Diagram Surat Keluar

- a) Pengguna harus menekan menu surat keluar untuk mengakses dan melihat daftar surat keluar.
- b) Setelah pengguna menekan menu surat keluar, sistem akan memuat halaman surat keluar.
- c) Apabila sistem berhasil memuat halaman surat keluar, maka sistem akan menampilkan halaman dan daftar surat keluar yang dikirim kepada pengguna lain.

- d) Apabila sistem gagal memuat halaman surat keluar, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.

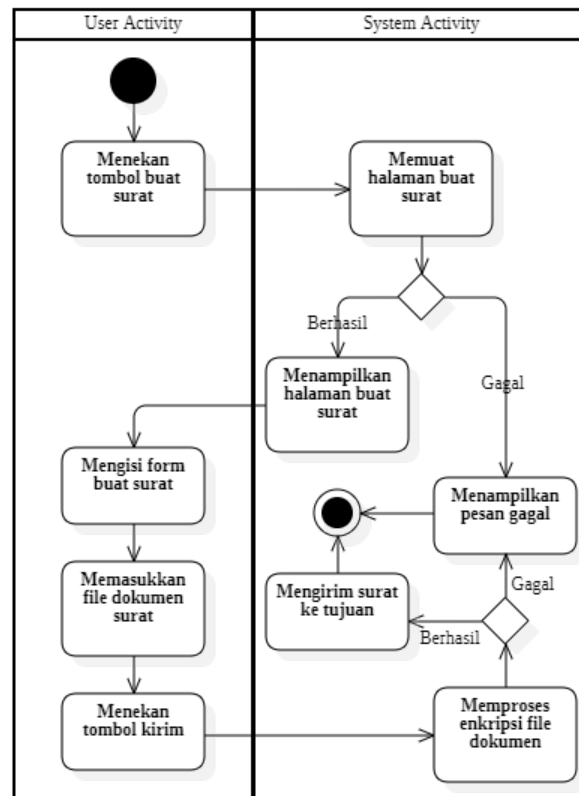
7) Arsip Surat



Gambar 17 - Activity Diagram Arsip Surat

- Pengguna harus menekan menu arsip surat untuk mengakses dan melihat daftar surat yang diarsipkan.
- Setelah pengguna menekan menu arsip surat, sistem akan memuat halaman arsip surat.
- Apabila sistem berhasil memuat halaman arsip surat, maka sistem akan menampilkan halaman dan daftar surat yang diarsipkan oleh pengguna.
- Apabila sistem gagal memuat halaman arsip surat, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.

8) Buat Surat

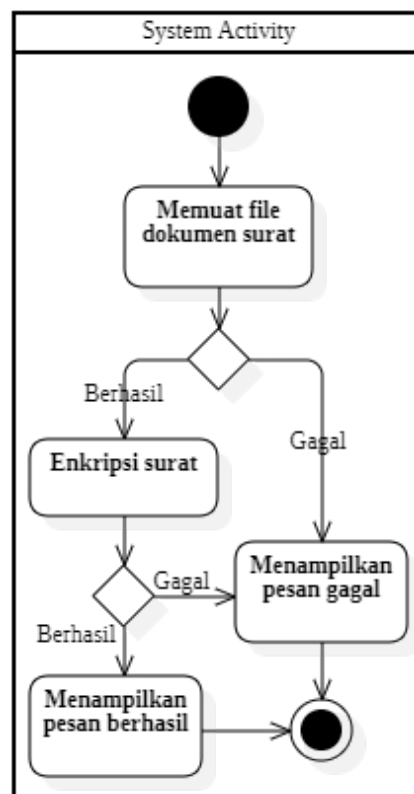


Gambar 18 - Activity Diagram Buat Surat

- Pengguna harus menekan tombol buat surat untuk membuat surat baru.
- Setelah pengguna menekan tombol buat surat, sistem akan memuat halaman untuk membuat surat.
- Apabila sistem berhasil memuat halaman buat surat, maka sistem akan menampilkan halaman buat surat berisi *form* isian untuk membuat surat (lanjut ke poin e).
- Apabila sistem gagal memuat halaman buat surat, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.
- Pengguna harus mengisi *form* isian yang dibutuhkan untuk membuat surat.

- f) Pengguna harus mengunggah *file* surat yang akan dikirimkan kepada pengguna lain.
- g) Pengguna harus menekan tombol kirim untuk mengirimkan surat.
- h) Setelah pengguna menekan tombol kirim, sistem akan memproses *form* isian yang telah diisi pengguna serta mengenkripsi *file* surat yang diunggah.
- i) Apabila sistem berhasil memproses dan mengenkripsi surat, maka sistem akan mengirim surat kepada pengguna yang dituju.
- j) Apabila sistem gagal memproses dan mengenkripsi surat, maka sistem akan menampilkan pesan gagal atau error kepada pengguna.

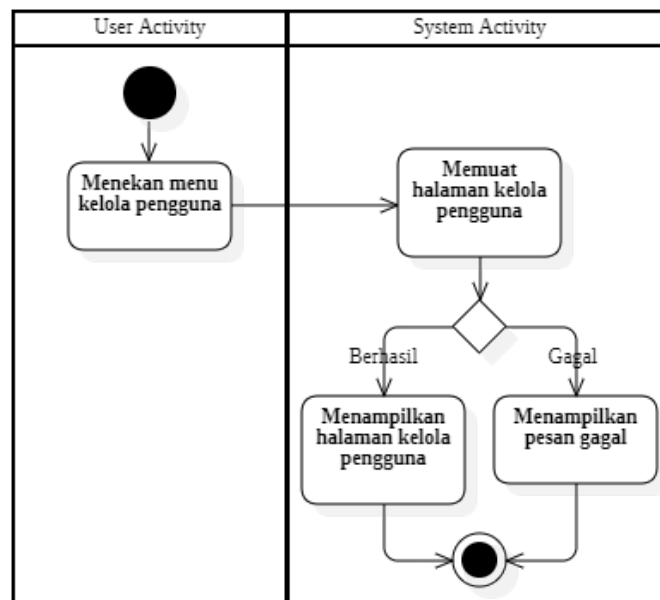
9) Enkripsi



Gambar 19 - Activity Diagram Enkripsi

- a) Sistem memuat *file* yang diunggah oleh pengguna.
- b) Apabila sistem berhasil memuat *file*, maka sistem akan melakukan enkripsi surat (lanjut ke poin d).
- c) Apabila sistem gagal memuat *file*, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.
- d) *File* yang berhasil dimuat oleh sistem akan dienkripsi.
- e) Apabila sistem berhasil melakukan enkripsi surat, maka sistem akan menampilkan pesan berhasil kepada pengguna.
- f) Apabila sistem gagal melakukan enkripsi surat, maka sistem akan menampilkan pesan gagal kepada pengguna.

10) Kelola Pengguna

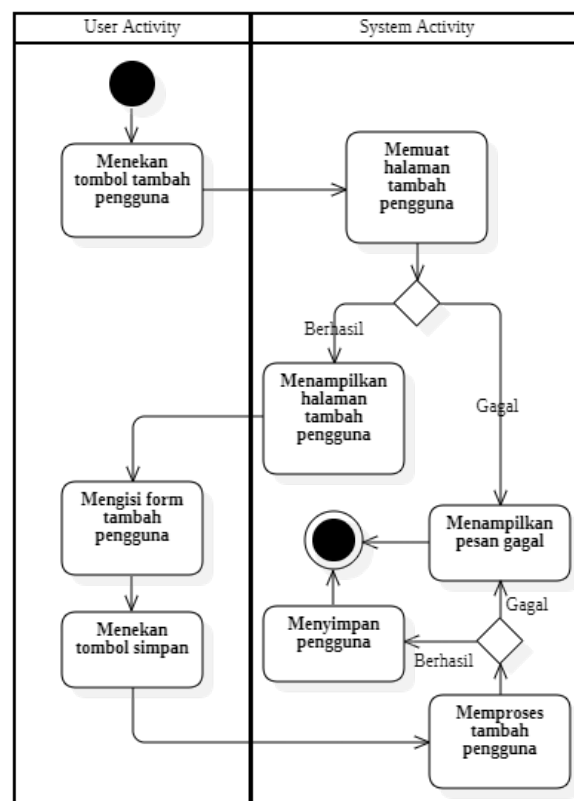


Gambar 20 - Activity Diagram Kelola Pengguna

- a) Admin harus menekan menu kelola pengguna untuk mengelola pengguna yang ada di dalam sistem.
- b) Setelah admin menekan menu kelola pengguna, sistem akan memuat halaman kelola pengguna.

- c) Apabila sistem berhasil memuat halaman kelola pengguna, maka sistem akan menampilkan halaman dan daftar anggota yang ada di dalam sistem.
- d) Apabila sistem gagal memuat halaman kelola pengguna, maka sistem akan menampilkan pesan gagal atau eror kepada pengguna.

11) Tambah Pengguna



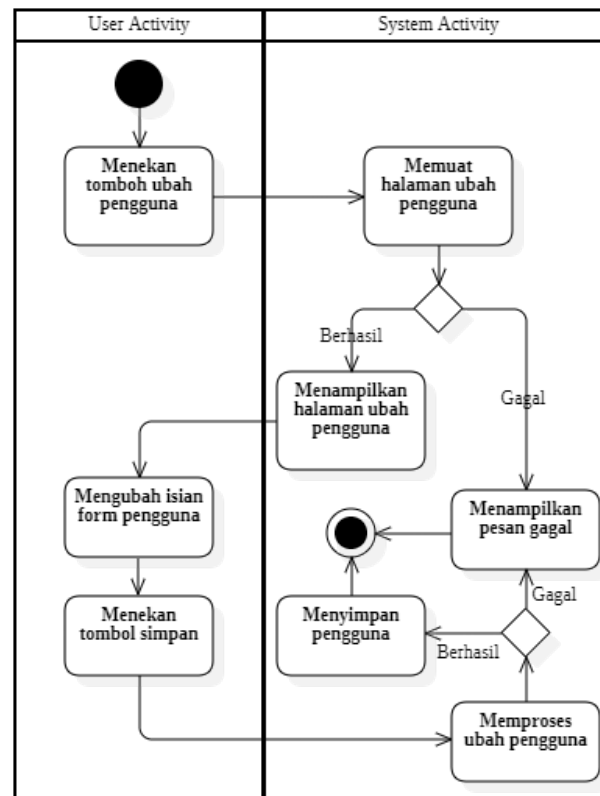
Gambar 21 - Activity Diagram Tambah Pengguna

- a) Admin harus menekan tombol tambah pengguna untuk menambahkan dan memasukkan pengguna ke dalam sistem.
- b) Setelah admin menekan tombol tambah pengguna, sistem akan memuat halaman tambah pengguna.
- c) Apabila sistem berhasil memuat halaman tambah pengguna, maka sistem akan menampilkan halaman

tambah pengguna dan menampilkan *form* isian untuk menambahkan pengguna (lanjut ke poin e).

- d) Apabila sistem gagal memuat halaman tambah pengguna, maka sistem akan menampilkan pesan gagal atau eror kepada admin.
- e) Setelah halaman tambah pengguna ditampilkan, admin harus mengisi *form* isian yang dibutuhkan.
- f) Admin harus menekan tombol simpan untuk menambahkan pengguna.
- g) Setelah admin menekan tombol simpan, sistem akan memproses penambahan pengguna.
- h) Apabila sistem berhasil memproses penambahan pengguna, maka sistem akan menampilkan pesan berhasil dan menyimpan penambahan pengguna.
- i) Apabila sistem gagal memproses penambahan pengguna, maka sistem akan menampilkan pesan gagal atau eror kepada admin.

12) Ubah Pengguna

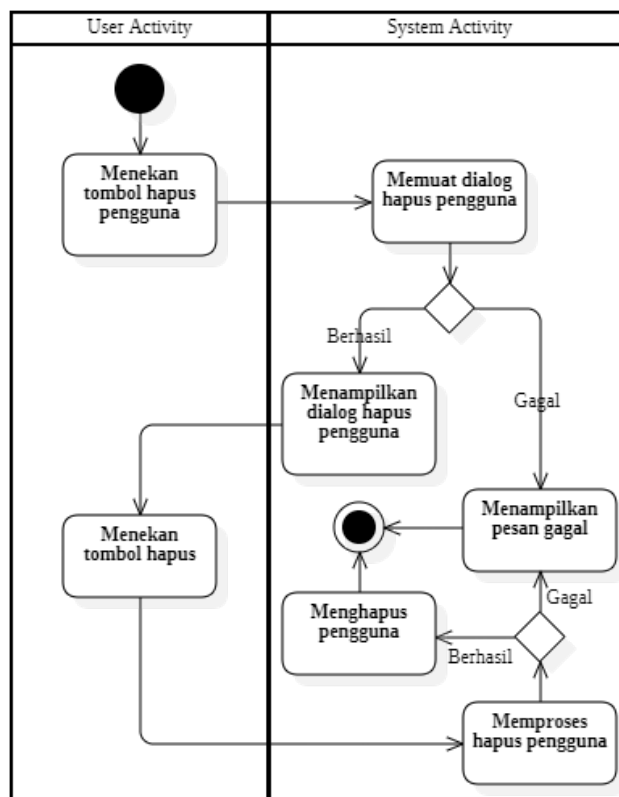


Gambar 22 - Activity Diagram Ubah Pengguna

- a) Admin harus menekan tombol ubah pengguna untuk mengubah pengguna yang ada di dalam sistem.
- b) Setelah admin menekan tombol ubah pengguna, sistem akan memuat halaman ubah pengguna.
- c) Apabila sistem berhasil memuat halaman ubah pengguna, maka sistem akan menampilkan halaman ubah pengguna dan menampilkan *form* isian untuk mengubah pengguna (lanjut ke poin e).
- d) Apabila sistem gagal memuat halaman ubah pengguna, maka sistem akan menampilkan pesan gagal atau error kepada admin.
- e) Setelah halaman ubah pengguna ditampilkan, admin harus mengisi *form* isian yang dibutuhkan.

- f) Admin harus menekan tombol simpan untuk menambahkan pengguna.
- g) Setelah admin menekan tombol simpan, sistem akan memproses pengubahan pengguna.
- h) Apabila sistem berhasil memproses pengubahan pengguna, maka sistem akan menampilkan pesan berhasil dan menyimpan pengubahan pengguna.
- i) Apabila sistem gagal memproses pengubahan pengguna, maka sistem akan menampilkan pesan gagal atau error kepada admin.

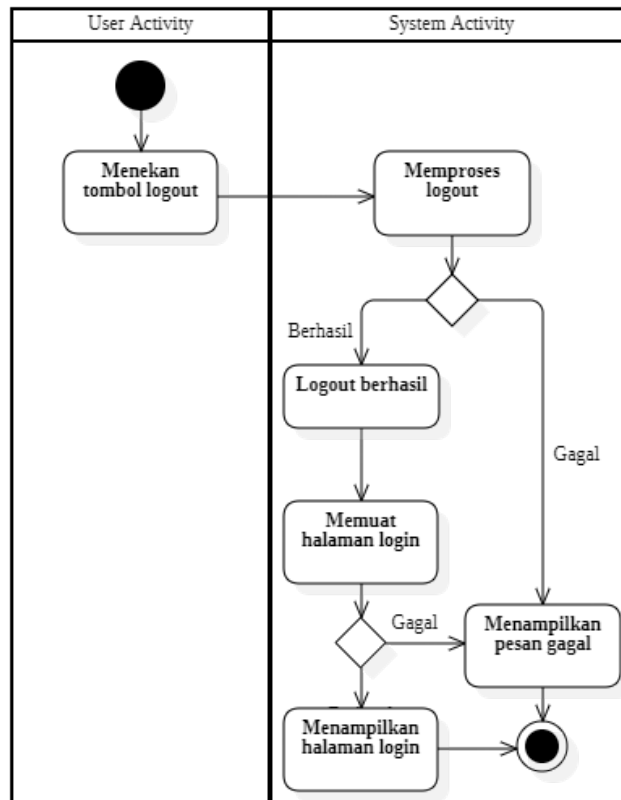
13) Hapus Pengguna



Gambar 23 - Activity Diagram Hapus Pengguna

- a) Admin harus menekan tombol hapus pengguna untuk menghapus pengguna yang ada di dalam sistem.
- b) Setelah admin menekan tombol hapus pengguna, sistem akan memuat dialog hapus pengguna.
- c) Apabila sistem berhasil memuat dialog hapus pengguna, maka sistem akan menampilkan dialog hapus pengguna (lanjut ke poin e).
- d) Apabila sistem gagal memuat dialog hapus pengguna, maka sistem akan menampilkan pesan gagal atau error kepada admin.
- e) Setelah dialog hapus pengguna ditampilkan, admin bisa menekan tombol hapus.
- f) Setelah admin menekan tombol hapus, sistem akan memproses penghapusan pengguna.
- g) Apabila sistem berhasil memproses penghapusan pengguna, maka sistem akan menampilkan pesan berhasil dan menghapus pengguna dari sistem.
- h) Apabila sistem gagal memproses penghapusan pengguna, maka sistem akan menampilkan pesan gagal atau error kepada admin.

14) Logout



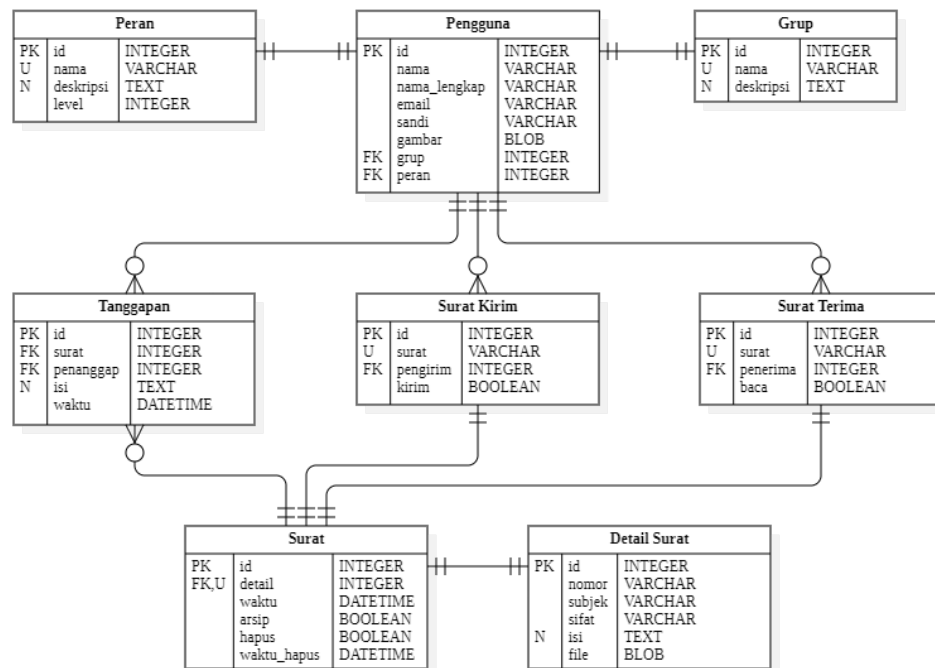
Gambar 24 - Activity Diagram Logout

- a) Admin/pengguna menekan tombol *logout*.
- b) Setelah admin/pengguna menekan tombol *logout*, sistem akan memproses *logout*.
- c) Apabila sistem berhasil memproses *logout* admin/pengguna, maka sistem akan menampilkan pesan berhasil *logout* dan memuat halaman *login* (lanjut ke poin e).
- d) Apabila sistem gagal memproses *logout* admin/pengguna, maka sistem akan menampilkan pesan gagal atau error kepada admin/pengguna.
- e) Setelah berhasil memproses *logout* admin/pengguna, sistem akan memuat halaman *login*.

- f) Apabila sistem berhasil memuat halaman *login*, maka sistem akan menampilkan halaman *login*.
- g) Apabila sistem gagal memuat halaman *login*, maka sistem akan menampilkan pesan gagal atau error.

3.2.2. Database

Database yang digunakan pada pembangunan sistem administrasi disposisi surat ini adalah MySQL dengan *engine* InnoDB. Berikut merupakan desain gambaran perancangan *database* pada sistem administrasi disposisi surat ini yaitu:



Gambar 25 - Entity Relationship Diagram

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

3.2.3. Mockup Interface

Berikut merupakan desain *mock up* yang dibuat untuk sistem administrasi disposisi surat yaitu:

The wireframe shows a login page titled 'Halaman Login'. Inside, there is a 'Formulir Login' box. At the top of the box is 'Selamat datang'. Below it are two input fields: 'Username: Isian username' and 'Password: Isian password'. At the bottom of the box is a 'Masuk' button.

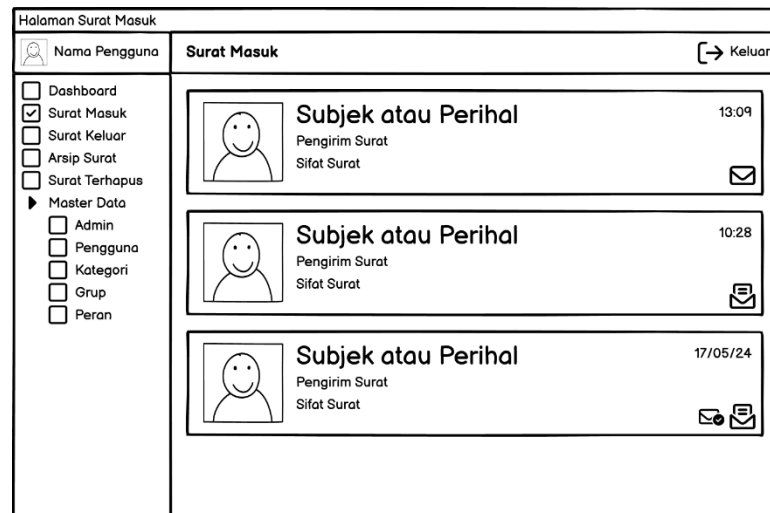
Gambar 26 - Wireframe Login

Pada halaman *login* ditampilkan *form* berisi *username* dan *password* yang harus diisi. Saat pengguna menekan tombol masuk, sistem akan melakukan verifikasi. *Login* berhasil apabila isian *username* dan *password* sesuai dengan yang ada di dalam sistem.

The wireframe shows a dashboard page titled 'Halaman Dashboard'. It has a sidebar on the left with a user profile icon and 'Nama Pengguna'. The sidebar menu includes: Dashboard (checked), Surat Masuk, Surat Keluar, Arsip Surat, Surat Terhapus, Master Data (expanded), Admin, Pengguna, Kategori, Grup, and Peran. The main content area is titled 'Dashboard' and has a 'Keluar' button. It features a welcome message: 'Selamat Datang, Pengguna Di Aplikasi Pemantauan Disposisi Surat' with an envelope icon. Below this are three summary cards: 'Surat Masuk' with the value 3, 'Surat Keluar' with the value 2, and 'Diarsipkan' with the value 4. Each card has a right-pointing arrow.

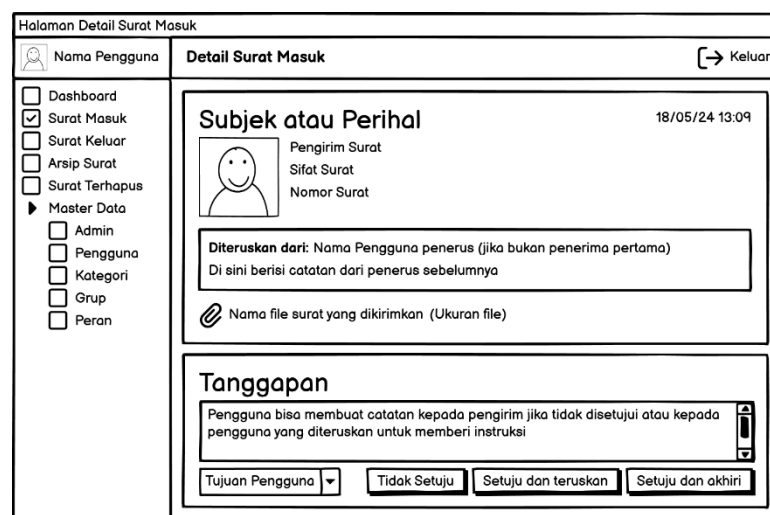
Gambar 27 - Wireframe Dashboard

Pada halaman *dashboard* ditampilkan ringkasan mengenai surat masuk, surat keluar, dan surat yang diarsipkan. Apabila setiap menu ditekan, maka akan menuju ke halaman setiap menu.



Gambar 28 - Wireframe Surat Masuk

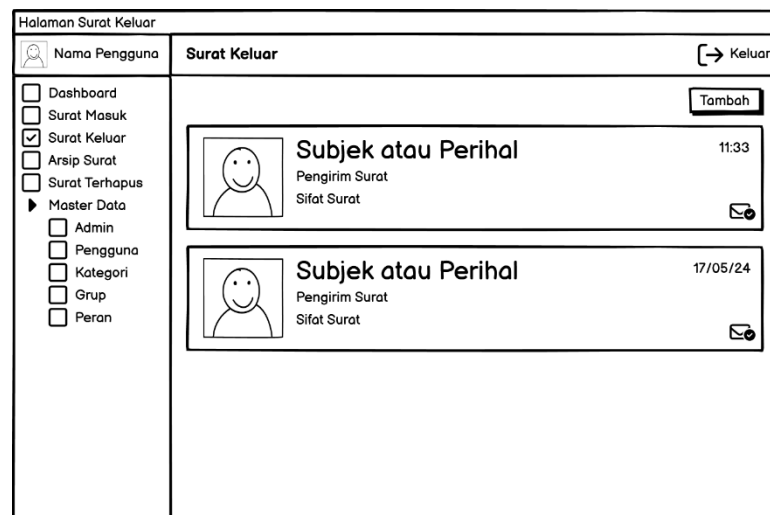
Pada halaman surat masuk ditampilkan daftar surat-surat yang diterima oleh pengguna dan ringkasan status surat pada setiap surat yang ditampilkan. Apabila setiap surat ini dipilih, maka surat akan terbuka dan menampilkan detail dari surat yang dipilih tersebut.



Gambar 29 - Wireframe Detail Surat Masuk

Pada halaman detail surat masuk ditampilkan detail dari surat yang dipilih pada halaman surat masuk. Halaman ini menampilkan detail dengan perincian sebagai berikut:

- a. Subjek/perihal;
- b. Pengirim surat;
- c. Sifat surat;
- d. Nomor surat;
- e. File surat;
- f. Catatan dari pengirim atau penerus surat sebelumnya;
- g. Tanggapan kepada pengirim pertama surat dan penerima surat selanjutnya.



Gambar 30 - Wireframe Surat Keluar

Pada halaman surat keluar ditampilkan daftar surat-surat yang dikirim oleh pengguna kepada pengguna lain dan ringkasan status surat pada setiap surat yang ditampilkan. Apabila setiap surat ini dipilih, maka surat akan terbuka dan menampilkan detail dari surat yang dipilih tersebut.

Halaman Detail Surat Keluar	
Nama Pengguna	Detail Surat Keluar [→] Keluar
☐ Dashboard ☐ Surat Masuk ☒ Surat Keluar ☐ Arsip Surat ☐ Surat Terhapus ▶ Master Data ☐ Admin ☐ Pengguna ☐ Kategori ☐ Grup ☐ Peran	Subjek atau Perihal 18/05/24 11:33 Pengguna Tujuan Surat Sifat Surat Nomor Surat Nama file surat yang dikirimkan (Ukuran file) Tanggapan ☒ Dikirim kepada Pengguna A (17/05/24 10:14) ☒ Disetujui dan diteruskan kepada Pengguna B (17/05/24 14:48) Catatan dari Pengguna A kepada Pengguna B ☒ Disetujui dan diteruskan kepada Pengguna C (18/05/24 11:42) Catatan dari Pengguna B kepada Pengguna C

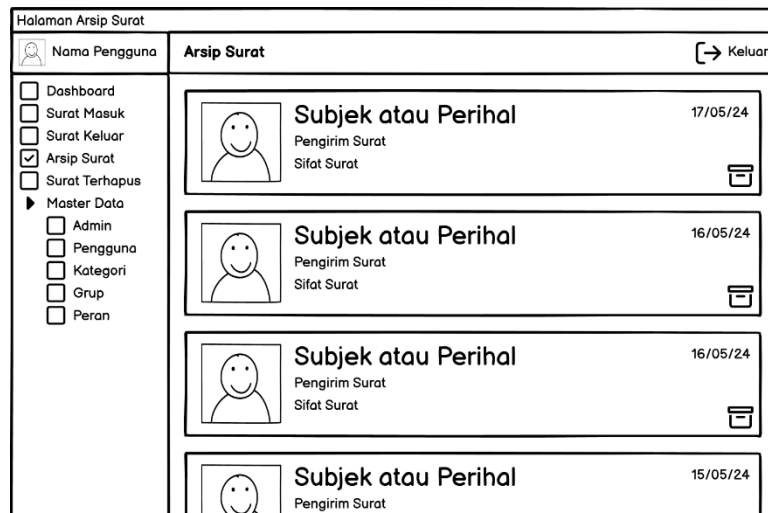
Gambar 31 - Wireframe Detail Surat Keluar

Pada halaman detail surat keluar ditampilkan detail surat yang dikirimkan kepada pengguna lain dan tanggapan dari setiap penerima surat kepada pengguna lainnya.

Halaman Tambah Surat Keluar	
Nama Pengguna	Tambah Surat Keluar [→] Keluar
☐ Dashboard ☐ Surat Masuk ☒ Surat Keluar ☐ Arsip Surat ☐ Surat Terhapus ▶ Master Data ☐ Admin ☐ Pengguna ☐ Kategori ☐ Grup ☐ Peran	Pengirim Isian nama pengguna pengirim pesan (dari pengguna yang digunakan) Penerima Daftar nama pengguna yang akan dijadikan penerima surat Perihal Isian subjek atau perihal surat Sifat Surat ☐ Sangat Segera ☐ Segera ☐ Rahasia ☐ Pilih File Nama file surat (setelah file dipilih) Kirim

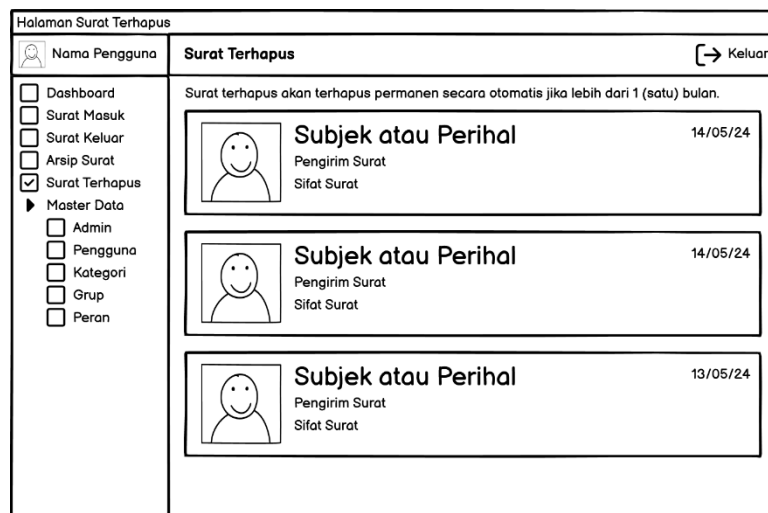
Gambar 32 - Wireframe Tambah Surat

Pada halaman tambah surat keluar ditampilkan formulir isian berupa data surat yang akan dikirimkan kepada pengguna lain. Juga diwajibkan untuk melampirkan file surat agar diperiksa oleh penerima surat.



Gambar 33 - Wireframe Arsip Surat

Pada halaman arsip surat ditampilkan daftar surat-surat yang diarsipkan oleh pengguna. Apabila setiap surat ini dipilih, maka surat akan terbuka dan menampilkan detail dari surat yang dipilih tersebut.



Gambar 34 - Wireframe Surat Terhapus

Pada halaman surat terhapus ditampilkan daftar surat-surat yang dihapus oleh pengguna. Surat yang ada di dalam daftar surat terhapus akan terhapus secara permanen dan otomatis apabila mencapai waktu 1 (satu) bulan sejak waktu penghapusan surat atau pengguna menekan tombol hapus permanen pada halaman surat terhapus.

3.2.4. Perancangan Pengujian

Pengujian yang digunakan dalam proses pembangunan sistem informasi pengiriman surat ini adalah pengujian *black box*. Pengujian perilaku adalah nama lain dari pengujian kotak hitam. Metode ini mengevaluasi fungsionalitas dan kegunaan aplikasi. Pengujian *black box* adalah jenis pengujian yang memeriksa semua persyaratan dan standar perangkat lunak. Pengujian *black box* memeriksa perangkat lunak hanya berdasarkan *input* dan *output* sistem, tanpa proses pemrograman internal apa pun.

a. Login

Tabel 6 - Skenario Black Box - Login

No.	Kasus Uji	Hasil yang Diharapkan
1.	Formulir isian <i>login</i> kosong.	Muncul pesan isian harus diisi.
2.	Mengisi isian <i>username</i> , tetapi mengosongkan isian <i>password</i> .	Muncul pesan isian harus diisi.
3.	Mengisi isian <i>password</i> , tetapi mengosongkan isian <i>username</i> .	Muncul pesan isian harus diisi.
4.	Mengisi isian <i>username</i> dan <i>password</i> dengan <i>username</i> tidak terdaftar.	Muncul pesan <i>username</i> atau <i>password</i> salah.
5.	Mengisi isian <i>username</i> dan <i>password</i> dengan <i>username</i> terdaftar dan <i>password</i> salah.	Muncul pesan <i>username</i> atau <i>password</i> salah.
6.	Mengisi isian <i>username</i> dan <i>password</i> dengan <i>username</i> terdaftar dan <i>password</i> benar.	Login berhasil sesuai dengan hak akses dan diarahkan ke halaman <i>dashboard</i> .

b. *Dashboard**Tabel 7 - Skenario Black Box - Dashboard*

No.	Kasus Uji	Hasil yang Diharapkan
1.	Pilih menu surat masuk.	Diarahkan ke halaman surat masuk.
2.	Pilih menu surat keluar.	Diarahkan ke halaman surat keluar.
3.	Pilih menu arsip surat.	Diarahkan ke halaman arsip surat.
4.	Pilih menu admin, khusus untuk hak akses admin.	Diarahkan ke halaman admin.
5.	Pilih menu pengguna, khusus untuk hak akses admin.	Diarahkan ke halaman pengguna.
6.	Pilih menu grup pengguna, khusus untuk hak akses admin.	Diarahkan ke halaman grup pengguna.

c. *Surat Masuk**Tabel 8 - Skenario Black Box - Surat Masuk*

No.	Kasus Uji	Hasil yang Diharapkan
1.	Tidak ada surat masuk.	Muncul halaman kosong.
2.	Ada surat masuk.	Muncul daftar surat yang diterima pengguna.
3.	Jika ada surat masuk, pilih surat.	Diarahkan ke halaman detail surat.

d. *Lihat Surat**Tabel 9 - Skenario Black Box - Lihat Surat*

No.	Kasus Uji	Hasil yang Diharapkan
1.	Surat dilihat oleh orang yang tidak berkepentingan.	Diarahkan ke halaman <i>dashboard</i> .

2.	Surat dilihat oleh orang yang tepat.	Muncul detail surat yang dipilih.
3.	Tekan tombol arsipkan.	Surat akan dipindah ke daftar arsip dan pengguna diarahkan ke halaman arsip.

e. Tanggapi Surat

Tabel 10 - Skenario Black Box - Tanggapi Surat

No.	Kasus Uji	Hasil yang Diharapkan
1.	Surat dilihat oleh orang yang tidak berkepentingan.	Diarahkan ke halaman <i>dashboard</i> .
2.	Surat dilihat oleh orang yang tepat.	Muncul detail surat.
3.	Formulir isian kosong, tetapi tekan tombol surat diteruskan.	Muncul pesan isian harus diisi.
4.	Mengisi isian email tujuan yang salah (tidak terdaftar), isian komentar/tanggapan kosong, lalu tekan tombol surat diteruskan.	Muncul pesan email tidak terdaftar.
5.	Mengisi isian email tujuan dengan benar, isian komentar/tanggapan kosong, lalu tekan tombol surat diteruskan.	Surat dikirim kepada tujuan tanpa mengirim isi komentar/tanggapan.
6.	Mengisi isian email tujuan dengan benar, mengisi isian komentar/tanggapan, lalu tekan tombol surat diteruskan.	Surat dikirim kepada tujuan dengan mengirim isi komentar/tanggapan.
7.	Tekan tombol surat tidak disetujui.	Surat dikirim kepada pengirim surat dengan status surat ditolak.

8.	Tekan tombol surat disetujui.	Surat dikirim kepada pengirim surat dengan status surat disetujui.
----	-------------------------------	--

f. Surat Keluar

Tabel 11 - Skenario Black Box - Surat Keluar

No.	Kasus Uji	Hasil yang Diharapkan
1.	Tidak ada surat keluar.	Muncul halaman kosong.
2.	Ada surat keluar.	Muncul daftar surat yang dikirim kepada pengguna lain.
3.	Jika ada surat keluar, pilih surat.	Diarahkan ke halaman detail surat.

g. Arsip Surat

Tabel 12 - Skenario Black Box - Arsip Surat

No.	Kasus Uji	Hasil yang Diharapkan
1.	Tidak ada arsip surat.	Muncul halaman kosong.
2.	Ada arsip surat keluar.	Muncul daftar surat yang diarsipkan oleh pengguna.
3.	Jika ada arsip surat, pilih surat.	Diarahkan ke halaman detail surat.

h. Buat Surat

Tabel 13 - Skenario Black Box - Buat Surat

No.	Kasus Uji	Hasil yang Diharapkan
1.	Formulir isian buat surat kosong, lalu tekan tombol kirim.	Muncul pesan isian harus diisi dan file harus dipilih.

2.	Mengisi email tujuan yang salah (tidak terdaftar) dan mengosongkan isian lainnya, lalu tekan tombol kirim.	Muncul pesan email tidak terdaftar, isian harus diisi, dan file harus dipilih.
3.	Mengisi isian email tujuan dengan benar, tetapi mengosongkan isian lainnya, lalu tekan tombol kirim.	Muncul pesan isian harus diisi dan file harus dipilih.
4.	Mengisi isian email tujuan dengan benar dan nomor surat, tetapi mengosongkan isian lainnya, lalu tekan tombol kirim.	Muncul pesan isian harus diisi dan file harus dipilih.
5.	Mengisi isian email tujuan dengan benar, nomor surat, perihal surat, dan mengosongkan isian lainnya, lalu tekan tombol kirim.	Muncul pesan file harus dipilih.
6.	Mengisi isian email tujuan dengan benar, nomor surat, perihal surat, dan memilih file bukan pdf, lalu tekan tombol kirim.	Muncul pesan file harus berformat PDF.
7.	Mengisi isian email tujuan dengan benar, nomor surat, perihal surat, dan memilih file pdf, lalu tekan tombol kirim.	Surat dikirim kepada tujuan dalam bentuk terenkripsi.

i. Kelola Pengguna

Tabel 14 - Skenario Black Box - Kelola Pengguna

No.	Kasus Uji	Hasil yang Diharapkan
1.	Jika pengguna tidak memiliki hak akses admin.	Diarahkan ke halaman <i>dashboard</i> .
2.	Jika pengguna memiliki hak akses admin.	Muncul daftar pengguna.

3.	Tekan tombol tambah pengguna.	Muncul formulir isian tambah pengguna.
4.	Tekan tombol tambah pengguna, formulir isian kosong, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.
5.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> , tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.
6.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dan nama lengkap, tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.
7.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang salah, tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi dan format email salah.
8.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.
9.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i> , dan mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.

10.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i> , grup pengguna, dengan <i>username</i> yang telah terdaftar, lalu tekan tombol tambah.	Muncul pesan <i>username</i> telah terdaftar.
11.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i> , grup pengguna, dengan email yang telah terdaftar, lalu tekan tombol tambah.	Muncul pesan email telah terdaftar.
12.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i> , grup pengguna, lalu tekan tombol tambah.	Muncul pesan pengguna berhasil ditambahkan.

j. *Logout*

Tabel 15 - Skenario Black Box - Logout

No.	Kasus Uji	Hasil yang Diharapkan
1.	Tekan tombol <i>logout</i> .	Sesi pengguna akan berakhir dan diarahkan ke halaman <i>login</i> .

BAB IV

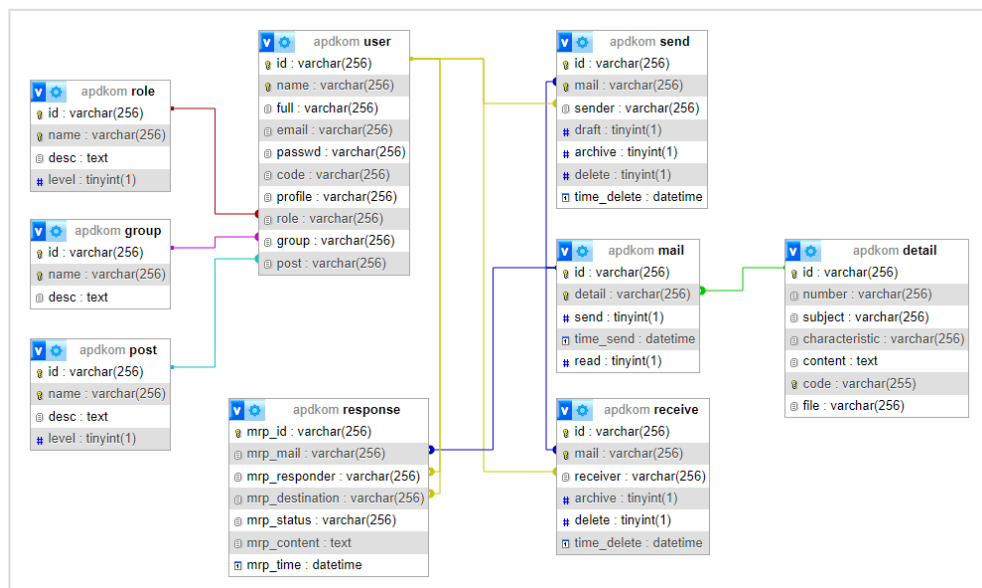
IMPLEMENTASI PENGEMBANGAN DAN PENGUJIAN SISTEM

Pada bab ini akan dijabarkan mengenai implementasi pengembangan sistem dan pengujian sistem administrasi disposisi surat.

4.1. Implementasi

4.1.1. Implementasi *Database*

Berikut merupakan implementasi dari perancangan *database* untuk sistem administrasi disposisi surat menggunakan *tool* phpMyAdmin dari aplikasi XAMPP. Terdapat 9 (sembilan) tabel yang saling terhubung ke setiap *primary key* di masing-masing tabel. Tabel *user* dihubungkan dengan tabel *role*, *group*, dan *post*. Kemudian tabel *mail* dihubungkan dengan tabel *detail* untuk mengambil data inti surat yang didistribusikan. Tabel *user* dan tabel *mail* dihubungkan melalui tabel *send*, *receive*, dan *response*.



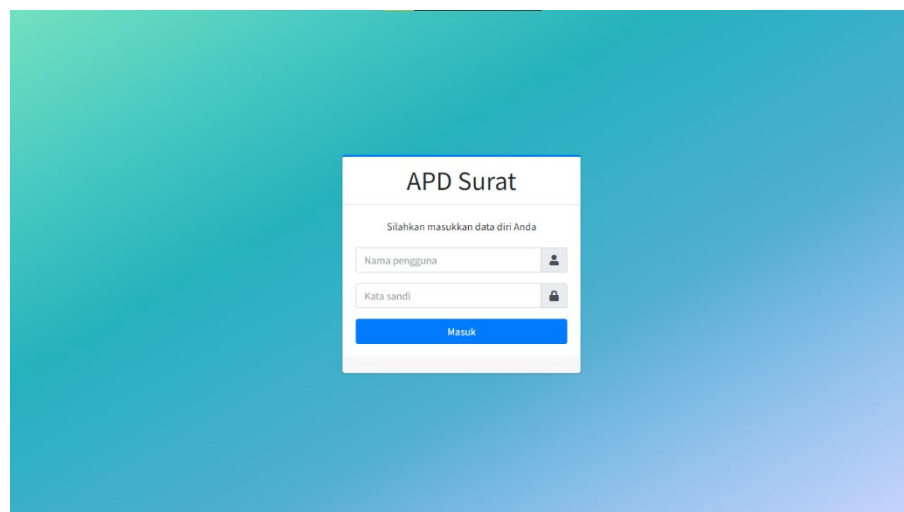
Gambar 35 - Database System

4.1.2. Implementasi *Interface*

Implementasi *interface* menggunakan *framework* CodeIgniter. Beberapa tampilan yang disediakan di antaranya adalah tampilan untuk *login*, halaman *dashboard*, halaman surat masuk, detail surat masuk beserta formulir untuk menanggapi surat, halaman surat keluar, detail surat keluar beserta pemantauan status surat, halaman arsip surat, dan pengelolaan pengguna.

a. *Login*

Halaman *login* adalah halaman yang pertama kali akan muncul ketika pergi ke alamat situs sistem administrasi disposisi surat pada penelitian ini.

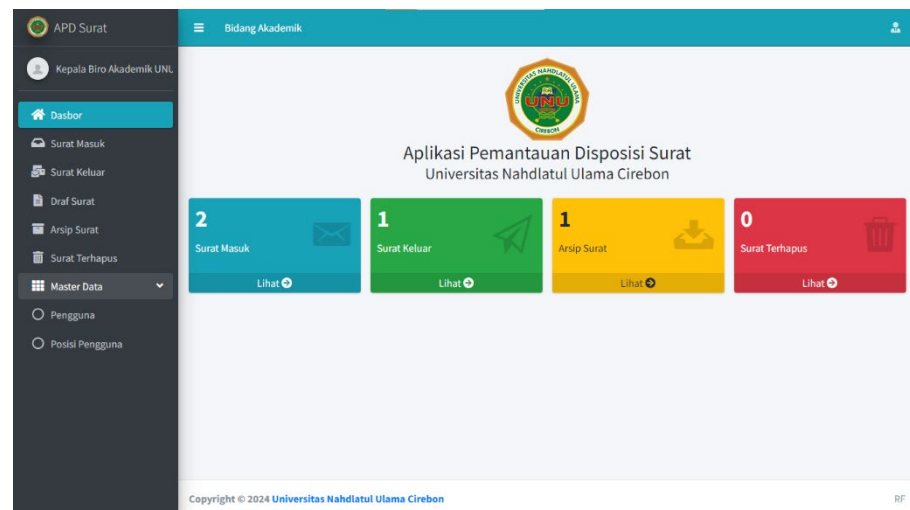


Gambar 36 - Interface Halaman Login

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*.

b. *Dashboard*

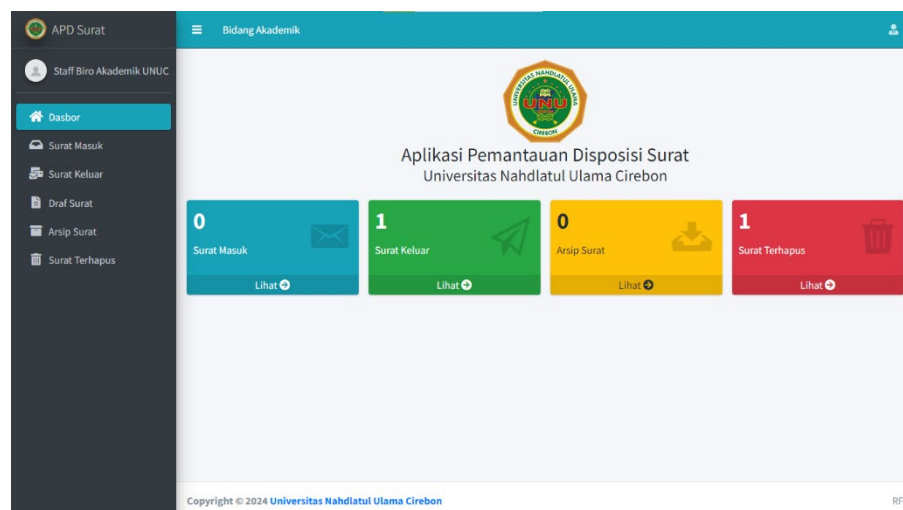
Halaman *dashboard* adalah halaman yang akan ditampilkan apabila proses *login* di awal berhasil.



Gambar 37 - Interface Halaman Dashboard Admin

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.

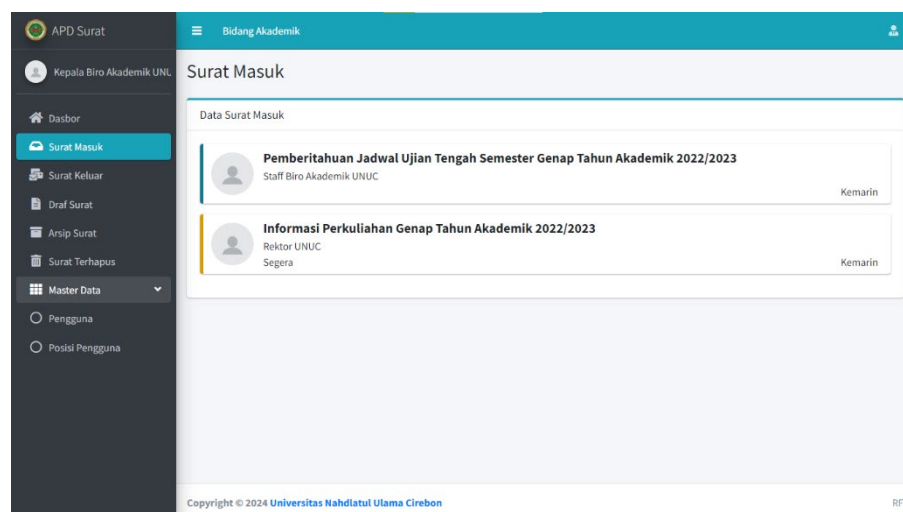
Pada bagian atas halaman ditampilkan bar yang menampilkan nama grup pengguna, profil pengguna, dan juga terdapat tombol *logout*. Pada bagian sisi samping kiri juga terdapat menu navigasi yang dapat dipilih untuk pergi ke halaman lain. Halaman yang dapat diakses tergantung dari hak akses yang dimiliki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



Gambar 38 - Interface Halaman Dashboard User

c. Surat Masuk

Halaman surat masuk akan ditampilkan apabila pengguna menekan tombol surat masuk di halaman *dashboard* atau memilih menu surat masuk pada menu navigasi.

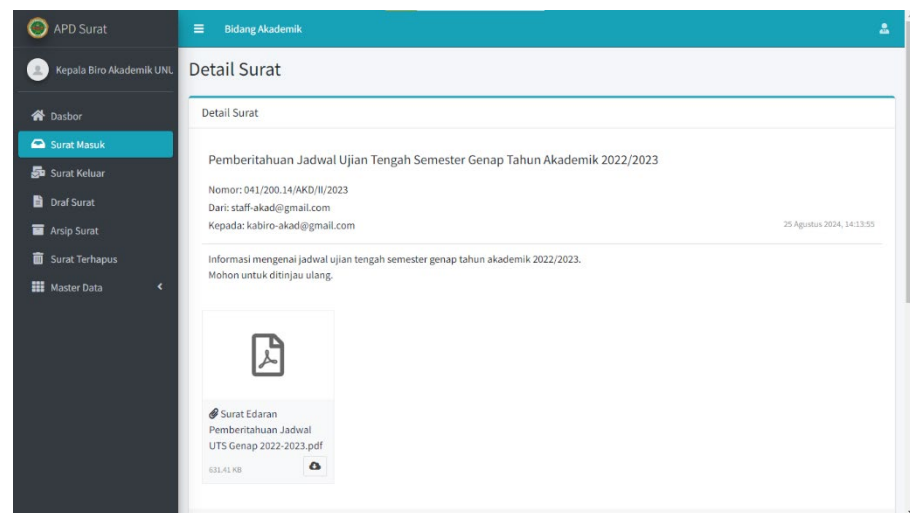


Gambar 39 - Interface Halaman Surat Masuk

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.

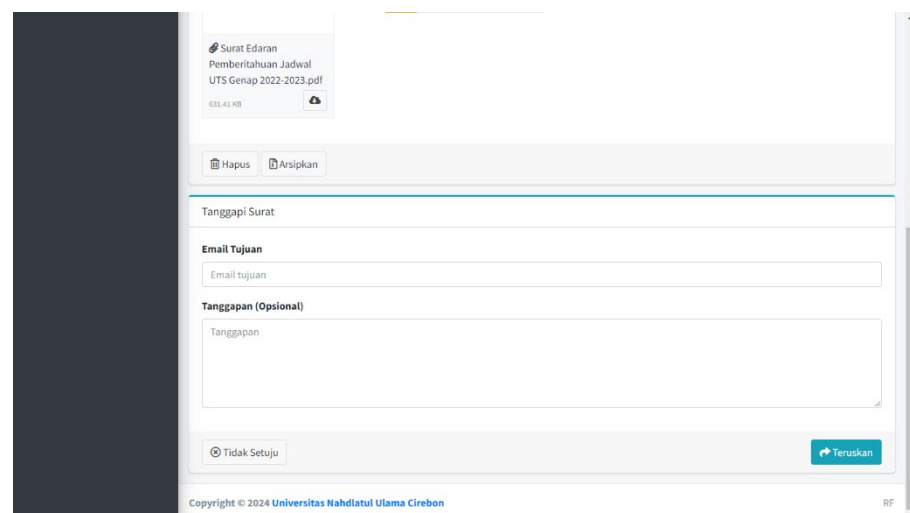
d. Detail Surat Masuk & Tanggapan

Halaman detail surat masuk adalah halaman yang akan ditampilkan apabila pengguna menekan salah satu surat pada daftar surat yang ada di halaman surat masuk.



Gambar 40 - Interface Halaman Detail Surat Masuk (Atas)

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.

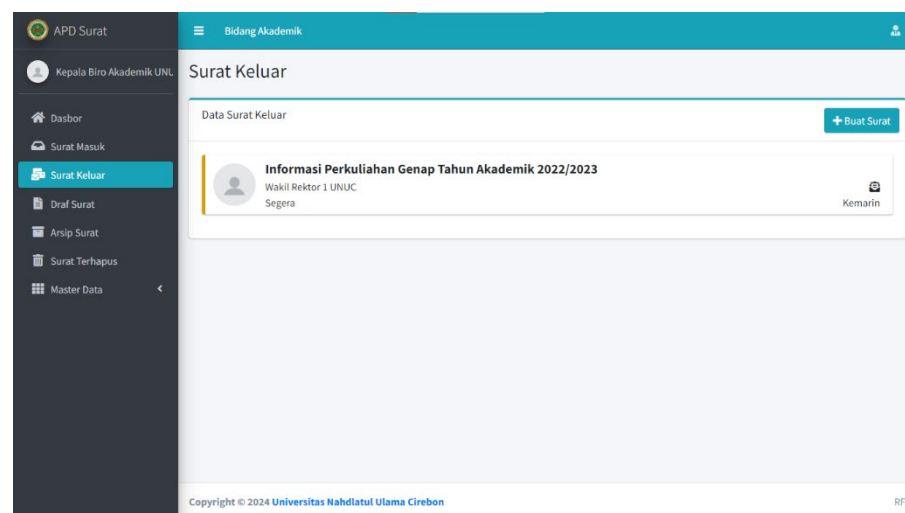


Gambar 41 - Interface Halaman Detail Surat Masuk (Bawah)

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.

e. Surat Keluar

Halaman surat keluar akan ditampilkan apabila pengguna menekan tombol surat keluar di halaman *dashboard* atau memilih menu surat keluar pada menu navigasi.



Gambar 42 - Interface Halaman Surat Keluar

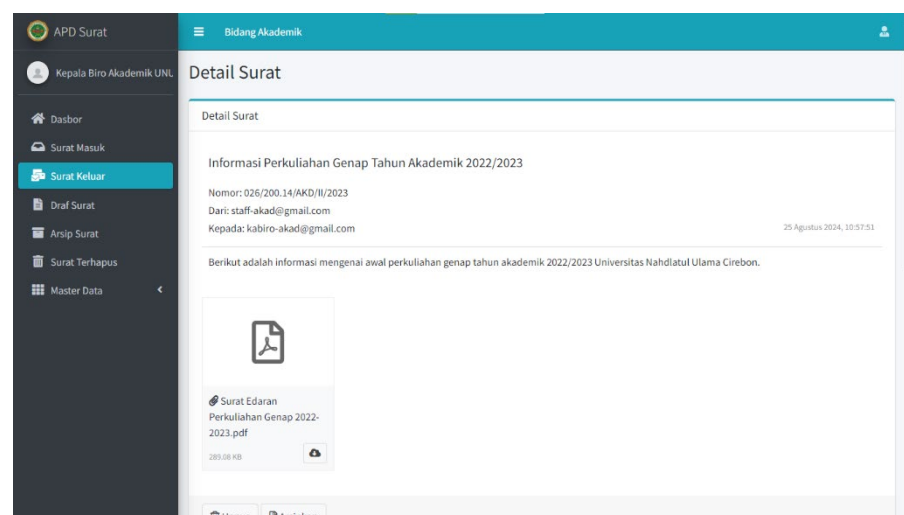
Pada halaman surat keluar ditampilkan daftar keseluruhan surat yang dikirim pengguna kepada pengguna lainnya. Pada setiap surat akan ditampilkan status terbaca apabila penerima surat sudah membuka surat yang dikirim atau menanggapi surat tersebut. Setiap surat dapat ditekan untuk melihat detail dari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

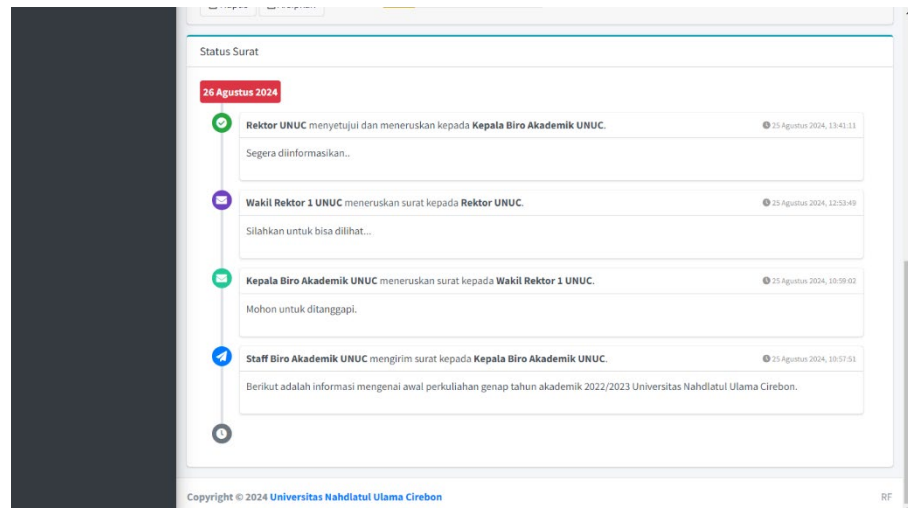
f. Detail Surat Keluar & Pantauan

Halaman detail surat keluar adalah halaman yang akan ditampilkan apabila pengguna menekan salah satu surat pada daftar surat yang ada di halaman surat keluar.



Gambar 43 - Interface Halaman Detail Surat Keluar (Atas)

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.

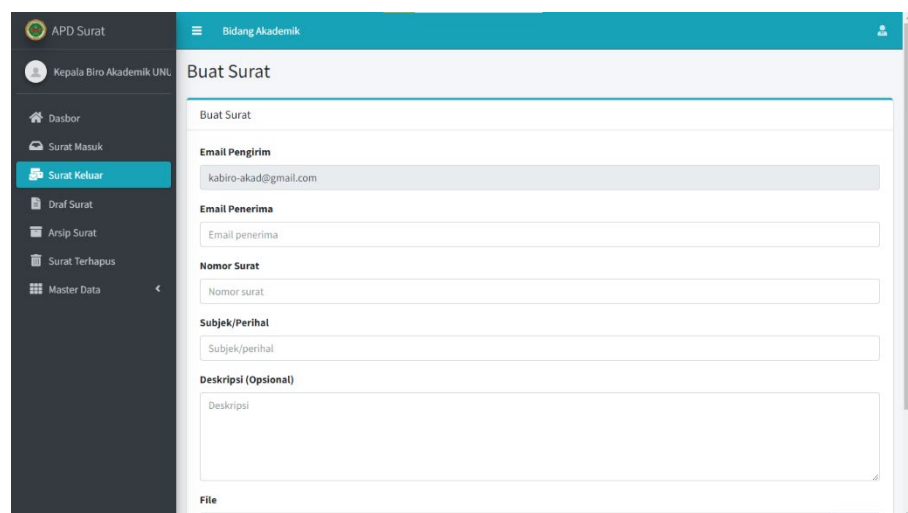


Gambar 44 - Interface Halaman Detail Surat Keluar (Bawah)

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.

g. Buat Surat

Halaman buat surat akan ditampilkan apabila pengguna menekan tombol buat surat yang ada pada halaman surat keluar.



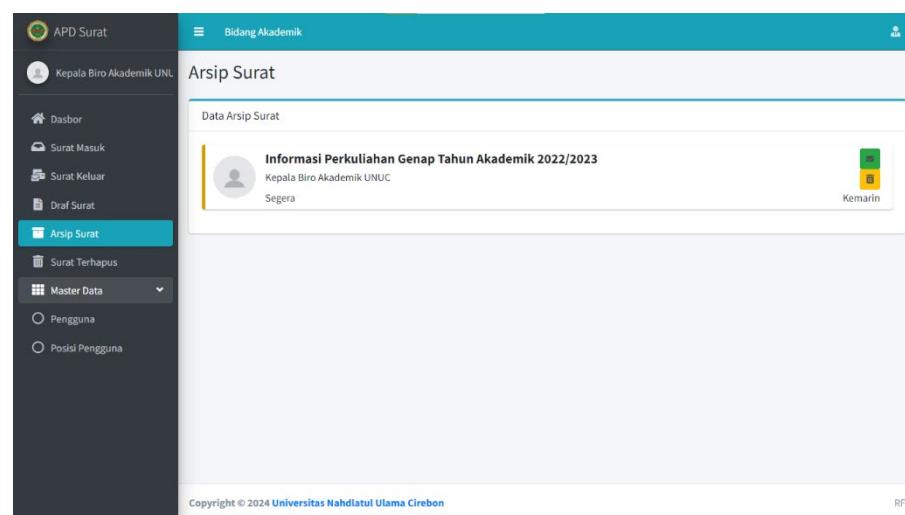
Gambar 45 - Interface Halaman Buat Surat

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.

h. Arsip Surat

Halaman arsip surat akan ditampilkan apabila pengguna menekan tombol arsip surat di halaman *dashboard* atau memilih menu arsip surat pada menu navigasi.

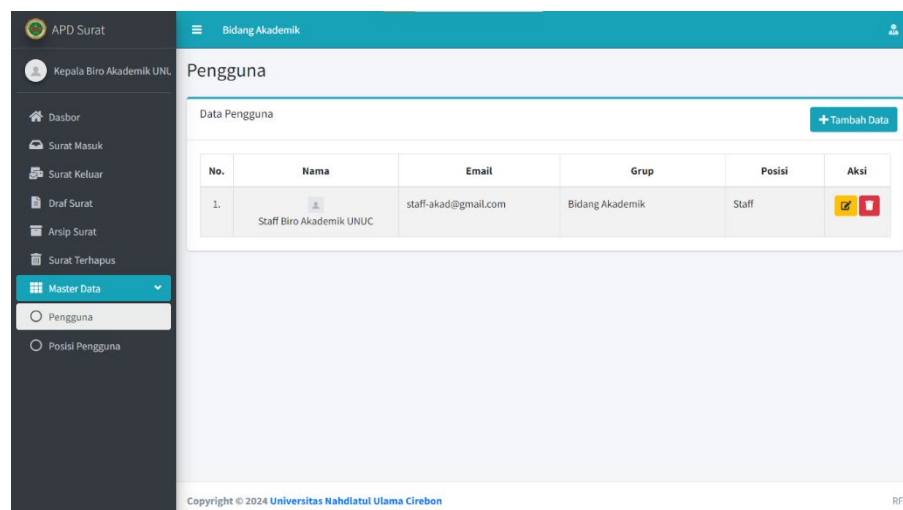


Gambar 46 - Interface Halaman Arsip Surat

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.

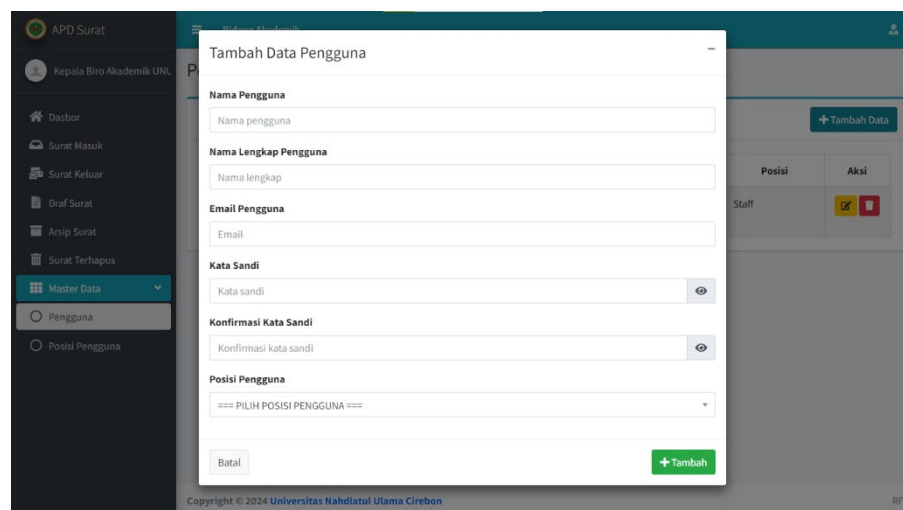
i. Kelola Pengguna

Halaman kelola pengguna akan ditampilkan apabila pengguna memilih menu pengguna pada menu navigasi. Menu pengguna hanya dapat diakses oleh pengguna yang memiliki hak akses admin, seperti kepala pimpinan.



Gambar 47 - Interface Halaman Data Pengguna

Pada halaman data pengguna ditampilkan daftar pengguna yang ada pada grup pengguna yang sama. Pada halaman ini, data pengguna dapat ditambahkan, diubah, maupun dihapus. Untuk menambah data pengguna dapat menekan tombol tambah data, dan kemudian ditampilkan formulir isian berupa data-data pengguna yang akan ditambahkan.



Gambar 48 - Interface Halaman Tambah Pengguna

Formulir isian yang harus diisi untuk menambahkan data pengguna di antaranya yaitu nama pengguna (*username*), nama lengkap pengguna, email pengguna, kata sandi (*password*), dan status posisi

pengguna. Daftar status posisi pengguna dapat dilihat pada menu navigasi posisi pengguna.

4.1.3. Implementasi Algoritma ECC

Algoritma ECC (*Elliptic Curve Cryptography*) diimplementasikan untuk membuat kunci pada proses enkripsi dan dekripsi data. Data yang dienkripsi berupa data pengguna dan data surat yang ada pada sistem administrasi disposisi surat ini.

Nama Pengguna	Kode Pengguna	Gambar Profil Pengguna	Nama Lengkap Pengguna
staff-akad		blank_profile.jpg	Staff Biro Akademik UNUC
staff-mhs	9wkuPKy1we1yPn4D	ZR1pd7WC2EI8rb3xCrQXIn005IIZOTZnEJ3gN+W3gA	K8L1JlpAdxgIfm6HEzBjsO5oFG9bCKjha+QM9UGAGmVUOsI
staff-kjs	1qjIC85PhygGe8xT	xwFm/Cbld6eL1QZ781o6jSEcG2klqMTVzvQ0sf5n/x	8Sp0lpUUIIACHra5E003AWccGWpAZEISjKj9ceD5m62dgF588V
staff-keu		blank_profile.jpg	Staff Biro Keuangan UNUC
warek1	7qfcGdJc3hteUAjQ	LAy46UxtSulZMITFAzBVcanXSb5pf+VfnzwVWmtKKUTN	6AlvPTZEGKdV5JxxR/AaJJzaQ7luAMdImy4TRC5VY2Hkp+w
warek2	9LmWBJB2amezTlvp	+gOT8gJ5M0A/1g1409OI8b9zJddlfmrA0QAwiWyN17I	0lVVqsk4sCkUykinJr+vlfPwxBaXtu8B1GoBCufXvMFX8
warek3		blank_profile.jpg	Wakil Rektor 3 UNUC
warek4		blank_profile.jpg	Wakil Rektor 4 UNUC

Gambar 49 - Interface Halaman Data Pengguna Terenkripsi

Pada gambar di atas, terdapat sampel pengguna yang dapat dijadikan bukti implementasi enkripsi dan dekripsi menggunakan algoritma ECC. Data pada baris ke-2, ke-3, ke-5, dan ke-6 adalah contoh data yang telah dienkripsi, sedangkan data pada baris ke-1, ke-4, ke-7, dan ke-8 adalah contoh data yang telah didekripsi.

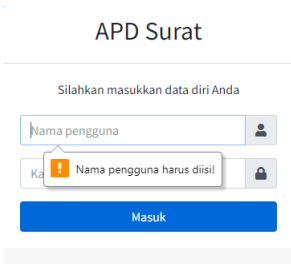
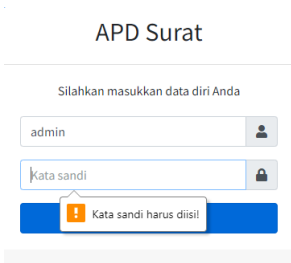
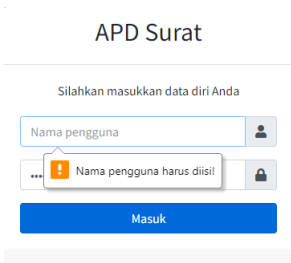
4.2. Pengujian

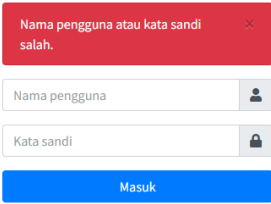
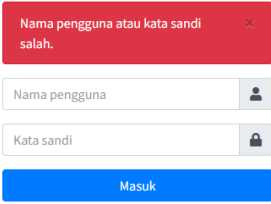
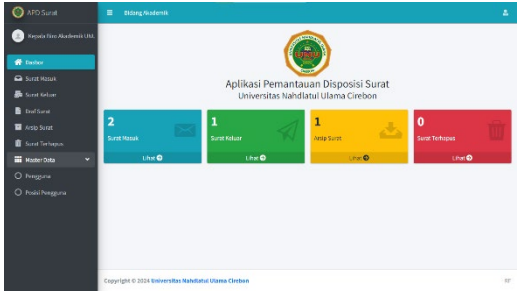
4.2.1. Pengujian Interface

Sistem administrasi disposisi surat diuji menggunakan metode *black box* untuk menguji skenario yang telah dirancang agar mendapatkan hasil yang diharapkan maupun yang tidak direncanakan.

a. *Login*

Tabel 16 - Pengujian Skenario Black Box - Login

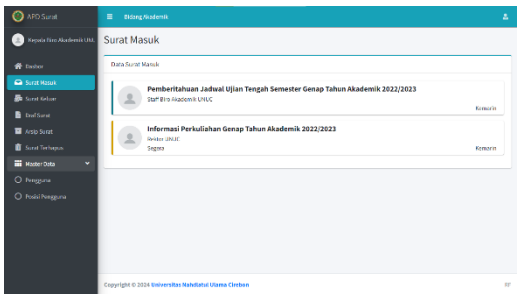
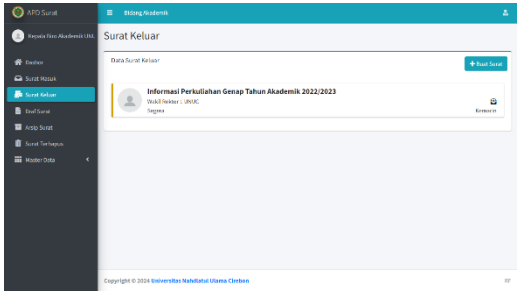
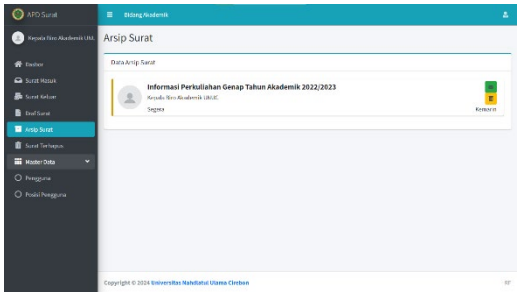
No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Formulir isian <i>login</i> kosong.	Muncul pesan isian harus diisi.	Sukses
			
2.	Mengisi isian <i>username</i> , tetapi mengosongkan isian <i>password</i> .	Muncul pesan isian harus diisi.	Sukses
			
3.	Mengisi isian <i>password</i> , tetapi mengosongkan isian <i>username</i> .	Muncul pesan isian harus diisi.	Sukses
			
4.	Mengisi isian <i>username</i> dan <i>password</i> dengan <i>username</i> tidak terdaftar.	Muncul pesan <i>username</i> atau <i>password</i> salah.	Sukses

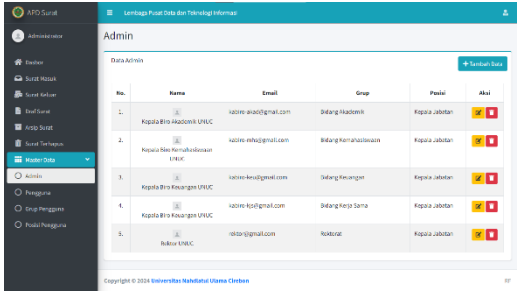
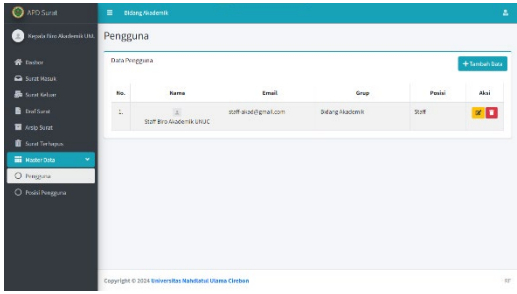
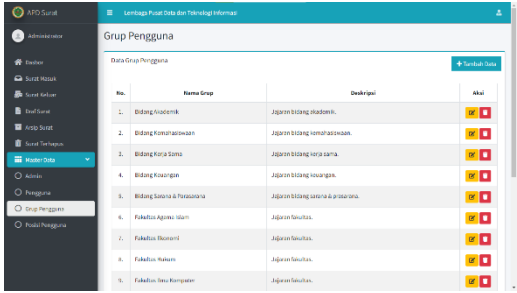
			
5.	Mengisi isian <i>username</i> dan <i>password</i> dengan <i>username</i> terdaftar dan <i>password</i> salah.	Muncul pesan <i>username</i> atau <i>password</i> salah.	Sukses
			
6.	Mengisi isian <i>username</i> dan <i>password</i> dengan <i>username</i> terdaftar dan <i>password</i> benar.	<i>Login</i> berhasil sesuai dengan hak akses dan diarahkan ke halaman <i>dashboard</i> .	Sukses
7.			
Total Hasil Pengujian Sukses			100%

Berdasarkan perancangan uji dan pengujian pada halaman *login* menunjukkan hasil sukses 100%.

b. *Dashboard*

Tabel 17 - Pengujian Skenario Black Box - Dashboard

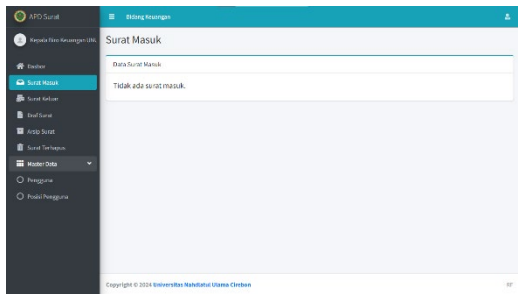
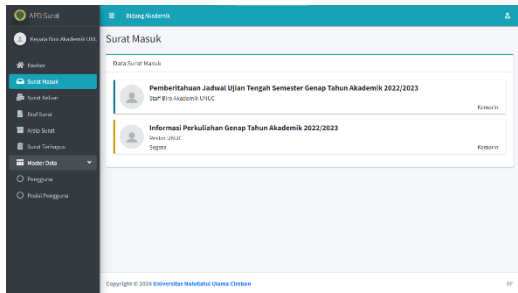
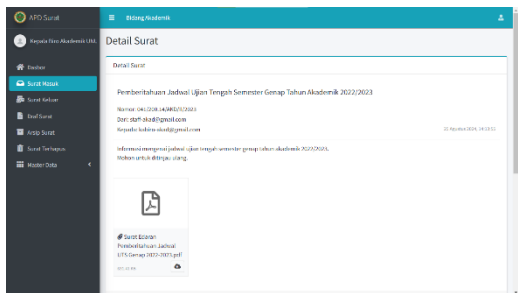
No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Pilih menu surat masuk.	Diarahkan ke halaman surat masuk.	Sukses
			
2.	Pilih menu surat keluar.	Diarahkan ke halaman surat keluar.	Sukses
			
3.	Pilih menu arsip surat.	Diarahkan ke halaman arsip surat.	Sukses
			
4.	Pilih menu admin, khusus untuk hak akses admin.	Diarahkan ke halaman admin.	Sukses

			
5.	Pilih menu pengguna, khusus untuk hak akses admin.	Diarahkan ke halaman pengguna.	Sukses
			
6.	Pilih menu grup pengguna, khusus untuk hak akses admin.	Diarahkan ke halaman grup pengguna.	Sukses
			
Total Hasil Pengujian Sukses			100%

Berdasarkan perancangan uji dan pengujian pada halaman *dashboard* menunjukkan hasil sukses 100%.

c. Surat Masuk

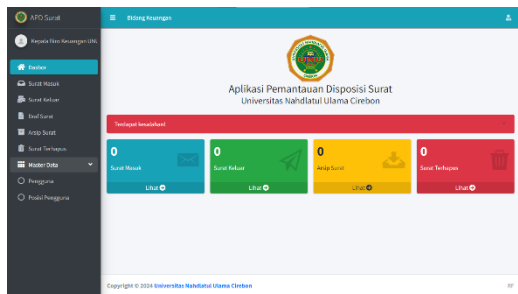
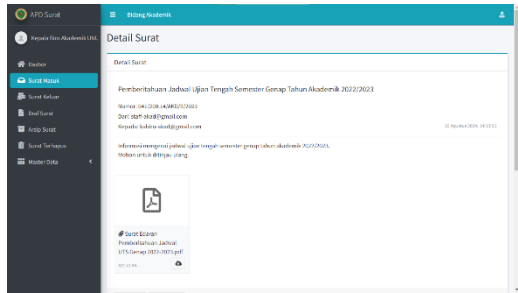
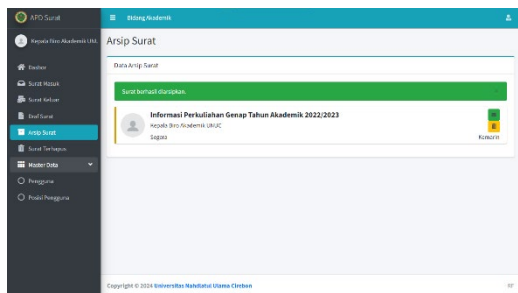
Tabel 18 - Pengujian Skenario Black Box - Surat Masuk

No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Tidak ada surat masuk.	Muncul halaman kosong.	Sukses
			
2.	Ada surat masuk.	Muncul daftar surat yang diterima pengguna.	Sukses
			
3.	Jika ada surat masuk, pilih surat.	Diarahkan ke halaman detail surat.	Sukses
			
Total Hasil Pengujian Sukses			100%

Berdasarkan perancangan uji dan pengujian pada halaman surat masuk menunjukkan hasil sukses 100%.

d. Lihat Surat

Tabel 19 - Pengujian Skenario Black Box - Lihat Surat

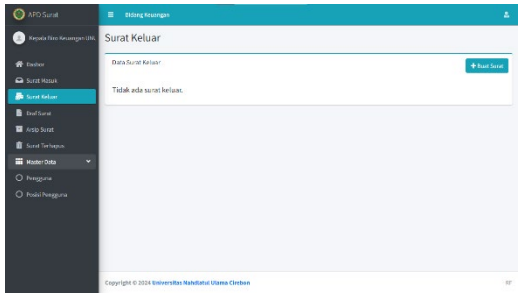
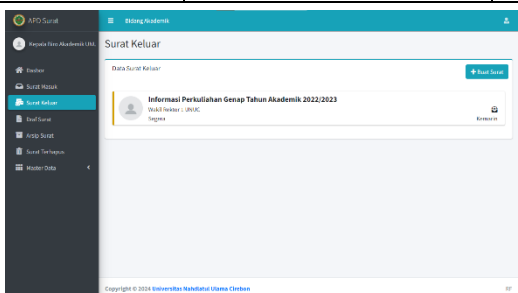
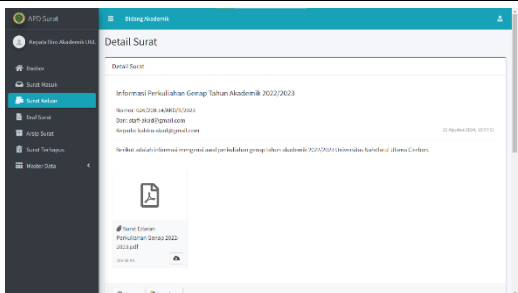
No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Surat dilihat oleh orang yang tidak berkepentingan.	Diarahkan ke halaman <i>dashboard</i> .	
			
2.	Surat dilihat oleh orang yang tepat.	Muncul detail surat yang dipilih.	Sukses
			
3.	Tekan tombol arsipkan.	Surat akan dipindah ke daftar arsip dan pengguna diarahkan ke halaman arsip.	Sukses
			

	isian komentar/tanggapan kosong, lalu tekan tombol surat diteruskan.		
	Terdapat Kesalahan Email tujuan tidak ditemukan!		
5.	Mengisi isian email tujuan dengan benar, isian komentar/tanggapan kosong, lalu tekan tombol surat diteruskan.	Surat dikirim kepada tujuan tanpa mengirim isi komentar/tanggapan.	Sukses
	 Kepala Biro Akademik UNUC 26 Agustus 2024, 09:06:36 > Surat ini diteruskan kepada Wakil Rektor 1 UNUC.		
6.	Mengisi isian email tujuan dengan benar, mengisi isian komentar/tanggapan, lalu tekan tombol surat diteruskan.	Surat dikirim kepada tujuan dengan mengirim isi komentar/tanggapan.	Sukses
	 Kepala Biro Akademik UNUC 25 Agustus 2024, 10:59:02 > Surat ini diteruskan kepada Wakil Rektor 1 UNUC. Mohon untuk ditanggapi.		
7.	Tekan tombol surat tidak disetujui.	Surat dikirim kepada pengirim surat dengan status surat ditolak.	Sukses
	 Wakil Rektor 1 UNUC 26 Agustus 2024, 13:09:12 > Surat ini ditolak oleh Wakil Rektor 1 UNUC.		
8.	Tekan tombol surat disetujui.	Surat dikirim kepada pengirim surat dengan status surat disetujui.	Sukses
	 Wakil Rektor 1 UNUC 26 Agustus 2024, 13:15:27 > Surat ini telah disetujui oleh Wakil Rektor 1 UNUC dan diteruskan kepada Kepala Biro Akademik UNUC.		
Total Hasil Pengujian Sukses			100%

Berdasarkan perancangan uji dan pengujian pada halaman tanggap surat menunjukkan hasil sukses 100%.

f. Surat Keluar

Tabel 21 - Pengujian Skenario Black Box - Surat Keluar

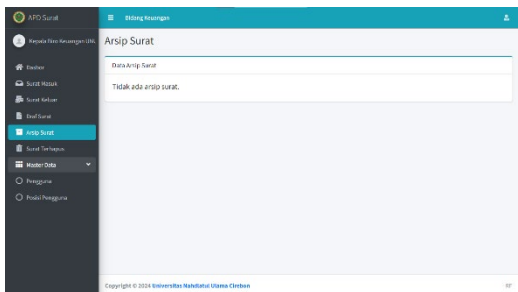
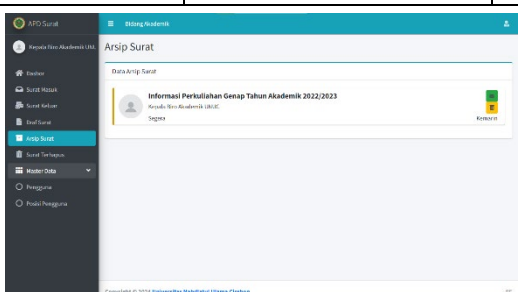
No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Tidak ada surat keluar.	Muncul halaman kosong.	Sukses
			
2.	Ada surat keluar.	Muncul daftar surat yang dikirim kepada pengguna lain.	Sukses
			
3.	Jika ada surat keluar, pilih surat.	Diarahkan ke halaman detail surat.	Sukses
			

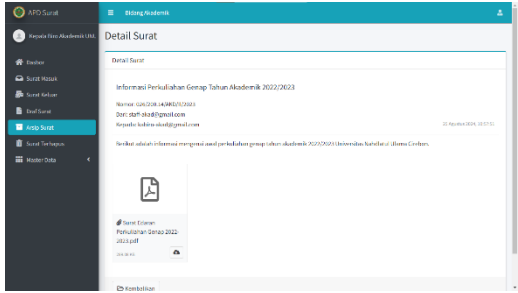
Total Hasil Pengujian Sukses	100%
-------------------------------------	-------------

Berdasarkan perancangan uji dan pengujian pada halaman surat keluar menunjukkan hasil sukses 100%.

g. Arsip Surat

Tabel 22 - Pengujian Skenario Black Box - Arsip Surat

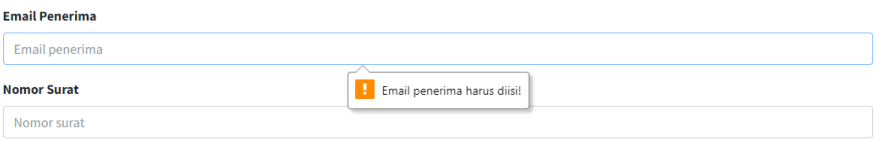
No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Tidak ada arsip surat.	Muncul halaman kosong.	Sukses
			
2.	Ada arsip surat.	Muncul daftar surat yang diarsipkan oleh pengguna.	Sukses
			
3.	Jika ada arsip surat, pilih surat.	Diarahkan ke halaman detail surat.	Sukses

	
Total Hasil Pengujian Sukses	
100%	

Berdasarkan perancangan uji dan pengujian pada halaman arsip surat menunjukkan hasil sukses 100%.

h. Buat Surat

Tabel 23 - Pengujian Skenario Black Box - Buat Surat

No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Formulir isian buat surat kosong, lalu tekan tombol kirim.	Muncul pesan isian harus diisi dan file harus dipilih.	Sukses
			
2.	Mengisi email tujuan yang salah (tidak terdaftar) dan mengosongkan isian lainnya, lalu tekan tombol kirim.	Muncul pesan email tidak terdaftar, isian harus diisi, dan file harus dipilih.	Sukses
			
3.	Mengisi isian email tujuan dengan benar, tetapi mengosongkan isian	Muncul pesan isian harus diisi dan file harus dipilih.	Sukses

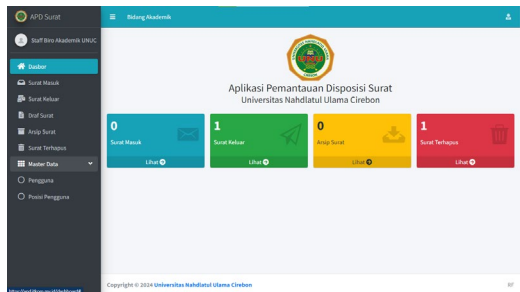
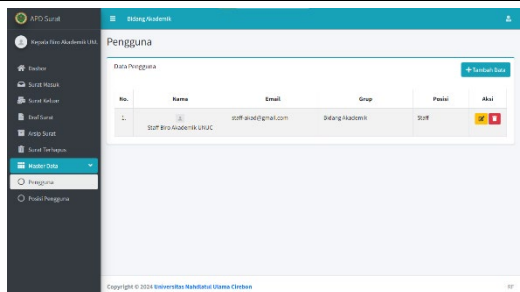
	lainnya, lalu tekan tombol kirim.		
	Terdapat Kesalahan - Nomor surat harus diisi! - Subjek/perihal harus diisi! - File harus diunggah!		
4.	Mengisi isian email tujuan dengan benar dan nomor surat, tetapi mengosongkan isian lainnya, lalu tekan tombol kirim.	Muncul pesan isian harus diisi dan file harus dipilih.	Sukses
	Terdapat Kesalahan - Subjek/perihal harus diisi! - File harus diunggah!		
5.	Mengisi isian email tujuan dengan benar, nomor surat, perihal surat, dan mengosongkan isian lainnya, lalu tekan tombol kirim.	Muncul pesan file harus dipilih.	Sukses
	Terdapat Kesalahan File harus diunggah!		
6.	Mengisi isian email tujuan dengan benar, nomor surat, perihal surat, dan memilih file bukan pdf, lalu tekan tombol kirim.	Muncul pesan file harus berformat PDF.	Sukses
	Terdapat Kesalahan File hanya boleh berekstensi PDF!		
7.	Mengisi isian email tujuan dengan benar, nomor surat, perihal surat, dan memilih file pdf, lalu tekan tombol kirim.	Surat dikirim kepada tujuan dalam bentuk terenkripsi.	Sukses

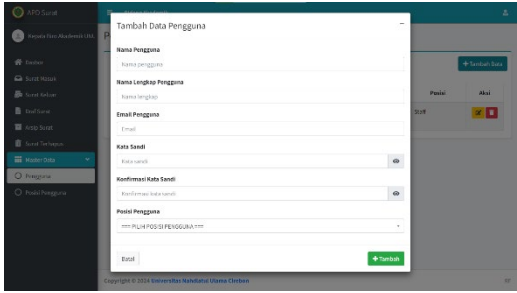
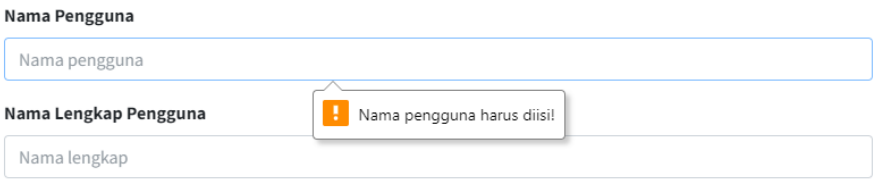
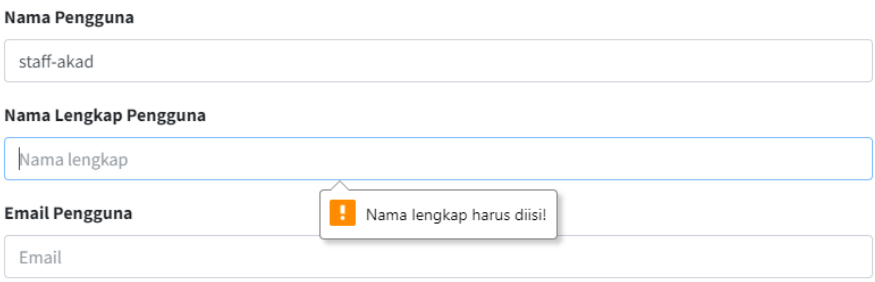
Surat berhasil dibuat dan dikirim.	
Total Hasil Pengujian Sukses	100%

Berdasarkan perancangan uji dan pengujian pada halaman buat surat menunjukkan hasil sukses 100%.

i. Kelola Pengguna

Tabel 24 - Pengujian Skenario Black Box - Kelola Pengguna

No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Jika pengguna tidak memiliki hak akses admin.	Diarahkan ke halaman <i>dashboard</i> .	Sukses
			
2.	Jika pengguna memiliki hak akses admin.	Muncul daftar pengguna.	Sukses
			
3.	Tekan tombol tambah pengguna.	Muncul formulir isian tambah pengguna.	Sukses

			
4.	Tekan tombol tambah pengguna, formulir isian kosong, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.	Sukses
			
5.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> , tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.	Sukses
			
6.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dan nama lengkap, tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.	

	Nama Pengguna staff-akad Nama Lengkap Pengguna Staff Biro Akademik UNUC Email Pengguna Email Kata Sandi Kata sandi ! Email tidak valid!		
7.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dan (format) email yang salah, tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi dan format email salah.	Sukses
	Nama Pengguna staff-akad Nama Lengkap Pengguna Staff Biro Akademik UNUC Email Pengguna staff@unuc.ac.id Kata Sandi Kata sandi ! Email tidak valid!		
8.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dan (format) email yang benar, tetapi mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.	Sukses

	Nama Pengguna staff-akad Nama Lengkap Pengguna Staff Biro Akademik UNUC Email Pengguna staff-akad@gmail.com Kata Sandi Kata sandi Konfirmasi Kata Sandi Konfirmasi kata sandi ! Kata sandi harus diisi!		
9.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i>, dan mengosongkan isian lainnya, lalu tekan tombol tambah.	Muncul pesan isian harus diisi.	Sukses
	Nama Pengguna staff-akad Email staff-akad@gmail.com Nama Lengkap Staff Biro Akademik UNUC Kata Sandi ***** Konfirmasi Kata Sandi ***** Grup Pengguna === PILIH GRUP PENGGUNA === ! Grup pengguna harus dipilih!		
10.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i>, grup pengguna, dengan	Muncul pesan <i>username</i> telah terdaftar.	Sukses

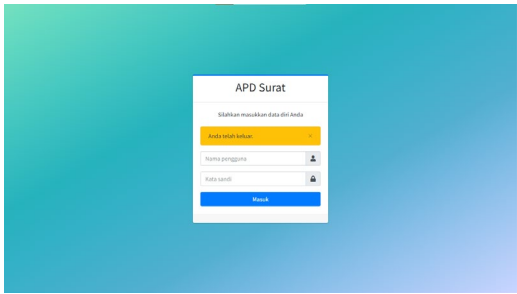
	<i>username</i> yang telah terdaftar, lalu tekan tombol tambah.		
			
11.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i> , grup pengguna, dengan email yang telah terdaftar, lalu tekan tombol tambah.	Muncul pesan email telah terdaftar.	Sukses
			
12.	Tekan tombol tambah pengguna, mengisi isian <i>username</i> dengan (format) email yang benar, <i>password</i> , grup pengguna, lalu tekan tombol tambah.	Muncul pesan berhasil ditambahkan.	Sukses
			
Total Hasil Pengujian Sukses			100%

Berdasarkan perancangan uji dan pengujian pada halaman kelola pengguna menunjukkan hasil sukses 100%.

j. *Logout*

Tabel 25 - Pengujian Skenario Black Box - Logout

No.	Kasus Uji	Hasil yang Diharapkan	Hasil Pengujian
1.	Tekan tombol <i>logout</i> .	Sesi pengguna akan berakhir dan	Sukses

		diarahkan ke halaman <i>login</i> .	
			
Total Hasil Pengujian Sukses			100%

Berdasarkan perancangan uji dan pengujian pada fungsi *logout* menunjukkan hasil sukses 100%.

4.2.2. Pengujian Algoritma ECC

Pengujian algoritma *Elliptic Curve Cryptography* (ECC) dilakukan dengan menghitung waktu yang dibutuhkan untuk pembuatan kunci, enkripsi, dan dekripsi. Pengujian dilakukan terhadap kata “Rumah” (5 karakter), “Indonesia” (9 karakter), “Fakultas Ilmu Komputer” (22 karakter), “Universitas Nahdlatul Ulama Cirebon” (35 karakter), “*Lorem ipsum dolor sit amet consectetur adipisicing elit.*” (56 karakter), dan “*Suscipit adipisci, pariatur, in deserunt iusto aliquam, non culpa ex repellendus tenetur asperiores cupiditate porro odit illum! Optio facilis repellendus sit praesentium?*” (171 karakter). Setiap kata diuji sebanyak 20 (dua puluh) kali untuk mendapatkan hasil rata-rata pengujian.

Berikut ini merupakan hasil rata-rata pengujian mulai dari proses pembangkitan kunci hingga proses enkripsi dan dekripsi menggunakan algoritma ECC, yaitu sebagai berikut:

Tabel 26 - Pengujian Algoritma ECC

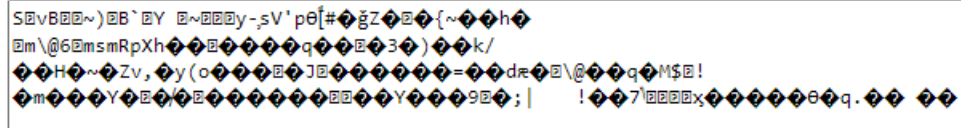
No.	Kalimat	Panjang Karakter	Pembangkitan Kunci	Enkripsi	Dekripsi
1.	Rumah	5	0.00134 ms	0.16575 ms	0.17611 ms
2.	Indonesia	9	0.00181 ms	0.17772 ms	0.18805 ms
3.	Fakultas Ilmu Komputer	22	0.00193 ms	0.20186 ms	0.18241 ms
4.	Universitas Nahdlatul Ulama Cirebon	35	0.00197 ms	0.18576 ms	0.18896 ms
5.	<i>Lorem ipsum dolor sit amet consectetur adipiscing elit.</i>	56	0.00216 ms	0.18131 ms	0.1876 ms
6.	<i>Suscipit adipisci, pariatur, in deserunt iusto aliquam, non culpa ex repellendus tenetur asperiores cupiditate porro odit illum! Optio facilis repellendus sit praesentium?</i>	171	0.00218 ms	0.28014 ms	0.25866 ms

Berdasarkan pengujian pada perhitungan lama waktu mulai dari proses pembangkitan kunci, proses enkripsi, dan proses dekripsi diperoleh hasil yang tidak jauh berbeda. Pada kalimat dengan panjang 171 karakter, waktu minimal yang diperoleh pada proses pembangkitan kunci adalah 0.0095 ms, sedangkan waktu maksimal yang diperoleh adalah 0.00787 ms. Pada proses enkripsi,

waktu minimal yang diperoleh adalah 0.22197 ms dan waktu maksimal yang diperoleh adalah 0.85211 ms. Serta pada proses dekripsi, waktu minimal yang diperoleh adalah 0.22197 ms dan waktu maksimal yang diperoleh adalah 0.44298 ms.

Size Encrypted Message: 187

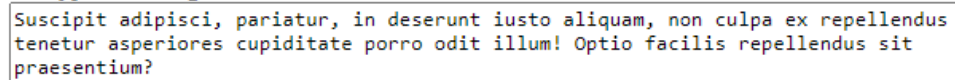
Encrypted Message:



S@vB@~)@B`@Y @~@y-sV'p@[#@gZ@{~@h@
 @m\@6@msmRpXh@@@q@@@3@)@k/
 @H@~@Zv,@y(o@@@@@J@@@@@=@@d@#@@@q@M\$@!
 @m@@@@Y@@@Y@@@@@9@;| !@@7@@@@x@@@@@6@q.@@@

Gambar 50 - Hasil Enkripsi

Decrypted Message:



Suscipit adipisci, pariatur, in deserunt iusto aliquam, non culpa ex repellendus
 tenetur asperiores cupiditate porro odit illum! Optio facilis repellendus sit
 praesentium?

Gambar 51 - Hasil Dekripsi

BAB V

KESIMPULAN DAN SARAN

5.1. 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.
4. Sistem administrasi disposisi surat berbasis *website* dapat menjadi solusi yang efektif dan dapat meningkatkan keamanan data pada sistem dengan menerapkan algoritma enkripsi.

5.2. Saran

Sistem administrasi disposisi persuratan pada penelitian ini masih memerlukan pengembangan lebih lanjut, baik dari segi tampilan maupun fitur yang terdapat di dalamnya. Penulis menyarankan untuk lebih menjadikan tampilan sistem yang *real time* tanpa perlu melakukan *refresh* halaman untuk setiap pembaruan surat yang masuk maupun keluar. Disarankan juga untuk menambahkan fitur pencarian untuk memudahkan pengguna menemukan surat yang ingin dicari.

DAFTAR PUSTAKA

- Akion. (2024, Maret 26). Sistem Informasi Administrasi Surat Menyurat Keendudukan di Kelurahan dengan Metode Chronological Filling System. *Jurnal Multidisiplin Saintek*, *II*(10), 111-136. doi:<https://doi.org/10.3785/kohesi.v2i10.2669>
- 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 Menggunakan 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>
- Arif, Z., & Nurokhman, A. (2022, September 22). Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris dalam Meningkatkan Keamanan Sistem Informasi. *Jurnal Teknologi Sistem Informasi*, *IV*(2), 394-405. doi:<https://doi.org/10.35957/jtsi.v4i2.6077>
- Badan Pengembangan dan Pembinaan Bahasa. (2023, Oktober). *KBBI VI Daring*, 3.11.1.0-20240115111814. Dipetik Februari 1, 2024, dari KBBI VI Daring - Disposisi: <https://kbbi.kemdikbud.go.id/entri/disposisi>
- Bintara, W. S. (2023, Oktober 22). *Pengertian Microsoft Visio - Fungsi, Fitur, Kelebihan*. Diambil kembali dari Dianisa: <https://dianisa.com/pengertian-microsoft-visio/>
- Damanik, P. S. (2019, Agustus). Implementasi Algoritma Elliptic Curve Cryptography (ECC) Untuk Penyandian Pesan Pada Aplikasi Chatting Client Server Berbasis Desktop. *Jurnal Riset Komputer*, *VI*(4), 395-400. doi:<http://dx.doi.org/10.30865/jurikom.v6i4.1398>

- Damanik, P. S. (2019). Implementasi Algoritma Elliptic Curve Cryptography (ECC) Untuk Penyandian Pesan Pada Aplikasi Chatting Client Server Berbasis Desktop. *Jurnal Riset Komputer (JURIKOM)*, 395-400.
- Dicoding Intern. (2021, Mei 19). *Contoh Use Case Diagram Lengkap dengan Penjelasannya*. Diambil kembali dari Dicoding Blog: <https://www.dicoding.com/blog/contoh-use-case-diagram/>
- Dicoding Intern. (2023, Juli 5). *Apa Itu Activity Diagram? Simak Contoh Implementasinya Berikut Ini!* Diambil kembali dari Dicoding Blog: <https://www.dicoding.com/blog/apa-itu-activity-diagram-simak-contoh-implementasinya-berikut-ini/>
- Fajrin, A. M., Benedict, J. R., & Kusuma, H. J. (2023, Februari 27). Analisis Performa dari Algoritma Kriptografi RSA dan ElGamal dalam Enkripsi dan Dekripsi Pesan. *Jurnal Riset Sistem Informasi dan Teknik Informatika*, VIII(1), 91-98. Diambil kembali dari <https://drive.google.com/file/d/1xa01RxxmthB90dHixNBtJi-UBZrUwixt/view>
- Faulina, A. R. (2023, Maret 23). *Apa itu UML? Ini Pengertian, Fungsi, dan Contohnya*. Diambil kembali dari Sekawan Media: <https://www.sekawanmedia.co.id/blog/apa-itu-uml/>
- Hermawan, A., & Ujianto, E. I. (2021, Februari 22). Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA. *Jurnal Nasional Informatika dan Teknologi Jaringan*, V(2), 325-330. doi:<https://doi.org/10.30743/infotekjar.v5i2.3585>
- Herpendi, Fathurrahmani, & Hafidz, K. A. (2022, Desember 16). Mobile Letter (Aplikasi Disposisi Surat dan Telaah Staf Berbasis Mobile). *Seminar Nasional Teknologi dan Multidisiplin Ilmu*, II(1), 68-76. doi:<https://doi.org/10.51903/semnastekmu.v2i1.155>
- Ignasius, A., & Sakti, D. V. (2022, Januari 28). Penerapan Algoritma AES (Advanced Encryption Standard) 128 Untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi. *Jurnal Sistem Komputer dan Teknik Informatika*, V(1), 1-10. doi:<https://doi.org/10.36080/skanika.v5i1.2118>

- 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>
- Martani, A., M, S., & Ikhsan, N. (2022, Juni 28). Design and Build a Company Profile Website Based on the Bootstrap Framework and CodeIgniter Framework at the FoundationIndependent Scholar Caliph. *Jurnal Multidisiplin Madani*, *II*(6), 2895-2912. doi:<https://doi.org/10.55927/mudima.v2i6.510>
- Mubarok, A., Purnomo, E., & Noor, C. M. (2019, Agustus 15). Pengembangan Aplikasi Pembayaran Sumbangan Pengembangan Pendidikan Berbasis Web. *Jurnal Responsif Riset Sains dan Informatika*, *I*(1), 6-15. doi:<https://doi.org/10.51977/jti.v1i1.60>
- Noviantoro, a., Silviana, A. B., Fitriani, R. R., & Permatasari, H. P. (2022, Juni 21). Rancangan dan Implementasi Aplikasi Sewa Lapangan Badminton Wilayah Depok berbasis Web. *Jurnal Teknik dan Science*, *I*(2), 88-103. doi:<https://doi.org/10.56127/jts.v1i2.108>
- Oktaviani, E., Rodianto, Noviana, S., & Nawassyarif. (2020, Agustus 29). Rancang Bangun Sistem Informasi untuk Meningkatkan Tata Kelola Administrasi Surat Menyurat. *Jurnal Informatika Teknologi dan Sains*, *II*(3), 203-207. doi:<https://doi.org/10.51401/jinteks.v2i3.757>
- Pratiwi, U., Wijaya, K., & Fajriyah. (2021, November 23). Penerapan Metode Prototype Pada Perancangan Sistem Administrasi Pembayaran Karate Berbasis Website: Studi Kasus Lemkari Prabumulih. *Jurnal Pengembangan Sistem Informasi dan Informatika*, *II*(3), 157-173. doi:<https://doi.org/10.47747/jpsii.v2i3.563>
- 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.dipaneegara.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>
- Ramadhani, F., Sari, I. P., & Satria, A. (2023, Oktober 11). Perancangan UI/UX Surat Keterangan Waris dalam Pengembalian Dana Haji Berbasis Web. *Jurnal Teknik*, *II*(3), 198-203. doi:<https://doi.org/10.56211/blendsains.v2i3.306>
- Santi, E. (2024, Apr 20). *VSCODE Adalah – Pengertian, Fitur, Kelebihan, dan Cara Menggunakannya*. Diambil kembali dari IDwebhost: <https://idwebhost.com/blog/vscode-adalah/>
- Sari, I. P., Syahputra, A., Zaky, N., Sibuea, R. U., & Zakhir, Z. (2022, Juni 30). Perancangan Sistem Aplikasi Penjualan dan Layanan Jasa Laundry Sepatu Berbasis Website. *Jurnal Teknik*, *I*(1), 31-37. doi:<https://doi.org/10.56211/blendsains.v1i1.67>
- Setiawan, R. (2021, Agustus 21). *Apa Itu Sequence Diagram dan Contohnya*. Diambil kembali dari Dicoding Blog: <https://www.dicoding.com/blog/apa-itu-sequence-diagram/>
- Setiawan, R. (2021, Oktober 13). *Memahami Class Diagram Lebih Baik*. Diambil kembali dari Dicoding Blog: <https://www.dicoding.com/blog/memahami-class-diagram-lebih-baik/>
- 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>
- Ula, M., Risawandi, & Rosdian. (2019, April). Sistem Pengenalan dan Penerjemahan Al-Qur'an Surah Al-Waqi'ah melalui Suara Menggunakan

- Transformasi Sumudu. *TECHSI*, 104-113.
doi:<https://doi.org/10.29103/techsi.v1i1.1294>
- Uly, A. C. (2024, Juli 14). *Apa Itu Apache? Pengertian Apache Serta Kelebihan dan Kekurangannya*. Diambil kembali dari Hostinger:
<https://www.hostinger.co.id/tutorial/apa-itu-apache>
- UPT TIK. (2023, Desember 11). *Mengenai Balsamiq, Aplikasi Wireframe Untuk Pemula*. Diambil kembali dari undiksha:
<https://upttik.undiksha.ac.id/mengenai-balsamiq/>
- Yusman, Y., & Harahap, S. P. (2020, Januari 8). Implementasi Website Alumni pada SMP PGRI 1 Padang. *Community Engagement & Emergence*, *I*(1), 27-29. doi:<https://doi.org/10.37385/ceej.v1i1.44>
- Yusuf, F., Muin, A. A., & Nisrawati. (2022, Juni 30). Rancang Bangun Aplikasi Disposisi Persuratan Berbasis Mobile Apps. *Journal Software, Hardware, and Information Technology*, *II*(2), 21-31.
doi:<https://doi.org/10.24252/shift.v2i2.32>
- Yusuf, F., Muin, A. A., & Nisrawati. (2022, Juni 30). Rancang Bangun Aplikasi Disposisi Persuratan Berbasis Mobile Apps. *SHIFT*, *II*(2), 21-31.
doi:<https://doi.org/10.24252/shift.v2i2.32>