PENGAMANAN DISTRIBUSI DATA KEPEGAWAIAN PADA BADAN KEPEGAWAIAN SUMATERA UTARA DENGAN MEMANFAATKAN ALGORITMA KRIPTOGRAFI ASIMETRIS RSA

SKRIPSI

DISUSUN OLEH

NOPRIAN SYAHPUTRA
NPM. 2009010093

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2024

PENGAMANAN DISTRIBUSI DATA KEPEGAWAIAN PADA BADAN KEPEGAWAIAN SUMATERA UTARA DENGAN MEMANFAATKAN ALGORITMA KRIPTOGRAFI ASIMETRIS RSA

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara

NOPRIAN SYAHPUTRA
NPM. 2009010093

PROGRAM STUDI STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2024

LEMBAR PENGESAHAN

Judul Skripsi	:	PENGAMANAN DISTRIBUSI DATA KEPEGAWAIAN PADA BADAN KEPEGAWAIAN SUMATERA UTARA DENGAN MEMANFAATKAN ALGORITMA KRIPTOGRAFI ASIMETRIS RSA
Nama Mahasiswa	:	NOPRIAN SYAHPUTRA
NPM	:	2009010093
Program Studi	:	SISTEM INFORMASI

Menyetujui
Komisi Pembimbing

(Ferdy Riza ST, M.Kom)
NIDN. 0103068901

Ketua Program Studi

(Martiano S.Pd, S.Kom., M.Kom)
NIDN. 0128029302

Dekan

(Dr. Al-Khowarizmi, S.Kom., M.Kom.)
NIDN. 0127099201

PERNYATAAN ORISINALITAS

PENGAMANAN DISTRIBUSI DATA KEPEGAWAIAN PADA BADAN KEPEGAWAIAN SUMATERA UTARA DENGAN MEMANFAATKAN ALGORITMA KRIPTOGRAFI ASIMETRIS RSA

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, 12 November 2024

Yang membuat pernyataan

Noprian Syahputra

NPM. 2009010093

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Noprian Syahputra
NPM	: 2009010093
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif *(Non-Exclusive Royalty free Right)* atas penelitian skripsi saya yang berjudul:

PENGAMANAN DISTRIBUSI DATA KEPEGAWAIAN PADA BADAN KEPEGAWAIAN SUMATERA UTARA DENGAN MEMANFAATKAN ALGORITMA KRIPTOGRAFI ASIMETRIS

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, 12 November 2024
Yang membuat pernyataa

Noprian Syahputra
NPM. 2009010093

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Noprian Syahputra
Tempat dan Tanggal Lahir	: Sei Alim Ulu, 12 Oktber 1999
Alamat Rumah	: Dusun II, Desa Sei Alim Ulu
Telepon/Faks/HP	: 082273329460
E-mail	: riannopriansyahputra@gmail.com
Instansi Tempat Kerja	: -
Alamat Kantor	: -

DATA PENDIDIKAN

SD	: SD Negeri 010047 Sei Alim Ulu	TAMAT: 2013
SMP	: SMP Swasta Daerah Air Batu	TAMAT: 2016
SMA	: SMA Negeri 1 Pulau Rakyat	TAMAT: 2019

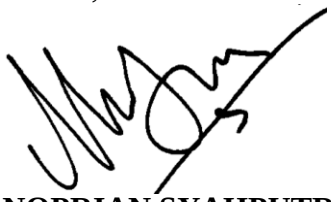
KATA PENGANTAR

Dengan rasa bersyukur kepada Tuhan Yang Maha Esa atas limpahan kasih- Nya, petunjuk-Nya, dan anugerah-Nya kepada kita semua, kami berhasilmenyelesaikan tugas akhir berjudul "**Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA**". Penulis tentunya berterima kasih kepada berbagai pihakdalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucap terima kasih kepada:

1. Bapak Prof. Dr. Agussani, M.AP., selaku Rektor Universitas MuhammadiyahSumatera Utara (UMSU)
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom selaku Dekan Fakultas IlmuKomputer dan Teknologi Informasi (FIKTI) UMSU.
3. Bapak Martiano, S.Pd, S.Kom., M.Kom selaku Ketua Program Studi SistemInformasi
4. Ibu Yoshida Sary, S.E., S.Kom., M.Kom selaku Sekretaris Program Studi Sistem Informasi
5. Bapak Ferdy Riza, ST, M.Kom selaku Dosen Pembimbing yang telah memberikan arahan dan bimbingan kepada penulis.
6. Bapak dan ibu dosen Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara yang telah memberikan banyak bekal ilmu kepada penulis.
7. Bapak dan Ibu Pimpinan dan seluruh staff Pegawai yang ada di Badan Kepegawaian Provinsi Sumatera Utara yang telah memberikan izin dan informasi yang tidak bisa penulis sebut namanya satu persatu.
8. Keluarga besar kedua orang tua yang saya cintai, saudara-saudara kami, atas doa, bimbingan, serta kasih sayang yang selalu tercurah selama ini.
9. Dan teman-teman seperjuangan kami di Jurusan Sistem Informasi, atas semua dukungan, semangat, serta kerjasamanya.

Saya selaku penulis menyadari di dalam penulisan skripsi ini masih banyak kekurangan. Oleh karena itu saya mengucapkan terima kasih banyak kepada semua pihak, semoga Allah SWT melimpahkan Rahmat-Nya kepada kita semua, semoga kiranya senantiasa membalas segala kabaikan kita semua. Aamiin.

Medan, 12 November2024



NOPRIAN SYAHPUTRA

PENGAMANAN DISTRIBUSI DATA KEPEGAWAIAN PADA BADAN KEPEGAWAIAN SUMATERA UTARA DENGAN MEMANFAATKAN ALGORITMA KRIPTOGRAFI ASIMETRIS

ABSTRAK

Dalam konteks penelitian ini, kami akan mengeksplorasi implementasi algoritma RSA untuk meningkatkan keamanan distribusi data kepegawaian pada BKPSU. Pendekatan ini akan memberikan perlindungan tambahan terhadap data sensitif, sehingga meningkatkan kepercayaan publik dan memenuhi standar keamanan yang ditetapkan. Untuk mengatasi masalah tersebut, diperlukan implementasi sistem keamanan yang kokoh dan dapat diandalkan. Salah satu solusi yang disarankan adalah menggunakan algoritma kriptografi asimetris RSA (Rivest-Shamir-Adleman). Dengan menerapkan algoritma ini, data kepegawaian dapat dienkripsi secara aman sehingga hanya pihak yang berwenang yang dapat membaca informasi tersebut. Dengan menggunakan algoritma RSA, keamanan data dapat dijamin karena sulit bagi peretas untuk mencari tahu kunci privat yang sesuai dengan kunci publik yang digunakan untuk enkripsi.

Kata Kunci : Keamanan, RSA, VB

SECURING THE DISTRIBUTION OF PERSONNEL DATA IN THE NORTH SUMATRA PERSONNEL AGENCY BY UTILIZING AN ASYMMETRIC CRYPTOGRAPHY ALGORITHM

ABSTRACT

In the context of this research, we will explore the implementation of the RSA algorithm to improve the security of personnel data distribution at BKPSU. This approach will provide additional protection to sensitive data, thereby increasing public trust and meeting established security standards. To overcome this problem, it is necessary to implement a strong and reliable security system. One suggested solution is to use the RSA (Rivest-Shamir-Adleman) asymmetric cryptographic algorithm. By implementing this algorithm, personnel data can be encrypted securely so that only authorized parties can read the information. By using the RSA algorithm, data security can be guaranteed because it is difficult for hackers to find out which private key corresponds to the public key used for encryption.

***Keywords**: Security, RSA, VB*

DAFTAR ISI

DAFTAR TABEL

HALAMAN

DAFTAR GAMBAR

HALAMAN

BAB I
PENDAHULUAN

1.1.Latar Belakang Masalah

Dalam dunia digital modern ini, keamanan data merupakan aspek krusial yang harus diperhatikan oleh organisasi, terutama dalam konteks data kepegawaian di lembaga publik seperti BKPSU. Dengan semakin banyaknya insiden keamanan data yang terjadi, perlindungan terhadap informasi kepegawaian tidak boleh diabaikan. Algoritma kriptografi asimetris RSA menawarkan pendekatan yang kuat untuk mengamankan data dengan menggunakan kunci publik dan pribadi yang berbeda. Dalam konteks penelitian ini, kami akan mengeksplorasi implementasi algoritma RSA untuk meningkatkan keamanan distribusi data kepegawaian pada BKPSU. Pendekatan ini akan memberikan perlindungan tambahan terhadap data sensitif, sehingga meningkatkan kepercayaan publik dan memenuhi standar keamanan yang ditetapkan. (Doe, J. (2022).

Untuk mennyelesaikan masalah tersebut, dibutuhkan implementasi sistem keamanan yang kokoh dan dapat diandalkan. Salah satu solusi yang disarankan adalah menggunakan algoritma kriptografi asimetris RSA (Rivest-Shamir-Adleman). Dengan menerapkan algoritma ini, data kepegawaian dapat dienkripsi secara aman sehingga hanya kelompok yang berwenang yang mampu mengakses informasi tersebut. (L. Adleman,2022)

Algoritma kriptografi asimetris RSA tergolongkan salah satu algoritma

kriptografi yang paling lazim digunakan untuk mengenkripsi dan mendekripsi data. Algoritma ini menggunakan kombinasi kunci publik dan kunci privat, di mana kunci publik berfungsi mengenkripsi data, sementara kunci privat digunakan untuk dekripsi. Dengan penerapan algoritma RSA, data menjadi lebih aman karena sulit bagi peretas untuk mencari tahu kunci privat yang sesuai dengan kunci publik yang digunakan untuk enkripsi.

Implementasi algoritma kriptografi RSA pada sistem distribusi data kepegawaian di BKPSU diharapkan dapat memberikan perlindungan yang efektif terhadap informasi sensitif. Dengan demikian, pegawai dan data kepegawaian BKPSU akan terlindungi dari ancaman peretasan dan pencurian informasi. Secara umum, kriptografi menggunakan dua teknik, yaitu simetris dan asimetris. Dalam kriptografi simetris, yang juga dikenal sebagai Private Key Cryptography, digunakan satu kunci yang sama untuk proses enkripsi dan dekripsi data (Ferdy Riza, 2018).

Berdasarkan permasalahan diatas, penulis tertarik untuk melakukan penelitian dengan judul **"Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA**".

1.2.Rumusan Masalah

Berdasarkan uraian latar belakang diatas, permasalahan yang akan dibahas dalam penelitian ini mencakup hal-hal berikut:

1. Bagaimana merancang sistem dalam mengamankan file teks dengan

algoritma RSA.

2. Bagaimana mengimplementasikan algoritma RSA dalam skema enkripsi untuk pengamanan data.
3. Bagaimana mengukur keberhasilan dan efektivitas implementasi RSA dalam menjaga keamanan data kepegawaian di BKPSU.

1.3.Batasan Masalah

Dalam melaksanakan penelitian ini, peneliti membatasi ruang masalah yang akan diteliti. Batasan-batasan masalah yang dipergunakan yaitu :

1. Penulis hanya menggunakan data excel sebagai input dan menghasilkan hasil output dengan bentuk excel juga.
2. Algoritma kriptografi yang dalam skema enkripsi yaitu algoritma RSA, dengan menggunakan jenis kunci asimetris.
3. Bahasa pemrograman yang diterapkan untuk menyelesaian penelitian ini Visual Studio.

1.4.Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk mengetahui proses enkripsi dan dekripsi pesan teks menggunakan skema enkripsi.
2. Untuk menerapkan algoritma RSA dalam skema enkripsi untuk pengamanan data.
3. Untuk merancang sebuah sistem keamanan dalam mengamankan data

kepegawaian provinsi sumatera utara dengan menggunakan algoritma RSA.

1.5.Manfaat Penelitian

Penelitian ini bertujuan untuk menghasilkan pemahaman yang mendalam tentang implementasi algoritma kriptografi asimetris RSA dalam pengamanan distribusi data kepegawaian di BKPSU, antara lain :

1. Bagi Peneliti

   Memberikan kontribusi pada pengetahuan dalam bidang keamanan data dan kriptografi. Temuan dan metodologi yang dikembangkan dalam penelitian ini dapat menjadi sumbangan berharga bagi literatur ilmiah dan masyarakat akademis yang tertarik pada topik tersebut.

2. Bagi Badan Kepegawaian Provinsi Sumatera Utara

   Data-data krusial milik badan kepegawaian bisa diamankan secara sistem sehingga para peretas atau penyadap tidak bisa langsung menggunakan data jika terjadi pencurian data.

3. Bagi Universitas

   Penelitian ini juga diharapkan dapat menambah bahan referensi yang bermanfaat bagi Universitas Muhammadiyah Sumatera Utara (UMSU), khususnya pada Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi.

BAB II
KAJIAN PUSTAKA

2.1.Landasan Teori

2.1.1. Pengamanan Data Kepegawaian

Pengamanan data kepegawaian menjadi isu krusial dalam setiap lembaga pemerintahan, termasuk Badan Kepegawaian Provinsi Sumatera Utara. Data kepegawaian mengandung informasi sensitif seperti identitas personal, riwayat pekerjaan, dan informasi lainnya yang harus dilindungi dari akses yang tidak sah. Implementasi sistem pengamanan yang efektif menjadi prioritas utama dalam menjaga kerahasiaan dan integritas data kepegawaian.

2.1.2. Aplikasi

Aplikasi adalah program siap pakai yang dapat menjalankan perintah pengguna untuk menghasilkan output yang akurat sesuai tujuan pembuatannya. Aplikasi ini dirancang sebagai solusi pemrosesan data yang diharapkan, biasanya berfokus pada komputasi atau pemrosesan data yang spesifik (Ari Setiaji, dkk : 2021).

2.1.3. Keamanan Data

Keamanan komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Banyak yang belum mengetahui bahwa keamanan (*security*) merupakan sebuah komponen yang sangat penting. Bagi perancang dan pengelola sistem informasi, masalah kemanan sering menjadi masalah. Kriptografi juga sangat

berperan dalam berkomunikasi, untuk melakukan enkripsi (pengacakan) data, lalu ditransaksikan dari awal ke akhir bahkan bisa melakukan dekripsi data yang diacak tersebut (Abdul Kodir : 2021).

Secara umum keamanan data ada beberapa aspek, yaitu sebagai berikut :

1. *Privacy*/*confidentiality*

   Privacy lebih kearah data-data yang bersifat rahasia, sedangkan *Confidentiality* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu.

2. *Integrity*

   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dengan saat informasi dikirimkan. Jika terdapat perbedaan antara informasi atau data yang dikirim dengan yang diterima maka aspek integrity tidak tercapai.

3. *Authenticity*

   Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah orang yang dimaksud.

4. *Availability*

   Aspek ini berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berbeda dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.

5. *Acces Control*

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. *Acces control* seringkali dilakukan dengan menggunakan kombinasi *user* id/password atau dengan menggunakan mekanisme lain (Muhammad Haris Hrp : 2020).

Keamanan sistem dapat diartikan sebagai upaya mencegah dan mengidentifikasi pengguna yang tidak terdaftar pada sistem atau jaringan komputer dengan tujuan untuk antisipasi risiko jaringan atau sistem komputer dari ancaman secara fisik maupun logik Ada tiga level tindakan dalam mengamankan sistem dari serangan, yaitu: Preventif atau pencegahan dengan cara melakukan konfigurasi sistem sebisa mungkin terhindar dari kesalahan. Kesalahan konfigurasi merupakan jenis risiko celah keamanan yang paling umum ditemukan pada sebuah sistem operasi workstation maupun server, framework, library dan aplikasi (Tohirin, 2020).

2.2.Pengertian Algoritma

Algoritma terdiri dari langkah-langkah terstruktur yang dirancang untuk menyelesaikan masalah atau mencapai tujuan tertentu. Dalam hal keamanan informasi, algoritma kriptografi memiliki peran krusial dalam melindungi kerahasiaan dan integritas data. Salah satu algoritma kriptografi yang umum digunakan adalah algoritma RSA (Rivest-Shamir-Adleman). RSA merupakan algoritma kriptografi asimetris yang memanfaatkan kunci publik dan kunci privat untuk enkripsi dan dekripsi data. (D. R. Stinson, 2019)

Berdasarkan persyaratan ini, algoritma dapat didefinisikan sebagai

keamanan data kepegawaian yang didapatkan dari karakteristik algoritma enkripsi dengan menggunakan hasil review untuk mencapai tujuan yang telah ditentukan sebelumnya. (L. Adleman,2022)

Istilah algoritma diambil dari nama Abu Ja'far Mohammed ibn Musa al-Khawarizmi, seorang ilmuwan arab yang menggagas ilmu dasar operasi aritmatika (penjumlahan, pengurangan, pembagian, perkalian).

Seperti yang dikatakan oleh (Kadir, 2021) didalam bukunya yaitu "Algoritma adalah sekumpulan langkah rinci yang ditujukan untuk kopmuter dalam menyelesaikan suatu masalah. Langkah-Langkah yang dimaksud adalah agar bisa dituangkan ke dalam program, sehingga bisa dieksekusi oleh komputer".

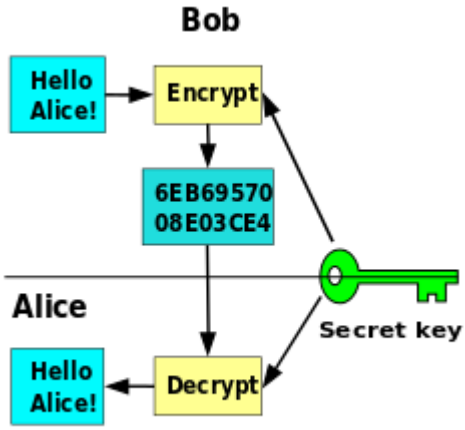
2.3.Pengertian Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik untuk mengamankan komunikasi dengan mengubah teks biasa menjadi bentuk yang tidak dapat dibaca atau hanya dapat dibaca oleh penerima yang ditentukan (W. Stallings, 2019).

Kriptografi merupakan sebuah cabang ilmu yang berkaitan dengan teknik-teknik untuk menjaga kerahasiaan informasi dengan cara mengubah teks asli menjadi bentuk yang tidak dapat dimengerti kecuali oleh penerima yang ditentukan. Tujuan utama dari kriptografi adalah untuk menjaga kerahasiaan, integritas, dan autentikasi data. (F. Riza, 2024)

Kriptografi modern umumnya dibagi menjadi dua jenis utama: kriptografi

simetris dan kriptografi asimetris. Kriptografi simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi data, sementara kriptografi asimetris menggunakan pasangan kunci yang berbeda, yaitu kunci publik dan kunci privat. (Saddle River, 2020).



Gambar 2.1 Proses Kunci Publik dan Privat
(Sumber :www.answers.com)

2.3.1. Kriptografi Klasik

Kriptografi klasik merupakan kriptografi yang sudah digunakan pada zaman dahulu sebelum computer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi klasik terbagi menjadi 2 yaitu :

a. Chipher Substitusi (Substitution Cipher)

   Merupakan algoritm kriptografi yang mula-mula digunakan oleh kaisar romawi, Julius Caesar (sehingga dinamakan juga caesar chiper), untuk menyandikan pesan yang ia kirim kepada para gubernurny. Caranya adalah mengganti/mensubstitusi setiap karakter dengan karakter lain sesuai susunan abjad. (Muhammad Haris Hrp : 2020)

b. Chiper Transposisi

Pada chiper transposisi, plainteks tetap sama, tetapi urutannya diubah. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian karakter dalam sebuah teks. Nama lain dari metode ini adalah permutasi. (Muhammad Haris Hrp : 2020)

2.3.2. Kriptografi modern

Kriptografi modern merupakan teknik kriptografi yang beroperasi dalam mode karakter. Pengoprasian kriptografi ini dalam mode bit berarti semua data dan informasi (kunci, plainteks, maupun chipher teks) semua dinyatakan dalam rangkaian string ataupun bit biner 0 dan 1. Kriptografi modern terbagi 2 yaitu : (Muhammad Haris Hrp : 2020)

a. Algoritma Simetris

Merupakan pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi dekripsi. Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma seperti:

1) Data Encryption Standard (DES)
2) Advance Encryption System (AES)
3) International Data Encryption Algorithm (IDEA)
4) A5
5) RC4

b. Algoritma Asimetris

c. Merupakan pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi untuk proses dekripsi. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA(Rivest, Shamir, Adleman) (Muhammad Haris Hrp : 2020)

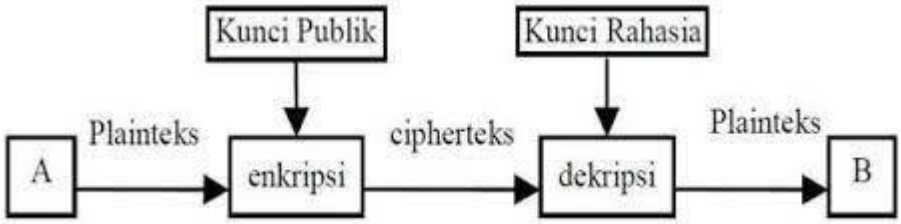
2.3.3. Algoritma Kriptografi Asimetris

Skema ini adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Skema ini disebut juga sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (public-key) atau dapat diketahui siapa saja, tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya, disebut privatekey (Albert Ginting, 2020).

Dalam banyak literatur klasik disimpulkan bahwa kriptografi merupakan seni sekaligus ilmu guna menjaga kerahasiaan informasi atau pesan menggunakan cara penyandian pada pesan atau informasi itu sendiri sehingga tidak dapat dipahami lagi maksudnya. Berdasarkan sifat dari kunci yang dipakai, algoritma terbagi dua, yakni simetris dan asimetris. Sederhananya, algoritma simetris menggunakan satu kunci rahasia, sedangkan asimetris disebut juga public key algorithm menggunakan sepasang kunci rahasia dan kunci publik di mana kunci publik digunakan untuk proses enkripsi dan kunci rahasia digunakan untuk dekripsi. Alur kunci publik algoritma asimetris dapat dilihat pada gambar 2.2. Salah satu algoritma Asimetris adalah RSA (*Rivest Shamir Adleman*) yang pertama kali ditemukan oleh di 1977. Penamaan RSA diambil dari ketiga nama tengah penemunya. RSA masih diimplementasikan

dan direkomendasikan dalam berbagi aplikasi selama belum ditemukan algoritma yang mangkus untuk memfaktorkan bilangan bulat menjadi bilangan primanya. Tingkat kompleksitas memfaktorkan bilangan besar merupakan penentu keamanan RSA (Tohirin, 2020)

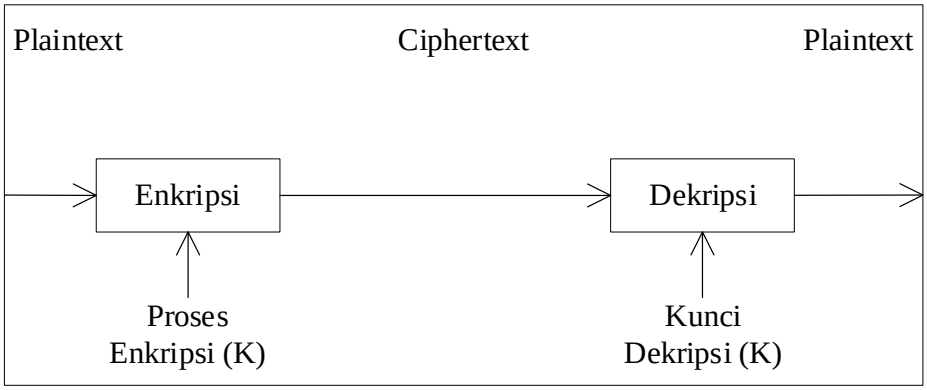
Kunci publik (e) dipilih sebagai bilangan bulat eksponensial yang relatif prima terhadap nilai φ(n), yang berarti e harus memiliki faktor-faktor prima yang berbeda dengan nilai φ(n). Biasanya, nilai e yang umum digunakan adalah bilangan prima kecil, seperti 65537 atau 3.



Gambar 2.2 Proses Enkripsi/Deskripsi Algoritma Asimetris
(Sumber : Denny Ardianta Sitepu, 2022)

2.3.4. Kriptografi Simetris

Algoritma simetris *(symmetric algorithm*) adalah algortima yang menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi



Gambar 2.3 Proses algoritma *kriptografi simetris*
(Sumber : Rachmayanti & Wirawan, 2022)

AES Merupakan standar algoritma *kriptografi* terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology)* sebagai pengganti algoritma DES (*Data Encryption Standard)* yang sudah berakhir masa penggunaanya. Algoritma AES adalah algoritma *kriptografi* yang dapat mengenkripsi dan mendeskripsi data dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Pada Algoritma AES.(Suparman, 2022)

Pada algoritma AES, panjang blok input, blok output, dan state adalah 128 bit. Dengan ukuran data 128 bit, Nb = 4, yang berarti setiap baris data memiliki panjang 4 byte. Meskipun blok input berukuran 128 bit, kunci yang digunakan dalam algoritma AES tidak harus memiliki panjang yang sama dengan blok input. Cipher key dalam AES dapat berupa kunci dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci ini akan mempengaruhi jumlah putaran (round) yang diterapkan dalam algoritma AES. (Rachmayanti & Wirawan, 2022)

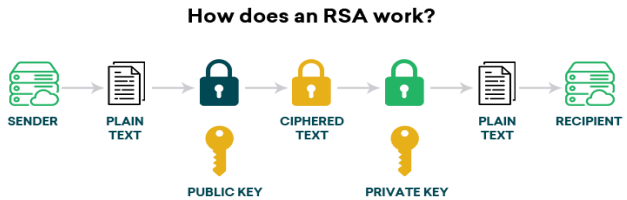
2.4.Kriptografi RSA

2.4.1. Pengertian RSA

RSA (Rivest-Shamir-Adleman) adalah salah satu algoritma kriptografi asimetris yang paling banyak digunakan. Algoritma ini melibatkan penggunaan sepasang kunci, yaitu kunci publik dan kunci privat, yang digunakan untuk enkripsi dan dekripsi (R. L. Rivest et al., 2019). Keunggulan utama dari algoritma RSA adalah kemampuannya untuk menghasilkan pasangan kunci publik dan kunci privat yang digunakan untuk melakukan enkripsi dan dekripsi data. Kunci publik dapat digunakan oleh siapa saja

untuk mengenkripsi pesan, sedangkan kunci privat hanya diketahui oleh penerima yang dituju dan digunakan untuk mendekripsi pesan yang telah dienkripsi. Proses enkripsi dan dekripsi dalam algoritma RSA didasarkan pada operasi matematika pada bilangan bulat besar. Secara sederhana, proses enkripsi dilakukan dengan mengalikan pesan dengan eksponen publik dan mengambil modulus dari hasil perkalian tersebut. Sedangkan proses dekripsi dilakukan dengan mengalikan pesan terenkripsi dengan eksponen privat dan mengambil modulus dari hasil perkalian tersebut. Keamanan algoritma RSA didasarkan pada kesulitan dalam memecahkan masalah faktorisasi bilangan bulat besar. Dalam implementasinya, ukuran kunci RSA biasanya ditentukan oleh panjang bilangan prima yang digunakan untuk menghasilkan pasangan kunci. Penerapan algoritma RSA dalam pengamanan distribusi data kepegawaian pada Badan Kepegawaian Provinsi Sumatera Utara akan memungkinkan pertukaran data yang aman dan terjamin kerahasiaannya antara berbagai unit kerja dalam badan tersebut. Dengan menggunakan kriptografi asimetris, data kepegawaian dapat dilindungi dengan baik dari akses yang tidak sah dan manipulasi data.

Perancangan Algoritma Kriptografi RSA memiliki beberapa yang akan dilakukan sebagai berikut :



Gambar 2.4 Cara Kerja RSA
(Sumber :www.answers.com)

Analisis Kebutuhan Sistem: Menganalisis kebutuhan sistem pengamanan data kepegawaian yang sesuai dengan regulasi dan kebijakan Badan Kepegawaian Provinsi Sumatera Utara.

Perancangan Sistem: Merancang sistem pengamanan data kepegawaian berbasis algoritma RSA, termasuk proses enkripsi, dekripsi, dan manajemen kunci.

Algoritma RSA pada dasarnya dapat dibedakan menjadi tiga bagian besar, yaitu algoritma pembangkitan kunci, algoritma enkripsi dan algoritma dekripsi. Algoritma utama dari sistem kriptografi RSA adalah (Harin Noor Octafiani : 2021). : Proses enkripsi menggunakan persamaan :

$$c = m^* e \bmod * n$$

Proses dekripsi menggunakan persamaan :

$$m = c^* d \bmod *n$$

Keterangan :

m : bilangan integer yang merepresentasikan pesan

c : bilangan integer yang merepresentasikan pesan tersandi

e : kunci enkripsi (bersifat publik)

d : kunci dekripsi (bersifat rahasia)

n : modulus (publik)

Bilangan e dan n merupakan kunci publik RSA diletakkan pada suatu direktori publik yang dapat diakses semua orang.

Algoritma RSA dikembangkan oleh tiga peneliti dari MIT

(Massachusetts Institute of Technology) pada tahun 1976, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA merupakan salah satu teknik kriptografi yang menggunakan pasangan kunci, di mana kunci untuk enkripsi berbeda dengan kunci untuk dekripsi. Kunci enkripsi disebut kunci publik, sedangkan kunci dekripsi disebut kunci privat. Siapa saja dapat memiliki kunci publik untuk melakukan enkripsi, tetapi hanya pemilik kunci privat yang dapat mendekripsi data. Kunci publik dapat dibagikan kepada siapa saja, sementara kunci privat hanya dimiliki oleh pihak tertentu (Yaya Suharya : 2020).

Algoritma RSA merupakan penerapan dari kriptografi asimetri, yaitu jenis kriptografi yang menggunakan dua kunci yang berbeda: kunci publik (public key) dan kunci pribadi (private key). Adapun tingkat kerahasian dari besaran besaran pada algoritma RSA diantaranya adalah besaranbesaran yang digunakan pada algoritma RSA:

1. p dan q bilangan prima (rahasia)
2. N = p . q (tidak rahasia)
3. $\Phi(n) = (p - 1)(q - 1)$ (rahasia)
4. e = (kunci enkripsi) (tidak rahasia)
5. d = (kunci dekripsi) (rahasia)
6. X (plainteks) (rahasia)
7. Y (cipherteks) (tidak rahasia) (Harin Noor Octafiani : 2021).

2.4.2. Komponen Algoritma Kriptografi Asimetris RSA

Secara umum algoritma kriptografi asimetris RSA (Rivest-Shamir-

Adleman) terdiri dari beberapa komponen utama yang bekerja bersama untuk mengenkripsi dan mendekripsi data serta untuk menghasilkan tanda tangan digital. Berikut adalah komponen-komponen utama dari algoritma RSA :

1. Pembangkitan pasangan kunci publik dan kunci privat. Kunci publik digunakan untuk enkripsi data, sementara kunci privat digunakan untuk dekripsi data. Proses pembangkitan kunci dilakukan dengan memilih dua bilangan bulat besar yang saling terkait secara matematis.
2. Proses enkripsi dalam algoritma RSA dilakukan dengan menggunakan kunci publik untuk mengubah pesan asli menjadi bentuk yang tidak dapat dibaca (cipher text). Enkripsi dilakukan dengan memangkatkan pesan asli ke dalam kekuatan eksponen kunci publik dan mengambil modulus dari hasil pangkat tersebut.
3. Proses dekripsi dalam algoritma RSA dilakukan dengan menggunakan kunci privat untuk mengembalikan cipher text menjadi pesan asli. Dekripsi dilakukan dengan cara memangkatkan cipher text ke dalam kekuatan eksponen kunci privat dan mengambil modulus dari hasil pangkat tersebut.
4. Algoritma RSA juga digunakan untuk membuat tanda tangan digital. Tanda tangan digital dibuat dengan mengenkripsi hash dari pesan menggunakan kunci privat pengirim. Penerima pesan kemudian dapat memverifikasi tanda tangan digital tersebut dengan menggunakan kunci publik pengirim.
5. Untuk menghasilkan tanda tangan digital, algoritma RSA

menggunakan fungsi hash untuk menghasilkan hash dari pesan yang akan ditandatangani. Fungsi hash menghasilkan nilai hash yang unik untuk setiap pesan yang digunakan sebagai input, sehingga memastikan keaslian dan integritas pesan.

6. Operasi aritmatika modular (pangkat dan modulus) merupakan komponen penting dari algoritma RSA. Dalam operasi enkripsi dan dekripsi, pangkat dan modulus digunakan untuk menghasilkan cipher text dan pesan asli. Operasi ini memungkinkan algoritma RSA untuk bekerja dengan bilangan bulat besar secara efisien.

2.4.3. Keuntungan dan Kelemahan Algoritma Kriptografi Asimetris RSA

Menurut A. Shamir & L.M Adleman. (2019) adapun keuntungan antara lain :

1. Keamanan tinggi menggunakan pasangan kunci publik dan kunci privat, di mana kunci publik digunakan untuk enkripsi dan kunci privat digunakan untuk dekripsi.
2. Tidak memerlukan pertukaran kunci rahasia di antara pihak yang berkomunikasi.
3. Autentikasi, yaitu memverifikasi identitas pengirim pesan.
4. Skalabilitas igunakan untuk mengamankan data dalam skala yang besar tanpa mengorbankan keamanan.

Adapun kelemahannya antara lain :

1. Kinerjanya yang lambat, terutama ketika digunakan untuk mengenkripsi dan mendekripsi data yang besar.
2. Untuk mencapai tingkat keamanan yang tinggi, algoritma RSA memerlukan kunci dengan panjang bit yang besar.
3. Keamanan algoritma RSA bergantung pada kesulitan dalam memecahkan masalah faktorisasi bilangan bulat besar

2.4.4. Proses Pembangkitan Kunci Algoritma RSA

Langkah-langkah yang dilakukan pada proses pembangkitan kunci adalah sebagai berikut :

1. Pilih 2 bilangan prima besa p dan q
2. Hitung nilai n, yaitu n = p*q
3. Hitung nilai m, yaitu m = (p-1)(q-1)
4. Pilih sebuah angka kecil e, coprime untuk m
5. Hitung nilai d dengan rumus yaitu

$$d*e \bmod m = 1$$

Kemudian nilai e dan n yang didapat menjadi pasangan kunci publik, sedangkan nilai d dan n sebagai pasangan kunci privat.

2.4.5. Proses Enkripsi Algoritma RSA

Untuk perhitungan enkripsi, setelah pasangan kunci publik didapat, maka proses enkripsi dihitung menggunakan persamaan :

$$ci=m * e \bmod n$$

Dimana :

3. Nilai ci adalah hasil dari perhitungan dan menjadi chiperteks
4. Nilai mi adalah merepresentasikan pesan atau plainteks yang telah diubah menjadi kode ASCII
5. Nilai e dan n merupakan pasangan kunci publik yang telah dibangkitkan melalui proses pembangkitan kunci.
6. Nilai d dan nilai n merupakan pasangan kunci privat yang telah dibangkitkan melalui proses pembangkitan kunci.

2.4.6. Proses Dekripsi Algoritma RSA

Untuk perhitungan dekripsi, setelah chiperteks diterima, maka chiperteks dikembalikan ke plainteks dengan menggunakan persamaan : m=c d mod n dimana : a. Nilai m merupakan hasil dari perhitungan untuk menghitung nilai yang akan dikembalikan menjadi plainteks b. Nilai c adalah representasi dari chiperteks atau pesan yang terenkripsi yang akan diubah menjadi plainteks

2.5 File

File adalah arsip aktif yang masih terdapat di unit kerja dan masih diperlukan dalam proses administrasi secara aktif, masih secara langsung digunakan. File atau arsip merupakan wadah yang digunakan untuk menyimpan atau menampung atau mengumpulkan data. Penyimpanan data dalam *file* terbagi dalam 2 jenis yaitu penyimpanan terstruktur dan tidak terstruktur. Penyimpanan terstruktur artinya penyimpanan data dikelola dengan memiliki bentuk atau keteraturan atau format tertentu, contoh *file table*, gambar, *worksheet*, dan lain-sebagainya. Ciri dari *file* terstruktur adalah

memiliki *header* yang menjadi data tentang struktur file tersebut dilanjutkan dengan data yang disimpannya. Sedangkan *file* tidak terstruktur adalah penyimpanan data dilakukan tanpa memiliki format data, data tersimpan sesuai dimana posisi disimpan (Fitriyani A et al., 2020)

2.6.Kerangka Berpikir Konseptual

Dalam mengembangkan pengamanan distribusi data kepegawaian pada Badan Kepegawaian Provinsi Sumatera Utara dengan memanfaatkan algoritma kriptografi asimetris RSA, kerangka berpikir konseptual penelitian ini akan didasarkan pada langkah-langkah berikut:

1. Analisis Kebutuhan Keamanan Data Kepegawaian
   Langkah pertama dalam kerangka konseptual adalah menganalisis kebutuhan keamanan data kepegawaian yang spesifik untuk Badan Kepegawaian Provinsi Sumatera Utara. Ini melibatkan identifikasi jenis-jenis data kepegawaian yang perlu diamankan, tingkat sensitivitasnya, dan ancaman keamanan yang mungkin dihadapi.
2. Studi Terhadap Sistem Keamanan Data Kepegawaian yang Ada
   Selanjutnya, akan dilakukan studi terhadap sistem keamanan data kepegawaian yang saat ini diterapkan di Badan Kepegawaian Provinsi Sumatera Utara. Hal ini bertujuan untuk memahami kelemahan dan kekuatan sistem yang ada serta mengevaluasi apakah sudah memenuhi standar keamanan yang dibutuhkan.
3. Perancangan Sistem Pengamanan dengan Algoritma RSA
   Setelah memahami kebutuhan dan menganalisis sistem yang ada,

langkah berikutnya adalah merancang sistem pengamanan data kepegawaian baru dengan memanfaatkan algoritma kriptografi asimetris RSA. Ini termasuk dalam perancangan pemilihan panjang kunci yang memadai, pengaturan proses enkripsi dan dekripsi, serta pengelolaan kunci.

4. Implementasi dan Uji Coba Sistem

   Sistem yang dirancang akan diimplementasikan dan diuji coba secara menyeluruh. Uji coba ini akan mencakup simulasi serangan keamanan, pengujian kinerja, serta evaluasi terhadap tingkat keamanan yang diberikan oleh sistem baru dibandingkan dengan sistem yang lama.

5. Evaluasi dan Penyempurnaan

   Langkah terakhir adalah evaluasi terhadap hasil uji coba dan feedback dari pengguna sistem. Dari evaluasi ini akan didapatkan masukan untuk melakukan penyempurnaan pada sistem pengamanan data kepegawaian yang telah dirancang.

2.7. *UML* (*Unified Modelling Language*)

Unified Modeling Language (UML) adalah sekumpulan konvensi pemodelan yang digunakan untuk mendefinisikan atau menggambarkan sistem perangkat lunak yang terkait dengan objek. UML merupakan salah satu alat yang sangat efektif dalam pengembangan sistem berbasis objek karena menawarkan bahasa pemodelan visual yang memungkinkan

pengembang untuk membuat blueprint atas visi mereka dalam bentuk yang terstruktur dan baku. UML juga berperan sebagai penghubung dalam mengkomunikasikan berbagai aspek sistem melalui elemen grafis yang dapat digabungkan.

Unified Modeling Language (UML) biasa digunakan untuk :

a. Menggambarkan batasan sistem dan fungsi-fungsi utama sistem secara umum, yang digambarkan menggunakan *use case* dan *aktor*.
b. Menggambarkan kegiatan atau proses bisnis yang terjadi secara umum, yang digambarkan menggunakan *interaction diagrams*.
c. Menggambarkan representasi struktur statis dari sebuah sistem dalam bentuk *class diagrams*.
d. Membuat model perilaku yang menggambarkan kebiasaan atau sifat sebuah sistem dengan menggunakan *state transition diagrams*.
e. Menyatakan arsitektur implementasi fisik melalui komponen dan pengembangan.
f. Menyampaikan atau memperluas*fungsionality* dengan *stereotypes*. (Alfina & Harahap, 2020) (Alfina & Harahap, 2020)

UML adalah bahasa spesifikasi standar yang digunakan untuk mendokumentasikan, mendeskripsikan, dan mengembangkan perangkat lunak. UML merupakan metodologi yang diterapkan dalam pengembangan sistem berorientasi objek dan juga alat bantu yang mendukung proses pengembangan sistem. Saat ini, UML banyak digunakan di industri sebagai

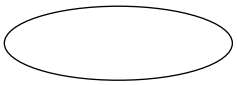
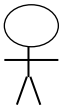
standar bahasa pemodelan umum dalam pengembangan perangkat lunak dan sistem

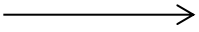
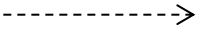
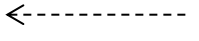
Alat bantu yang digunakan dalam perancangan berorientasi objek berbasiskan UML adalah Empat alat bantu sebagai berikut: *Use Case Diagram, Activity Diagram*, *Sequence Diagram* dan *Class Diagram.*

2.7.1. *Use Case Diagram*

Use Case Diagram merupakan pemodelan untuk melakukan (*behavior*) sistem informasi yang akan dibuat. Use Case mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Dapat dikatakan Use Case digunakan untuk mengetahui fungsi apa saja yang ada di dalam sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut. Symbol-simbol yang digunakan dalam Use Case Diagram Yaitu

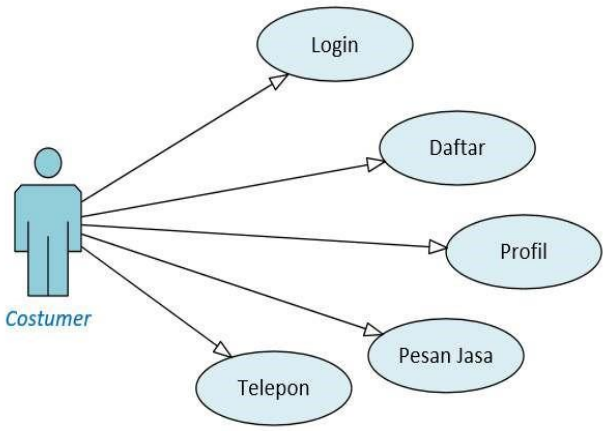
Tabel 2.1. Simbol *Use Case*

Gambar	Keterangan
	*Use case* menggambarkan fungsionalitas yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktor, biasanya dinyatakan dengan menggunakan kata kerja di awal nama *use case*.
	Aktor adalah *abstraction* dari orang atau sistem yang lain yang mengaktifkan fungsi dari target

	sistem. Untuk mengidentifikasikan aktor, harus ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang atau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan *use case*, tetapi tidak memiliki control terhadap *use case*.
	Asosiasi antara aktor dan *use case*, digambarkan dengan garis tanpa panah yang mengindikasikan siapa atau apa yang meminta interaksi secara langsung dan bukannya mengidikasikan aliran data.
	Asosiasi antara aktor dan *use case* yang menggunakan panah terbuka untuk mengidinkasikan bila aktor berinteraksi secara pasif dengan sistem.
	*Include*, merupakan di dalam *use case* lain (*required*) atau pemanggilan *use case* oleh *use case* lain, contohnya adalah pemanggilan sebuah fungsi program.
	*Extend*, merupakan perluasan dari *use case* lain jika kondisi atau syarat terpenuhi.

***(*Sumber : (Janis et al., 2020)**

Berikut ini merupakan contoh gambaran Use Case diagram sebagai berikut :

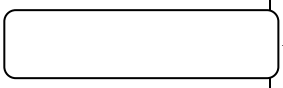
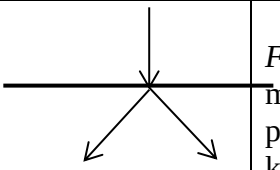


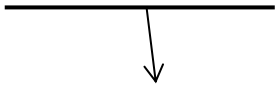
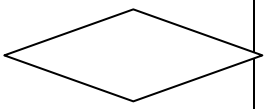
Gambar 2.5 Use Case Diagram
(Sumber : Janiver : 2020)

2.7.2. Diagram Aktivitas (*Activity Diagram*)

Activity Diagram menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis. Simbol- simbol yang digunakan dalam *activity diagram* yaitu:

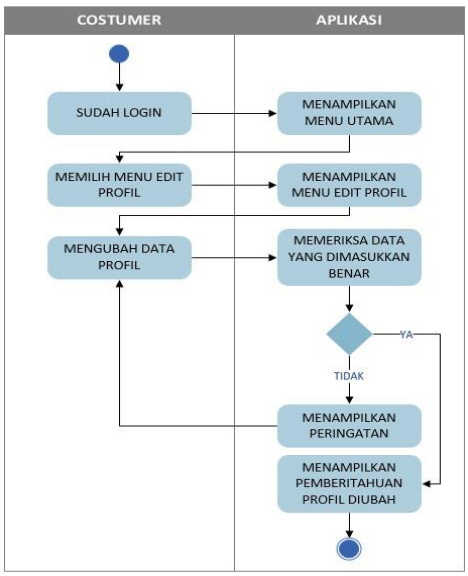
Tabel 2.2. Simbol *Activity Diagram*

Gambar	Keterangan
	*Start point*, diletakkan pada pojok kiri atas dan merupakan awal aktifitas.
	*End point*, akhir aktifitas.
	*Activites*, menggambarkan suatu proses/kegiatan bisnis
	*Fork* (Percabangan), digunakan untuk menunjukkan kegiatan yang dilakukan secara parallel atau untuk menggabungkan dua kegiatan pararel menjadi satu.
	*Join* (penggabungan) atau rake, digunakan

	untuk menunjukkan adanya dekomposisi.
	*Decision Points*, menggambarkan pilihan untuk pengambilan keputusan, *true*, *false*.
	*Swimlane*, pembagian *activity* diagram untuk menunjukkan siapa melakukan apa.

(Sumber : Janis et al., 2020)

Berikut ini merupakan contoh gambaran activity diagram sebagai berikut :

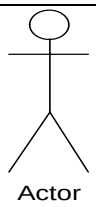
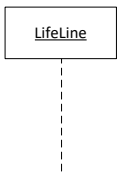
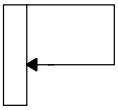


Gambar 2.6 Activity Diagram
(Sumber : Janiver : 2020)

2.7.3.*Sequence Diagram*

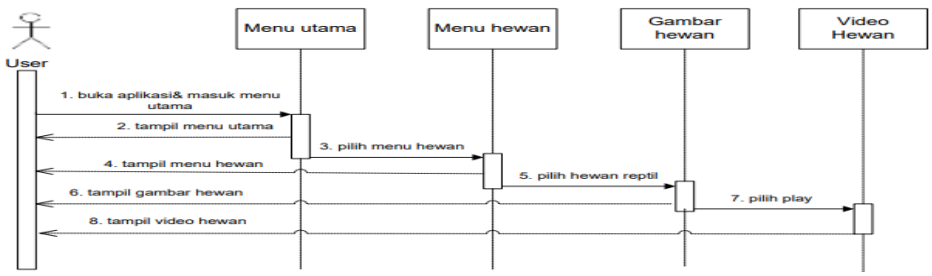
Sequence Diagram menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan pesan yang dikirimkan dan diterima antara objek. Simbol-simbol yang digunakan dalan *Sequence Diagram* yaitu:

Tabel 2.3. *Sequence Diagram*

Gambar	Keterangan
	Orang,Proses atau sistem lain yang berinteraksi dengan sistem informasi.
	Merepresentasikan entitas tunggal dalam sequence diagram, digambarkan dengan kotak. Entitas ini memiliki nama,*Stereotype* atau berupa *instance.*
	Message, simbol mengirim pesan antar *class*.
	*Recursive*, menggambarkan pengiriman pesan yang dikirim untuk dirinya sendiri.
	*Activation*, *Activation, activation* mewakili sebuah eksekusi operasi dari objek, panjang kotak ini berbanding lurus dengan durasi aktivitas sebuah operasi.
	Lifeline, garis titik-titik yang terhubung dengan objek, sepanjang *lifeline* terdapat *activation*.

(Sumber : (Janis et al., 2020)

Berikut ini merupakan contoh gambaran sequence diagram dapat dilihat pada Gambar 2.7 sebagai berikut :



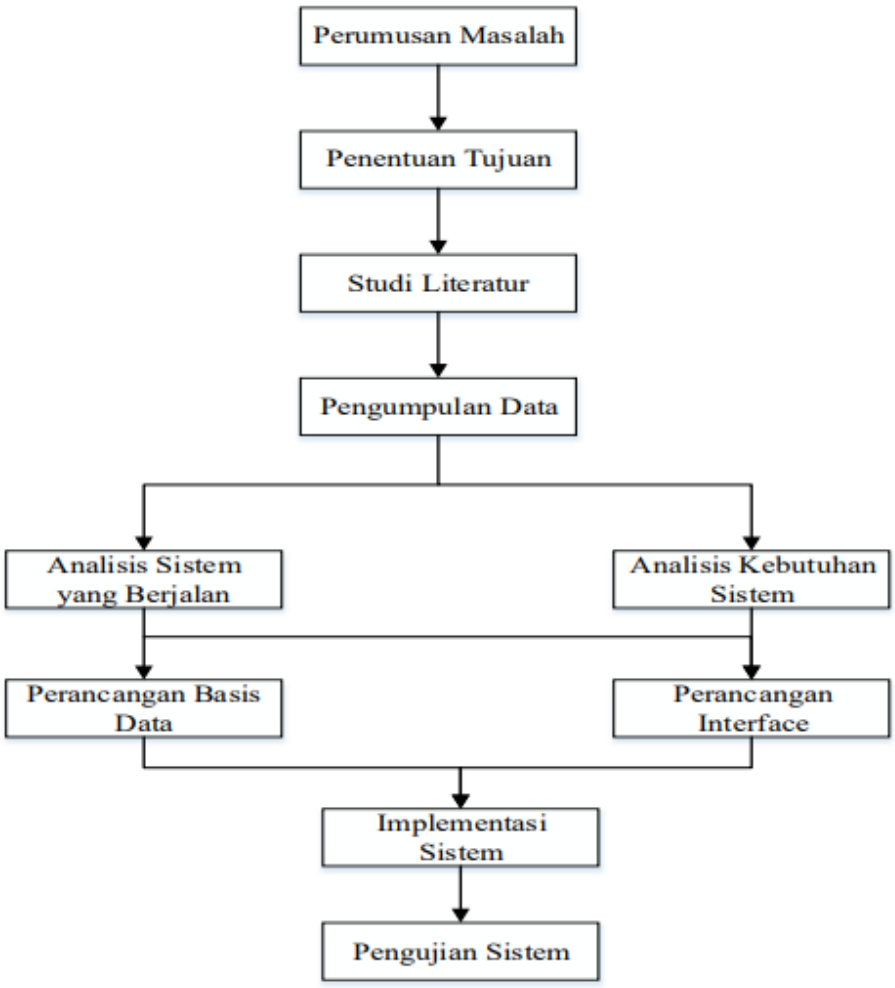
Gambar 2.7. Sequence Diagram
(Sumber : Andikos : 2020)

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Prosedur perancangan sistem dapat diuraikan kedalam tahapan *waterfall* yaitu *analysis* (analisis), *design* (desain), *implementation* (perkembangan), *testing* (percobaan), *maintenance* (pemeliharaan).



Gambar 3.1 Diagram Analisis Rancangan dengan *Waterfall*

Proses kegiatan penelitian dilakukan dalam beberapa tahapan seperti pada Gambar 3.1. yang diharapkan adalah terbangunnya sebuah system

Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA. Berikut beberapa tahapan yang harus dikerjakan dalam memperoleh hasil yang optimal:

1. Perumusan masalah merupakan penentuan masalah yang dihadapi.
2. Penentuan Tujuan merupakan arah dari penelitian yang dilakukan dan menentukan ke arah mana aplikasi yang akan dibangun.
3. Studi Literatur merupakan pencarian sumber daya yang berhubungan dengan Kriptografi Asimetris RSA. Sumber daya dapat diperoleh dari buku, ebook, artikel, jurnal atau internet yang dapat membantu dalam mencari bahan-bahan yang berkaitan dengan metode tersebut.
4. Pengumpulan data dilakukan dengan melakukan observasi atau pengamatan dan wawancara langsung ke pakar dalam Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara.
5. Analisa sistem yang sedang berjalan berguna untuk membandingkan dan menentukan apa saja kekurangan dari sistem sebelumnya, sehingga menjadi referensi untuk memperbaiki sistem yang akan dibangun.
6. Analisa kebutuhan sistem merupakan penentuan teknik penyelesaian suatu masalah dan menetukan apa saja yang dibutuhkan untuk membangun sistem baru setelah membandingkan dengan sistem sebelumnya.

7. Perancangan Database adalah proses untuk menentukan tabel-tabel yang dibutuhkan sehingga dapat digunakan sebagai tempat penyimpanan data dan informasi.
8. Perancangan Interface bertujuan untuk menentukan alur komunikasi antara pengguna dan sistem.
9. Implementasi sistem merupakan penerapan hasil program aplikasi yang telah dibangun.
10. Pengujian sistem merupakan tahapan untuk melakukan pengujian apakah sistem yang telah dirancang sudah sesuai dengan hasil analisis yang telah dilakukan dan apakah sistem yang dibuat sudah sesuai dengan fungsinya. Jika sudah, maka dilakukan pengoperasian sistem tersebut dan jika belum maka dilakukan pemeriksaan kembali bagian mana yang masih terdapat kekurangan.

3.2 Metode Pengumpulan Data

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpulan data terdapat beberapa cara, berikut diantaranya:

1. *Observation* (Pengamatan), yaitu pengumpulan data dan informasi yang dilakukan dengan cara pengamatan langsung ke lokasi Pada Badan Kepegawaian Provinsi Sumatera Utara.
2. *Interview* (Wawancara), yaitu pengumpulan data dengan cara melakukan tanya jawab dengan HRD untuk memperoleh data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara.

3. *Library Research* (Penelitian Perpustakaan), yaitu melakukan studi pustaka untuk data-data yang berhubungan dengan penelitian dalam bentuk jurnal dan buku.

3.2.1 Analisis Masalah

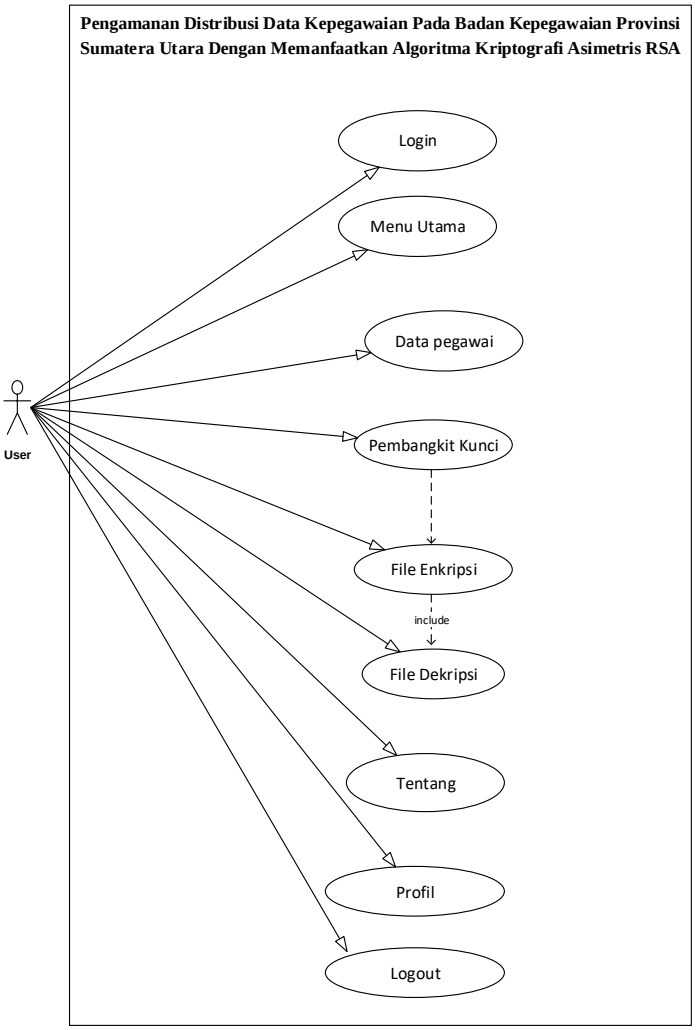
Dalam era digital saat ini, keamanan data merupakan aspek krusial yang harus diperhatikan oleh organisasi, terutama dalam konteks data kepegawaian di lembaga publik seperti BKPSU. Dengan semakin banyaknya insiden keamanan data yang terjadi, perlindungan terhadap informasi kepegawaian tidak boleh diabaikan. Algoritma kriptografi asimetris RSA menawarkan pendekatan yang kuat untuk mengamankan data dengan menggunakan kunci publik dan pribadi yang berbeda. Dalam konteks penelitian ini, kami akan mengeksplorasi implementasi algoritma RSA untuk meningkatkan keamanan distribusi data kepegawaian pada BKPSU. Pendekatan ini akan memberikan perlindungan tambahan terhadap data sensitif, sehingga meningkatkan kepercayaan publik dan memenuhi standar keamanan yang ditetapkan. Untuk mengatasi masalah tersebut, diperlukan implementasi sistem keamanan yang kokoh dan dapat diandalkan. Salah satu solusi yang disarankan adalah menggunakan algoritma kriptografi asimetris RSA (Rivest-Shamir-Adleman). Dengan menerapkan algoritma ini, data kepegawaian dapat dienkripsi secara aman sehingga hanya pihak yang berwenang yang dapat membaca informasi tersebut.

3.3 Perancangan

Desain sistem pada penelitian ini dibagi menjadi dua desain, yaitu desain sistem secara global untuk penggambaran model sistem secara garis besar dan desain sistem secara detail untuk membantu dalam pembuatan sistem. Desain sistem secara global menggunakan bahasa pemodelan UML yang terdiri dari *Use case Diagram*, *Activity Diagram* dan *Sequence Diagram*.

3.3.1 *Usecase* Diagram

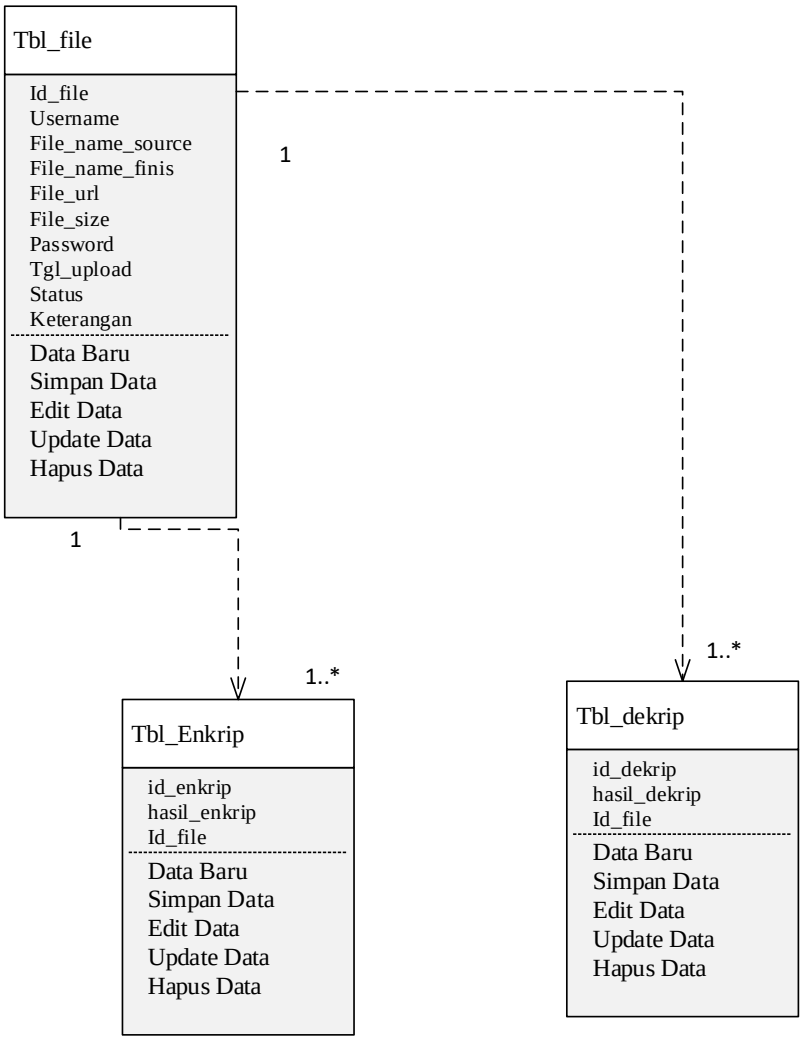
Dalam penyusunan suatu program diperlukan suatu model data yang berbentuk diagram yang dapat menjelaskan suatu alur proses sistem yang akan di bangun. Dalam penulisan skripsi ini penulis menggunakan metode UML yang dalam metode itu penulis menerapkan diagram *Use Case*. Maka digambarlah suatu bentuk diagram *Use Case* yang dapat dilihat pada gambar 3.2 berikut :



Gambar 3.2. *Use Case Diagram* Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA

3.2.2. *Class* Diagram

Rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada gambar 3.3 :



Gambar 3.3. *Class Diagram* Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA

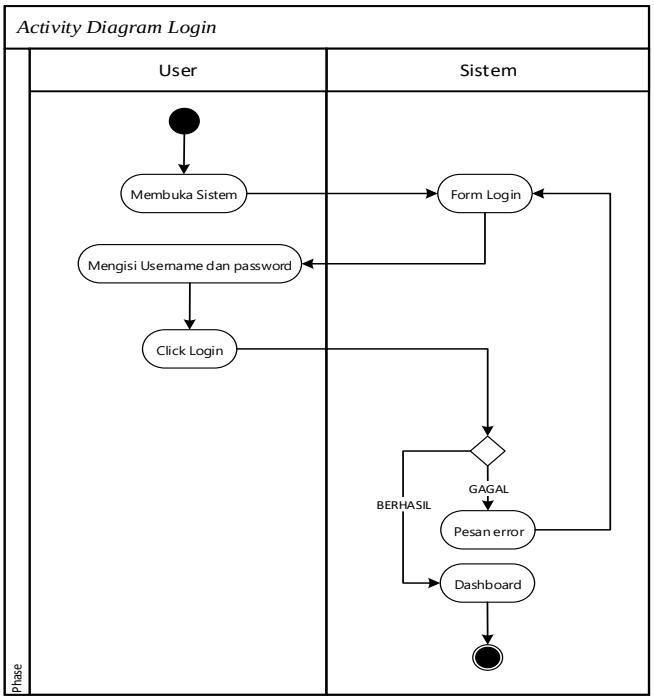
3.2.3. *Activity Diagram*

Activity Diagram menggambarkan aliran aktivitas yang berbeda, bagaimana setiap aliran dimulai, keputusan-keputusan yang dapat diambil, serta bagaimana sistem tersebut berakhir.

1. *Activity Diagram Login*

Adapun *Activity Diagram Login* dapat terlihat seperti pada gambar 3.4

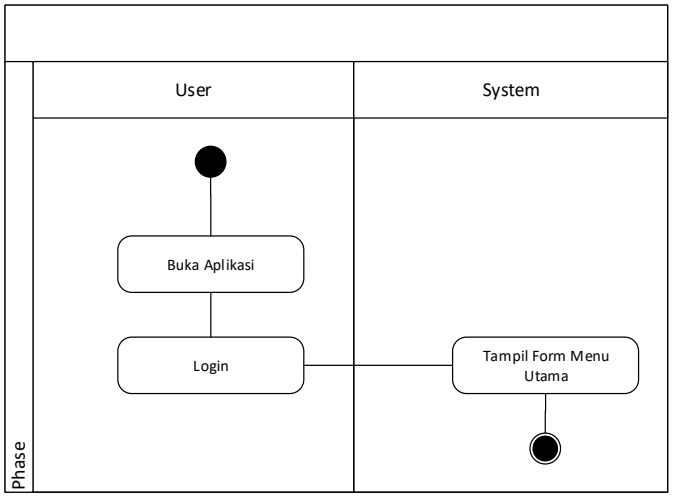
berikut:



Gambar 3.4. Activity Diagram Login

2. *Activity Diagram* Menu Utama

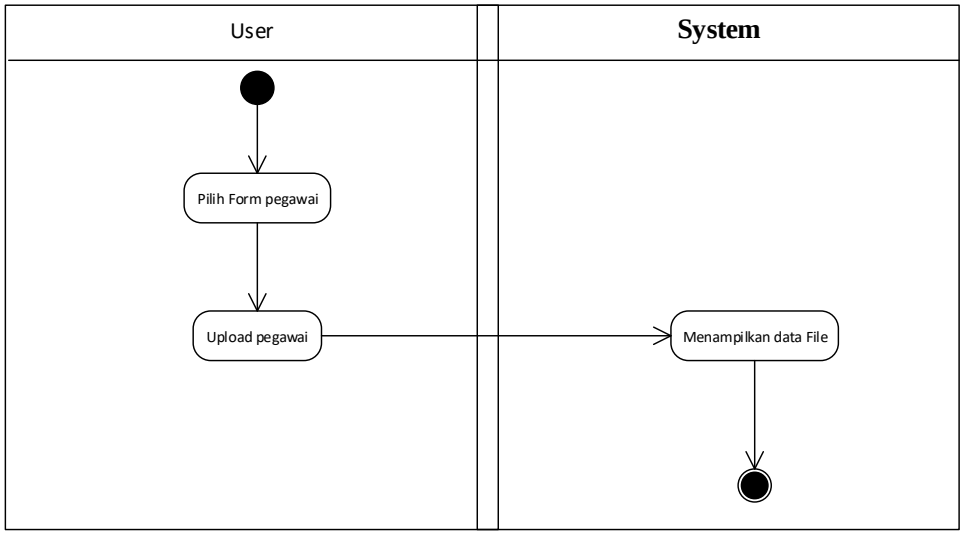
Serangkaian aktivitas menu utama yang dapat dilakukan admin dalam mengelola seluruh data yang terpusat dalam suatu program, dapat dilihat seperti pada gambar 3.5. berikut :



Gambar 3.5. *Activity* Diagram *Menu Utama*

3. *Activity Diagram* Pegawai

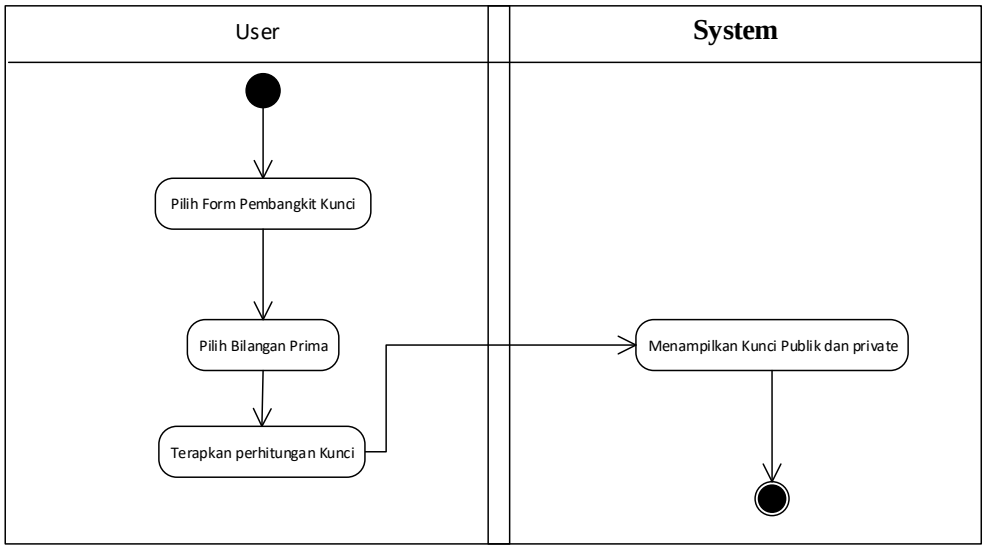
Serangkaian aktivitas data pegawai yang dapat dilakukan admin dalam mengelola data, dapat dilihat seperti pada gambar 3.6 berikut :



Gambar 3.6. *Activity Diagram* Data Pegawai

4. *Activity Diagram* Pembangkit Kunci

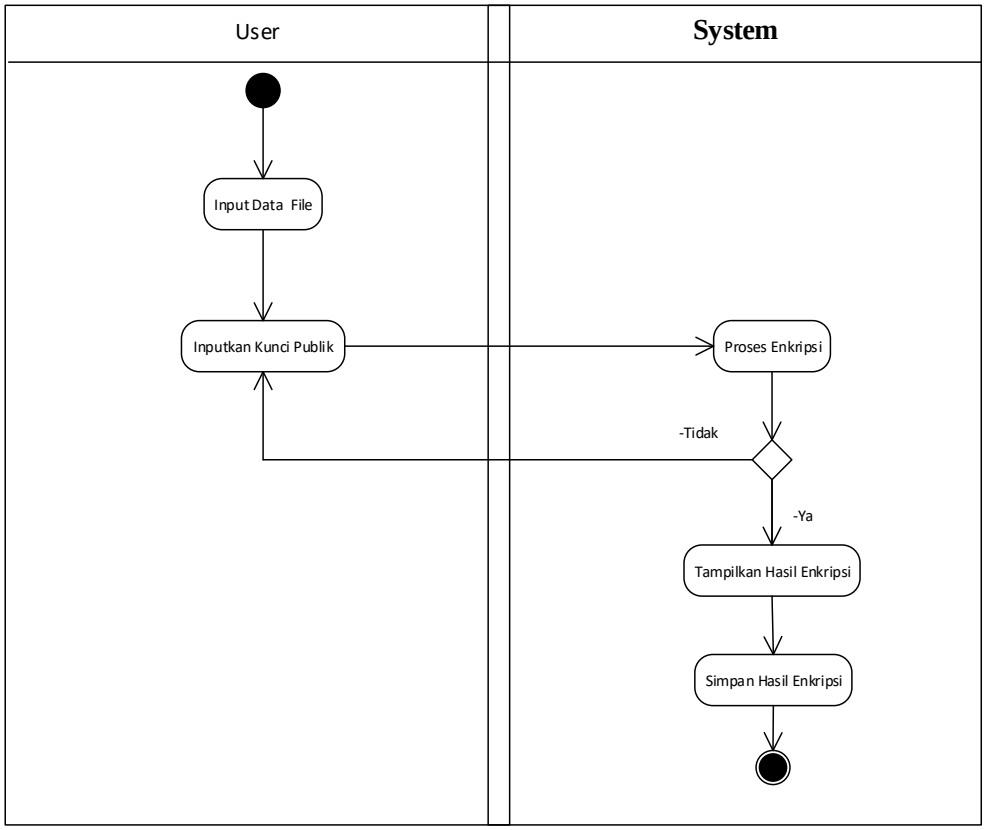
Serangkaian aktivitas data pembangkit kunci yang dapat dilakukan admin dalam mengelola data, dapat dilihat seperti pada gambar 3.7 berikut :



Gambar 3.7. *Activity Diagram* Data Pembangkit Kunci

5. *Activity Diagram* File Enkripsi

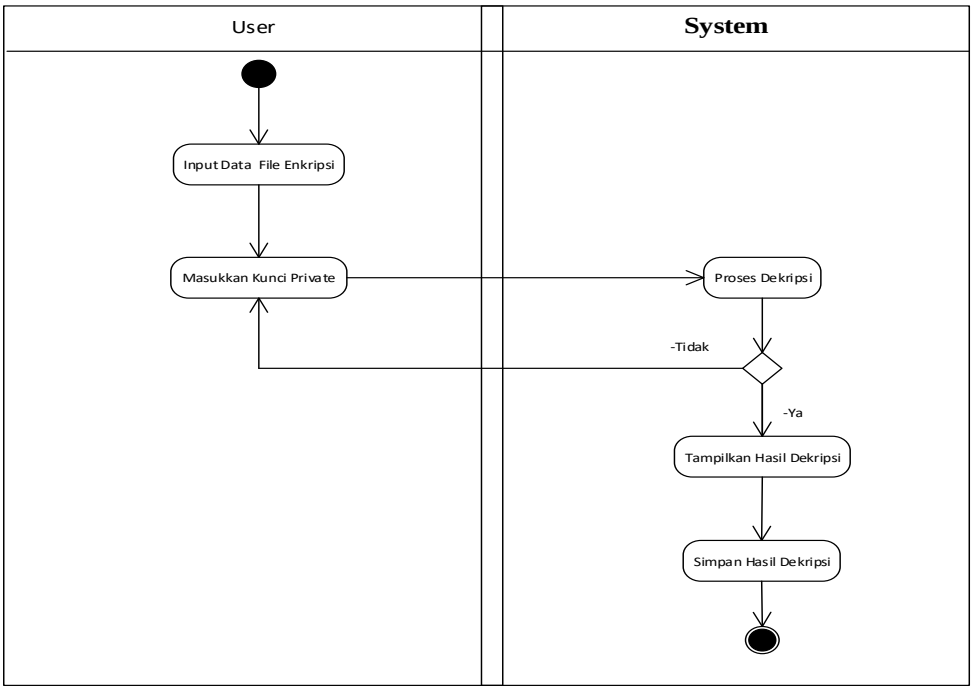
Serangkaian aktivitas file enkripsi yang dapat dilakukan admin dalam mengelola data, dapat dilihat seperti pada gambar 3.8 berikut :



Gambar 3.8. *Activity Diagram* Enkripsi

6. *Activity Diagram* Dekripsi

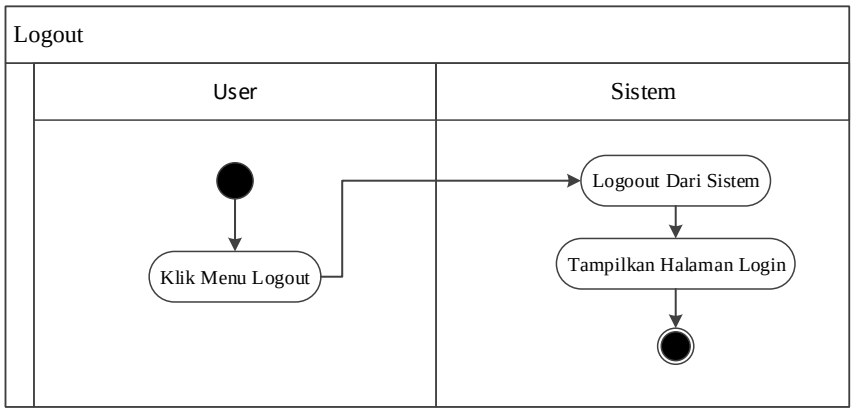
Serangkaian aktivitas file dekripsi yang dapat dilakukan admin dalam mengelola data, dapat dilihat seperti pada gambar 3.9 berikut :



Gambar 3.9. *Activity Diagram* Dekripsi

7. *Activity Diagram Logout*

Adapun *Activity Diagram Logout* dapat terlihat seperti pada gambar 3.10. berikut.



Gambar 3.10. Activity Diagram Logout

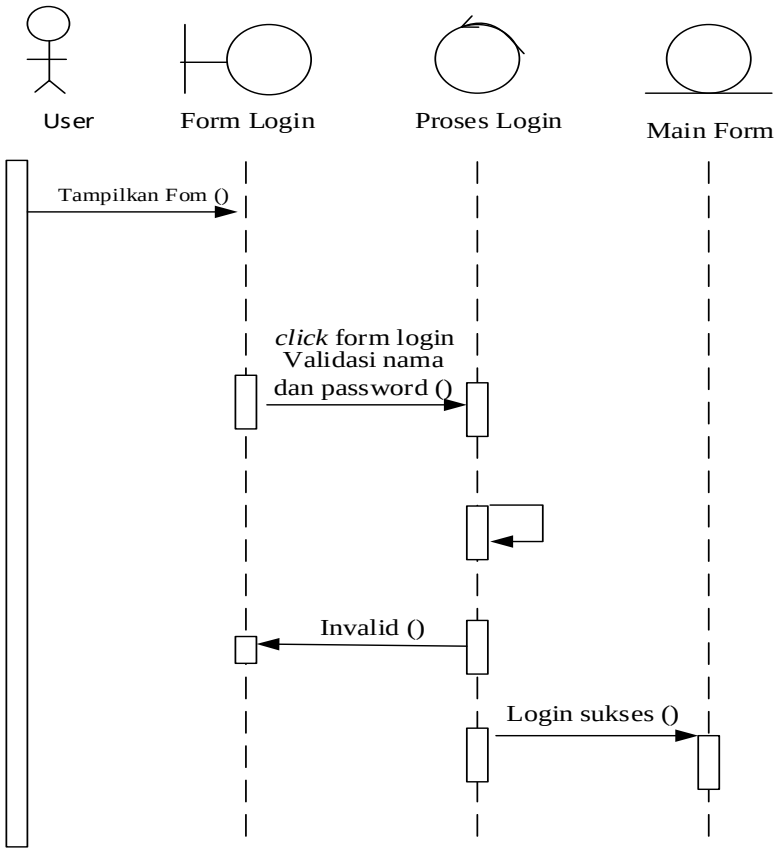
3.2.4. *Sequence Diagram*

Sequence Diagram adalah diagram yang menunjukkan interaksi antar objek dalam sistem, yang disusun berdasarkan urutan waktu. Interaksi ini

melibatkan objek-objek seperti pengguna, tampilan, dan lainnya, yang terjadi melalui pengiriman pesan.

1. *Sequence Diagram Login*

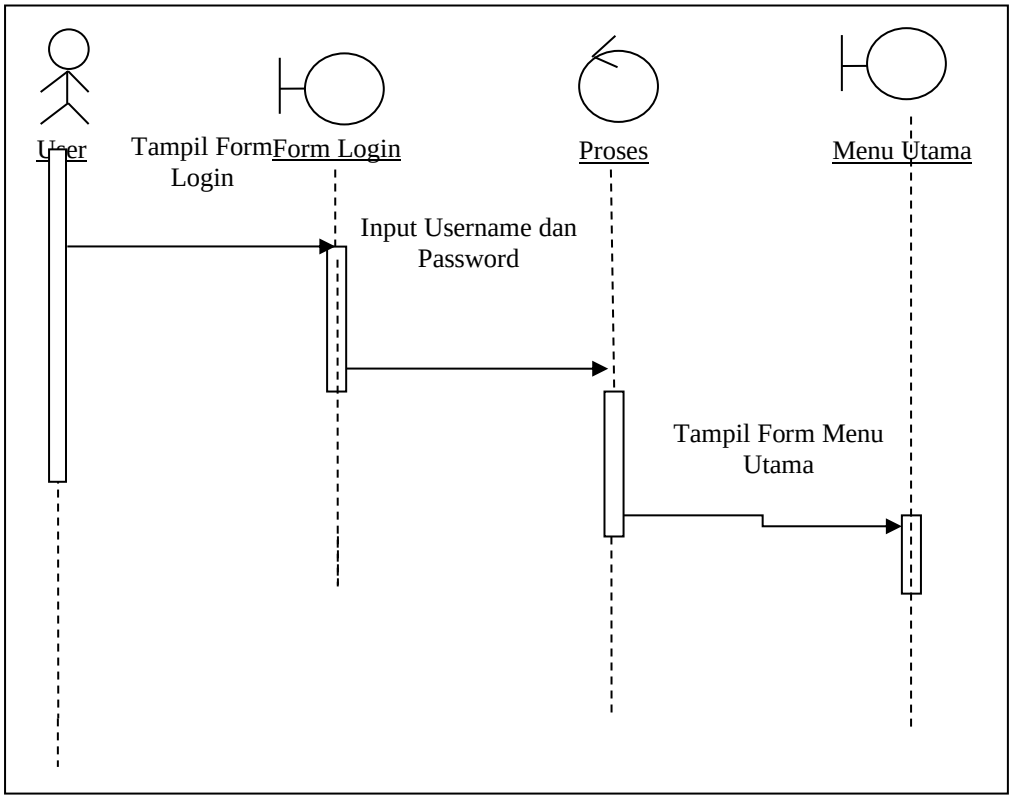
Serangkaian kerja melakukan *login* dapat terlihat seperti pada gambar 3.11. berikut.



Gambar 3.11. Sequence Diagram Login

2. *Sequence Diagram* Menu Utama

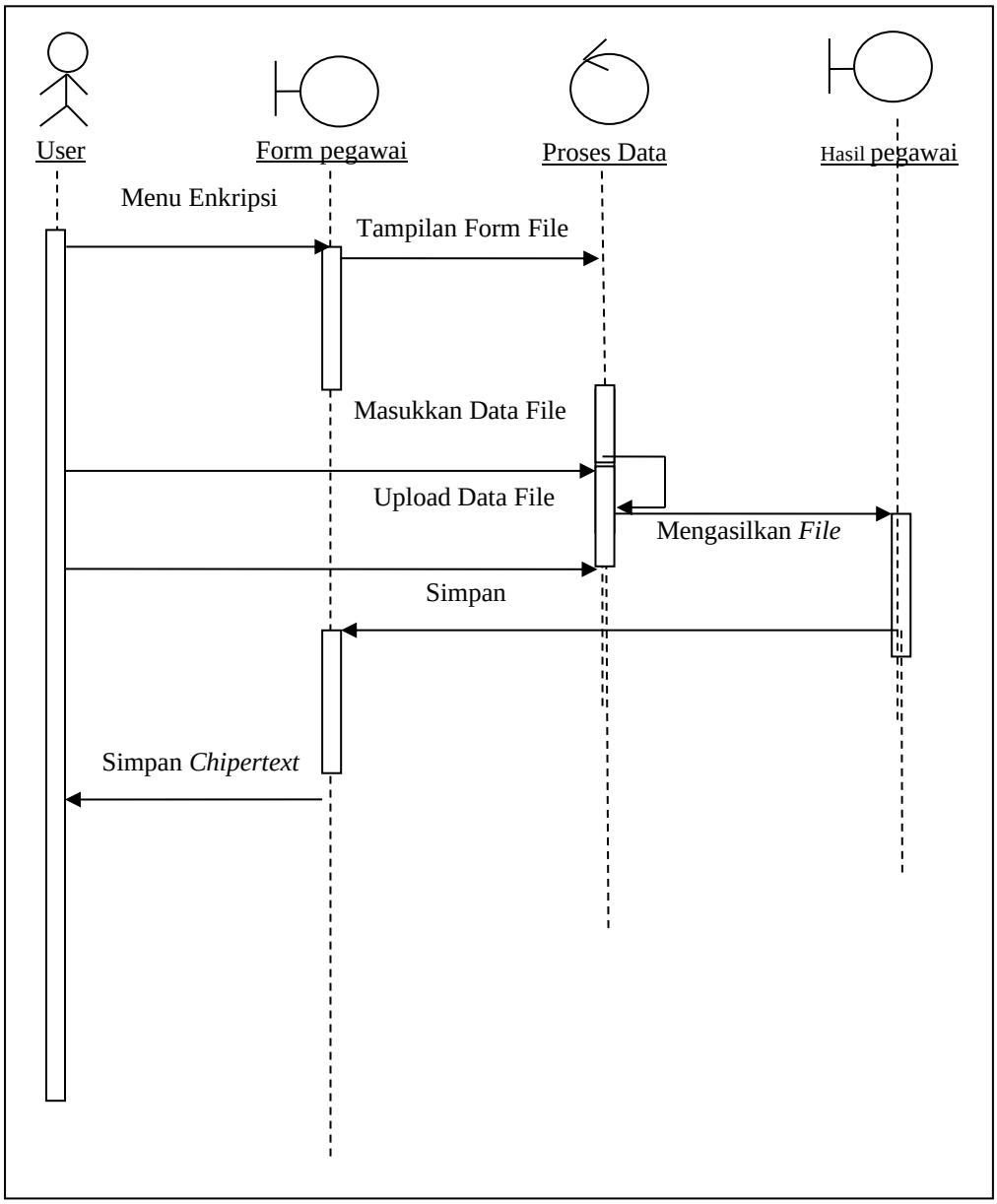
Serangkaian kerja untuk mengolah data yang terpusat pada sebuah sistem1dapat dilihat pada Gambar 3.12. dibawah ini.



Gambar 3.12. *Sequence Diagram* Menu Utama

3. *Sequence Diagram* pegawai

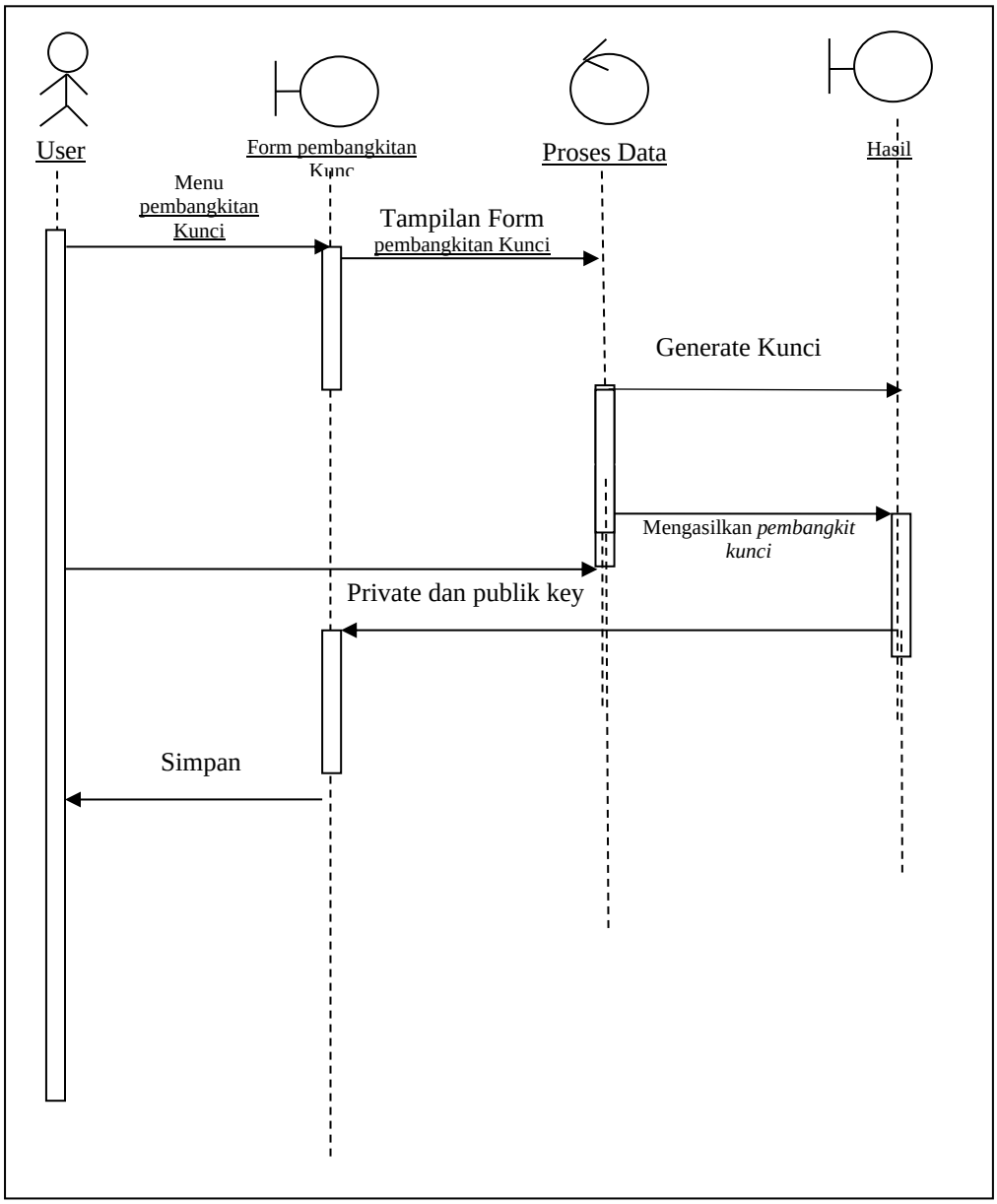
Serangkaian kerja melakukan pegawai dapat dilihat pada Gambar 3.13. dibawah ini.



Gambar 3.13. *Sequence Diagram* Pegawai

4. *Sequence Diagram* Pembangkitan Kunci

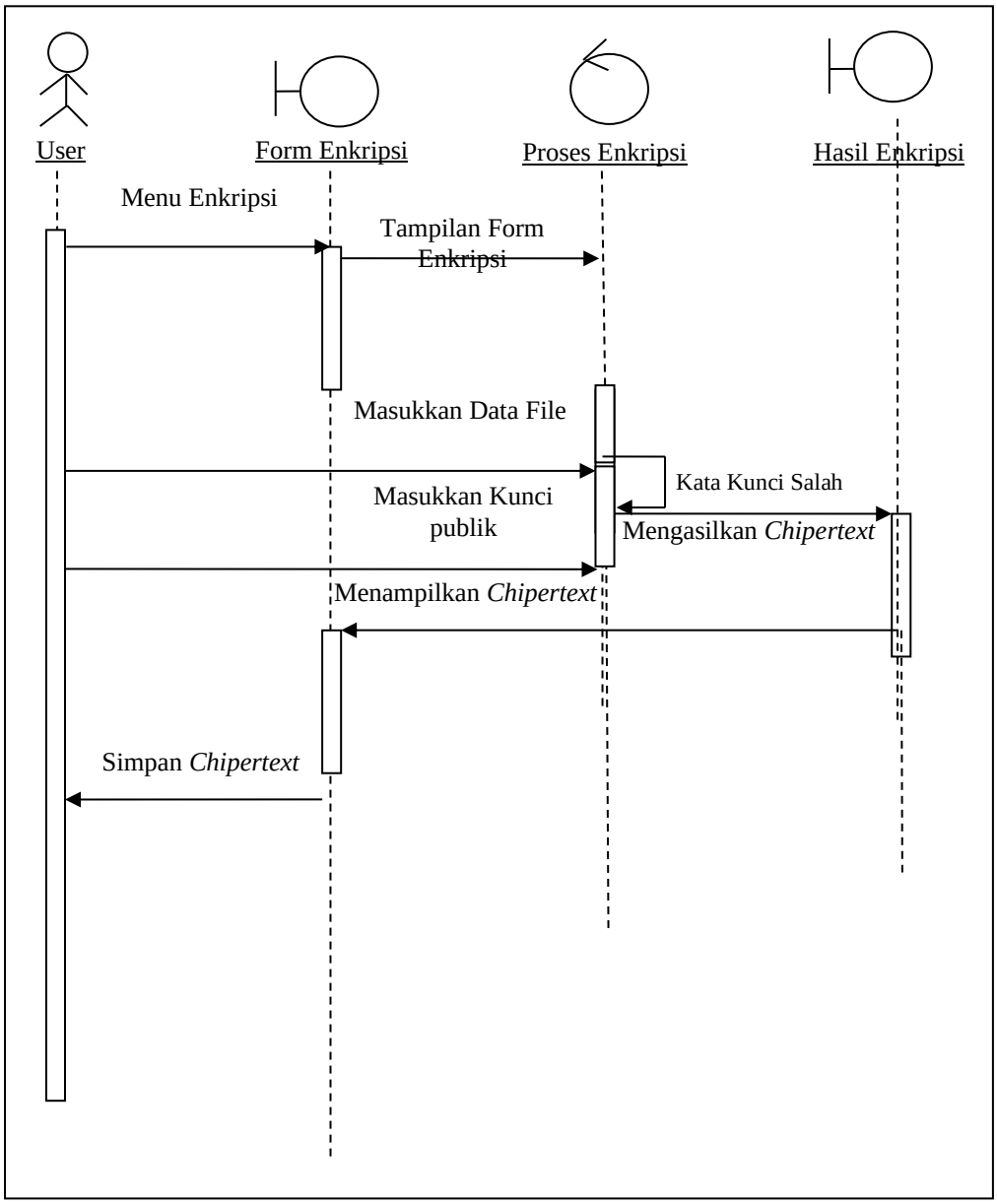
Serangkaian kerja melakukan pembangkitan kunci dapat dilihat pada Gambar 3.14. dibawah ini.



Gambar 3.14. *Sequence Diagram* Pembangkitan Kunci

5. *Sequence Diagram* Enkripsi

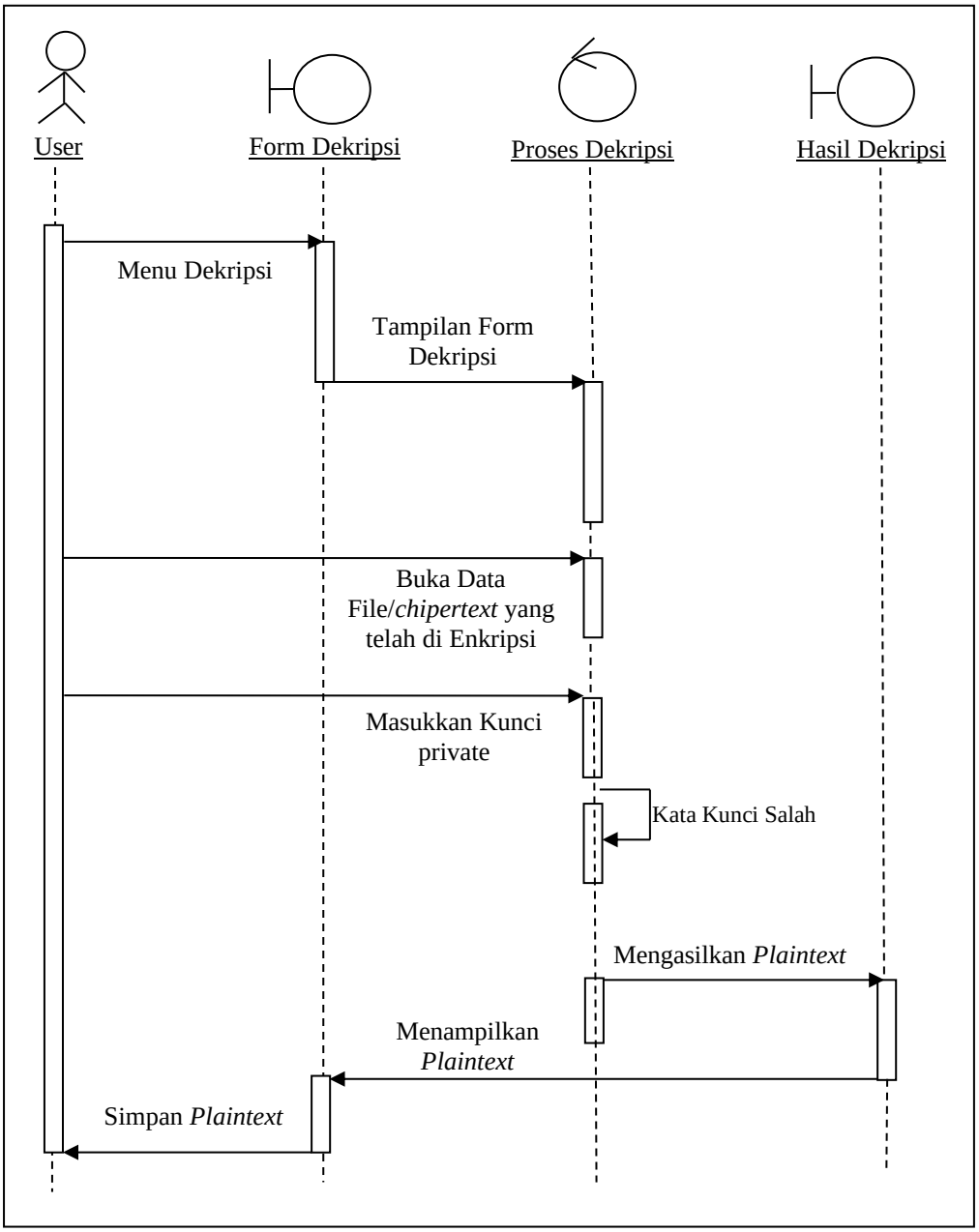
Serangkaian kerja melakukan enkripsi dapat dilihat pada Gambar 3.15. dibawah ini.



Gambar 3.15. *Sequence Diagram* Enkripsi

6. *Sequence Diagram* Dekripsi

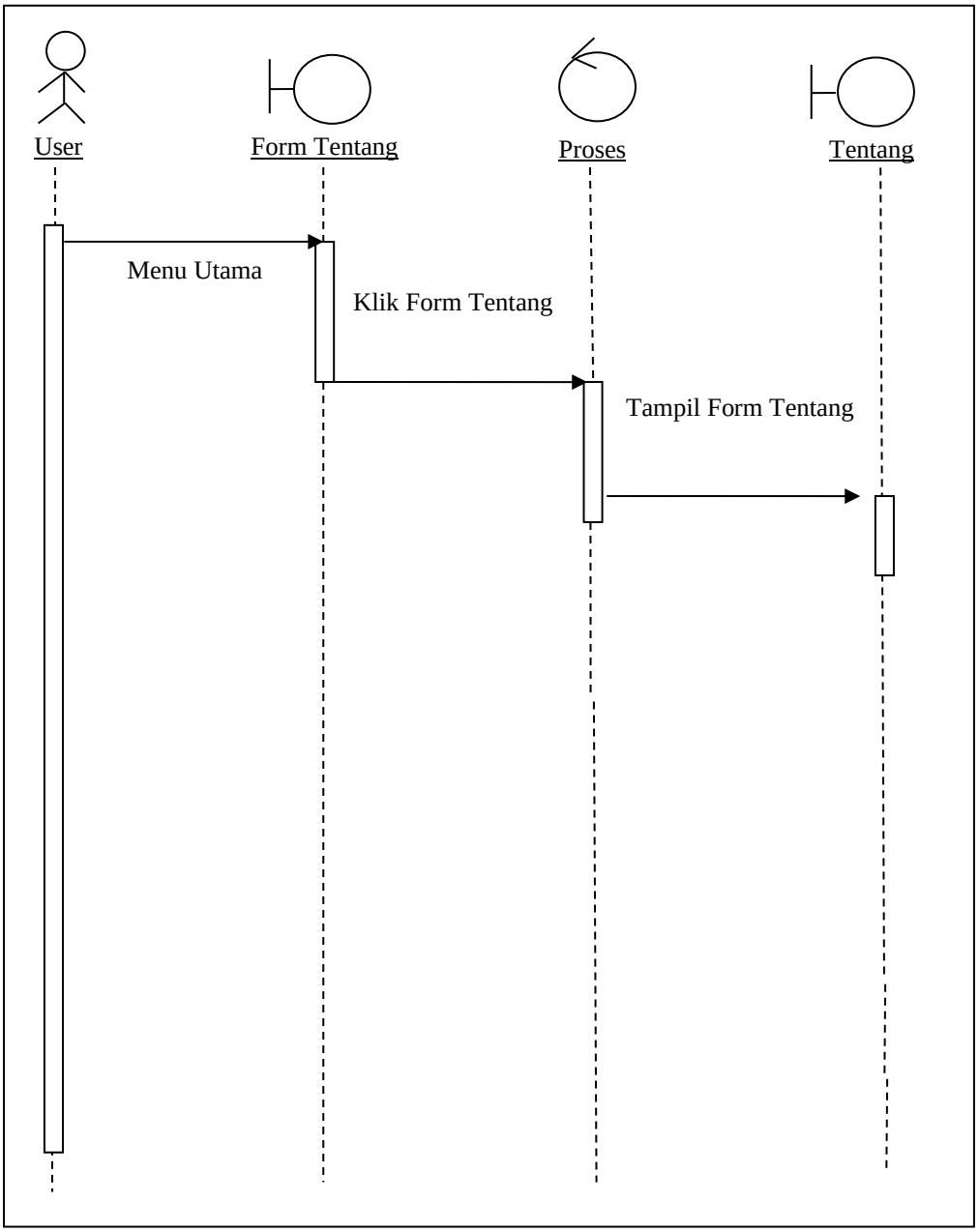
Serangkaian kerja melakukan dekripsi dapat dilihat pada Gambar 3.16. dibawah ini.



Gambar 3.16. *Sequence Diagram* Dekripsi

7. *Sequence Diagram* Tentang

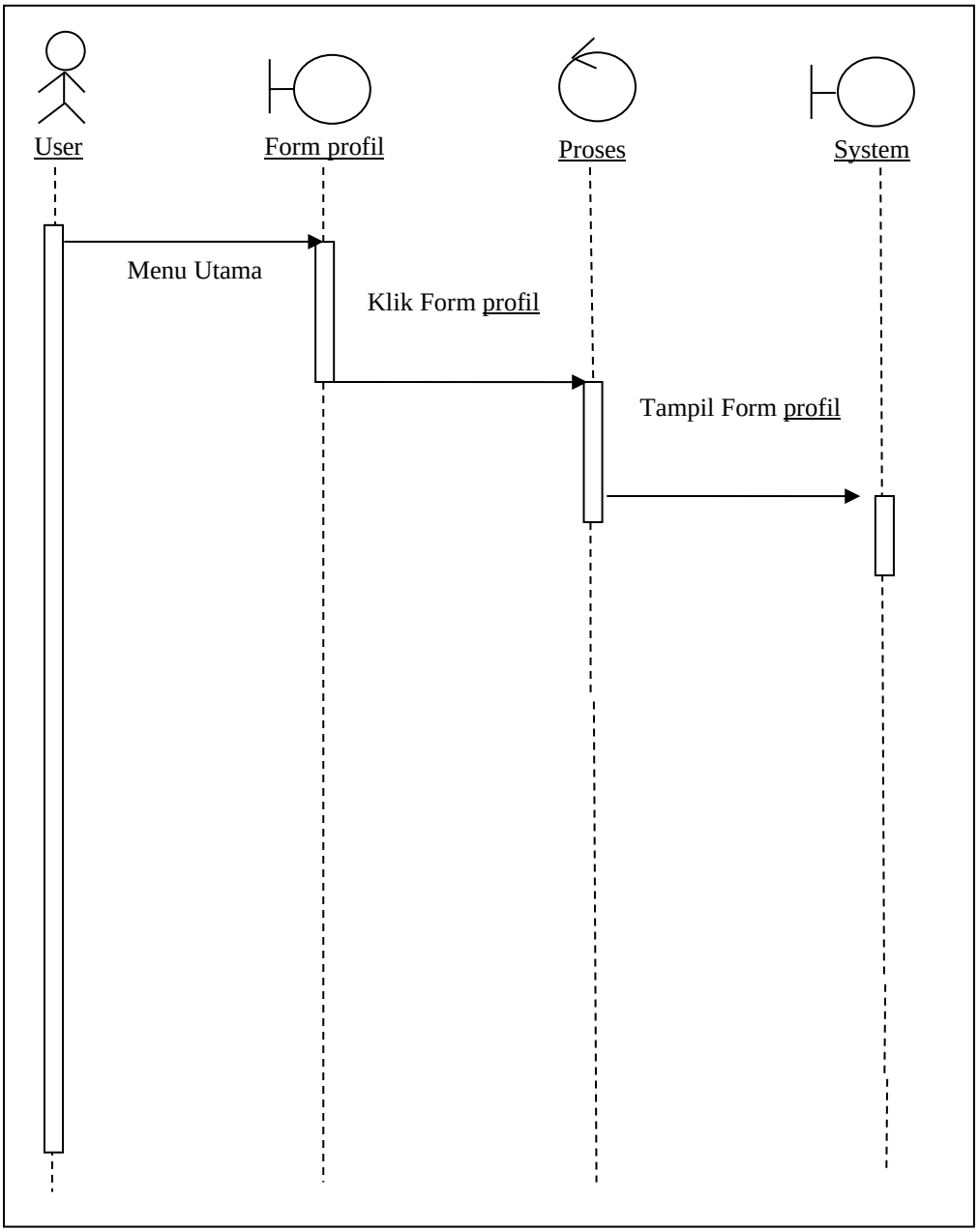
Serangkaian kerja melakukan tentang dapat dilihat pada Gambar 3.17 dibawah ini.



Gambar 3.17 *Sequence Diagram* Tentang

8. *Sequence Diagram* Profil

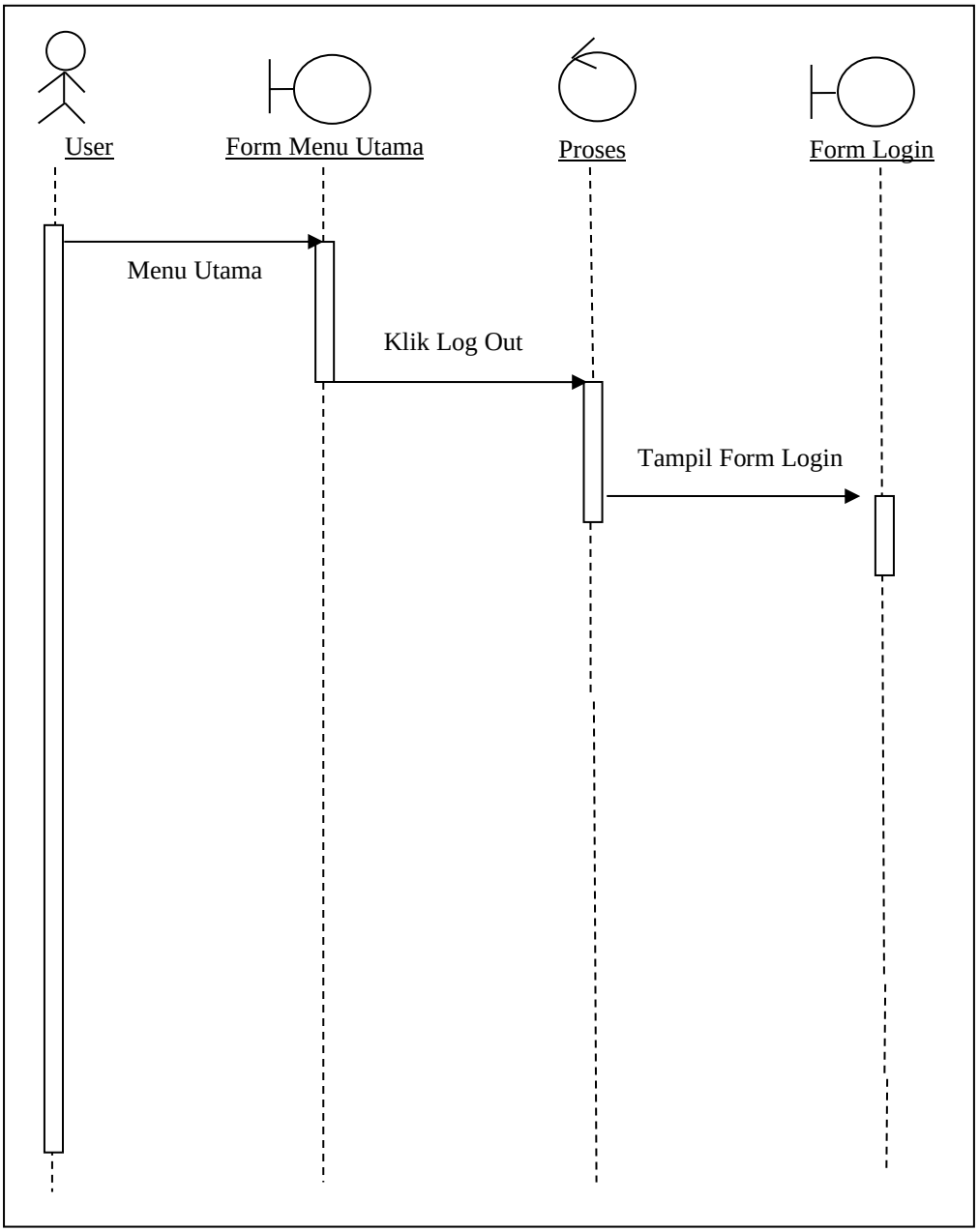
Serangkaian kerja melakukan profil dapat dilihat pada Gambar 3.18 dibawah ini.



Gambar 3.18. *Sequence Diagram* Profil

9. *Sequence Diagram* Log Out

Serangkaian kerja melakukan log out dapat dilihat pada Gambar 3.19 dibawah ini.

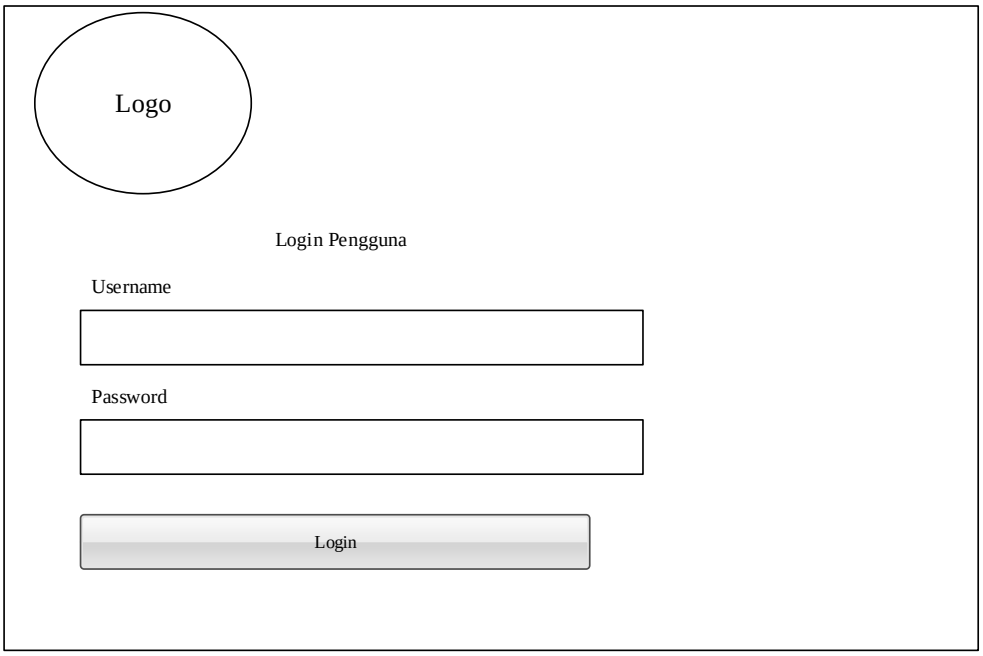


Gambar 3.19 *Sequence Diagram Log Out*

3.3. Desain *Interface*

1. Tampilan *Form Login*

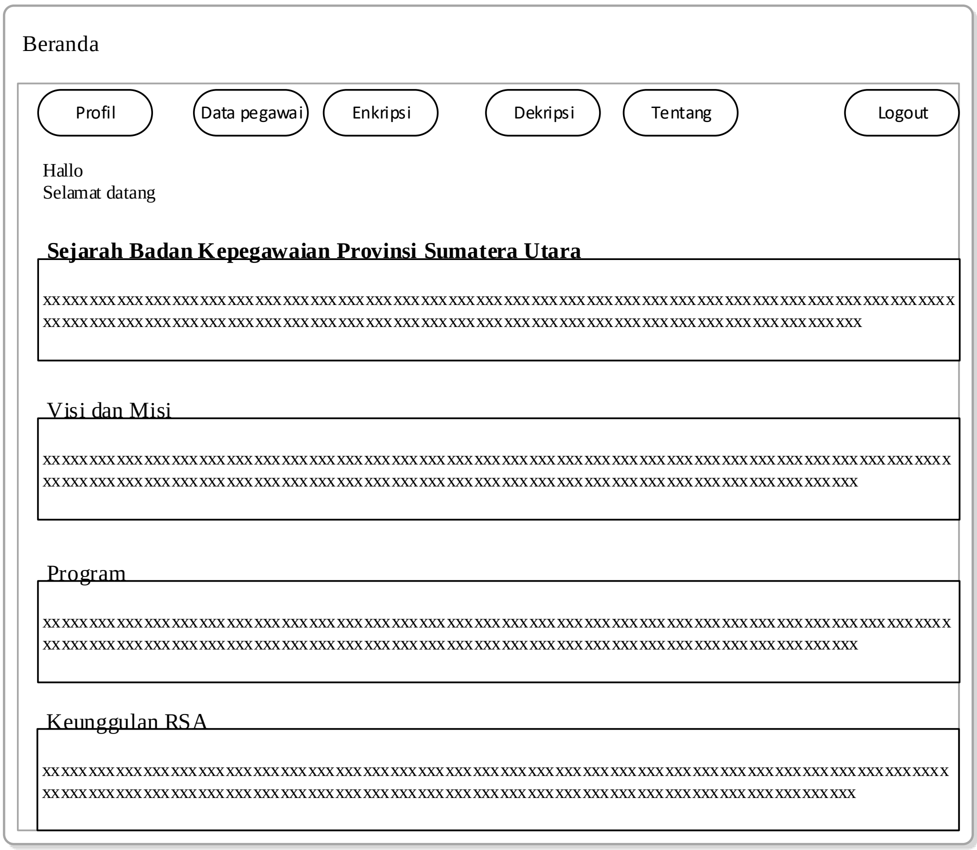
Tampilan sistem *login* yang dilakukan oleh *user* dapat ditunjukkan pada Gambar 3.20



Gambar 3.20. Tampilan *Form Login*

2. Perancangan *Form* Utama

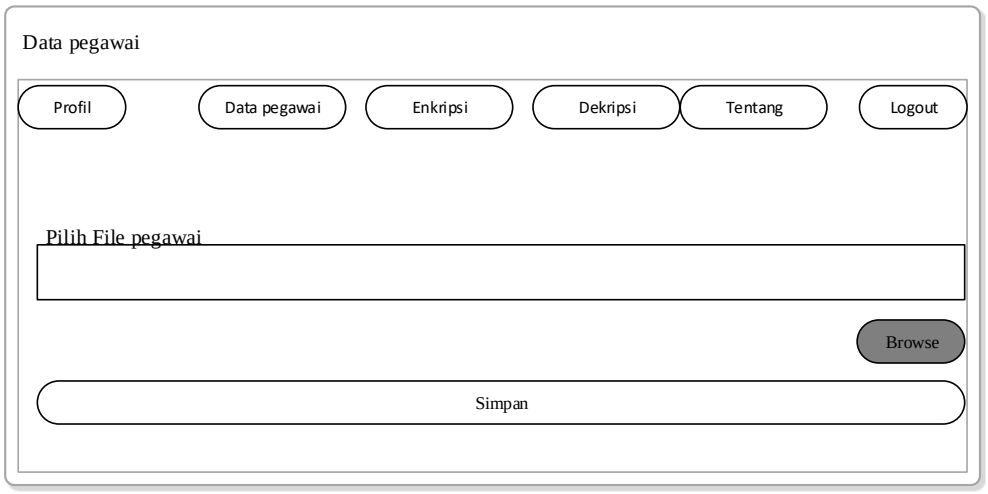
Perancangan *form* Utama ini terdiri dari empat buah *menu bar*. Untuk lebih jelasnya, perancangan *form* Utama dapat dilihat pada Gambar 3.21 sebagai berikut:



Gambar 3.21 Perancangan *Form* Utama

3. Perancangan *Form* Menu Pegawai

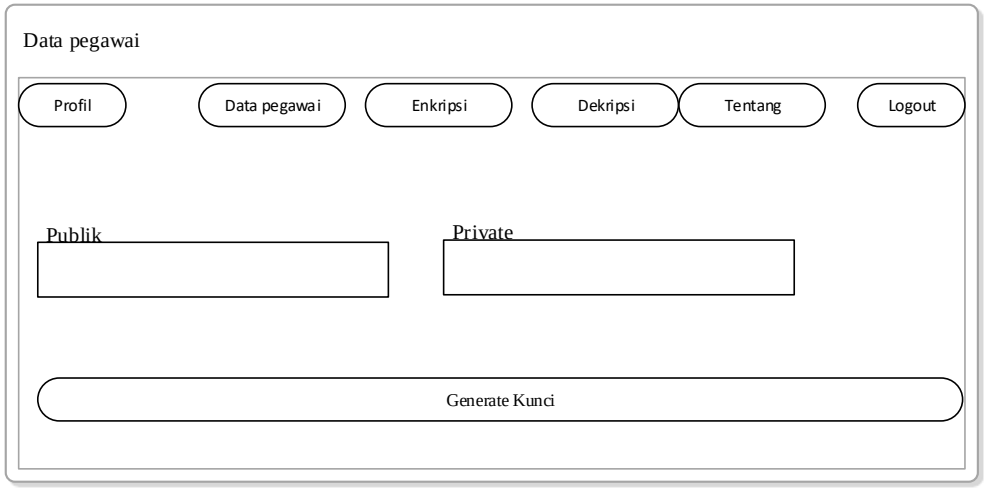
Perancangan *form* menu file ini menampilkan upload data pegawai. Untuk lebih jelasnya, perancangan *form* menu pegawai dapat dilihat pada Gambar 3.22 sebagai berikut:



Gambar 3.22. Perancangan *Form* Menu Pegawai

3. Perancangan *Form* Menu Pembangkit kunci

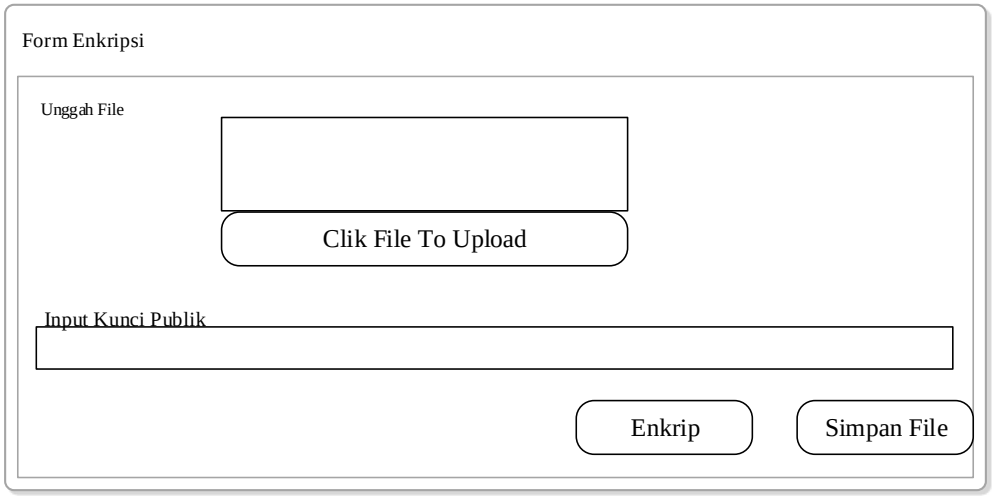
Perancangan *form* menu file ini menampilkan pembangkit kunci. Untuk lebih jelasnya, perancangan *form* menu pembangkit kunci dapat dilihat pada Gambar 3.23 sebagai berikut:



Gambar 3.23. Perancangan *Form* Menu pembangkit kunci

4. Perancangan *Form* Enkripsi

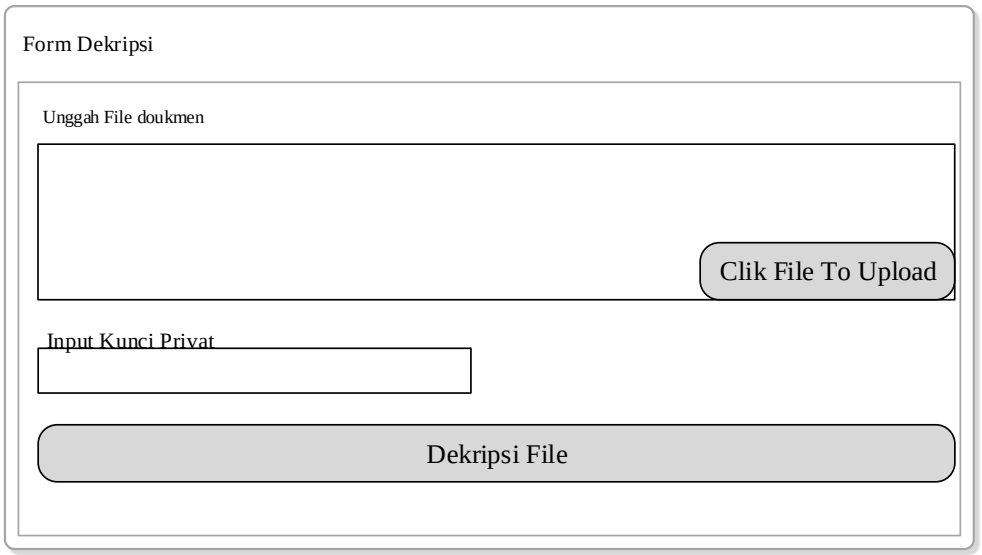
Perancangan *form* Enkripsi, untuk lebih jelasnya, perancangan *form* Enkripsi dapat dilihat pada Gambar 3.24 sebagai berikut:



Gambar 3.24. Perancangan *Form* Enkripsi

5. Perancangan *Form* Dekripsi

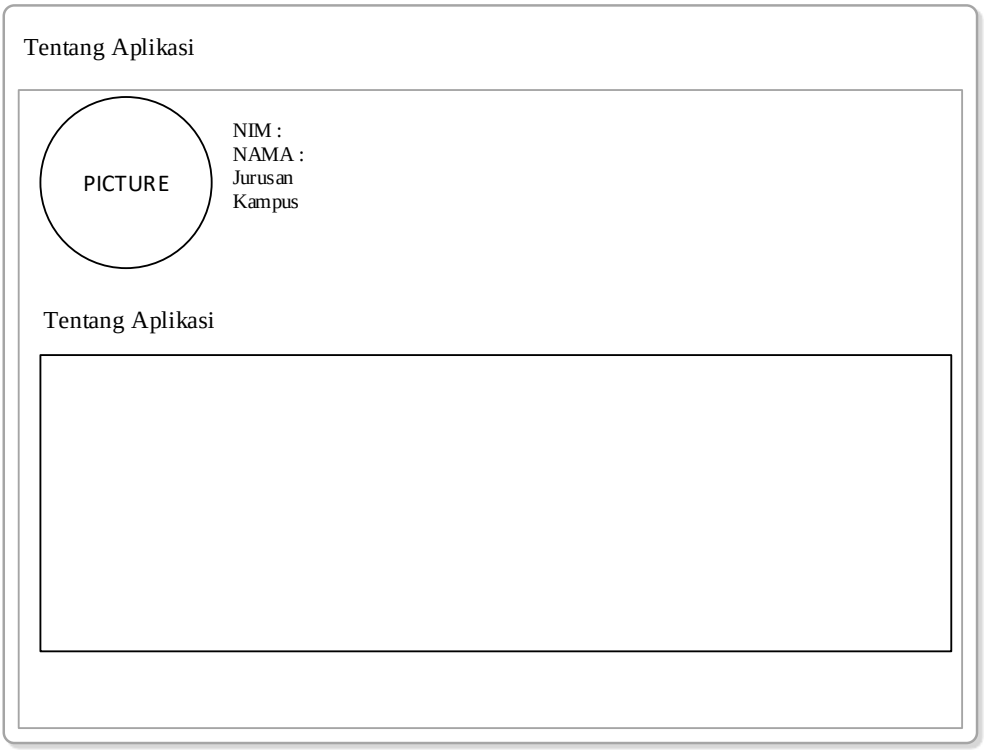
Perancangan *form* Dekripsi, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar 3.25 sebagai berikut:



Gambar 3.25 Perancangan *Form* Dekripsi

6. Perancangan *Form* Tentang

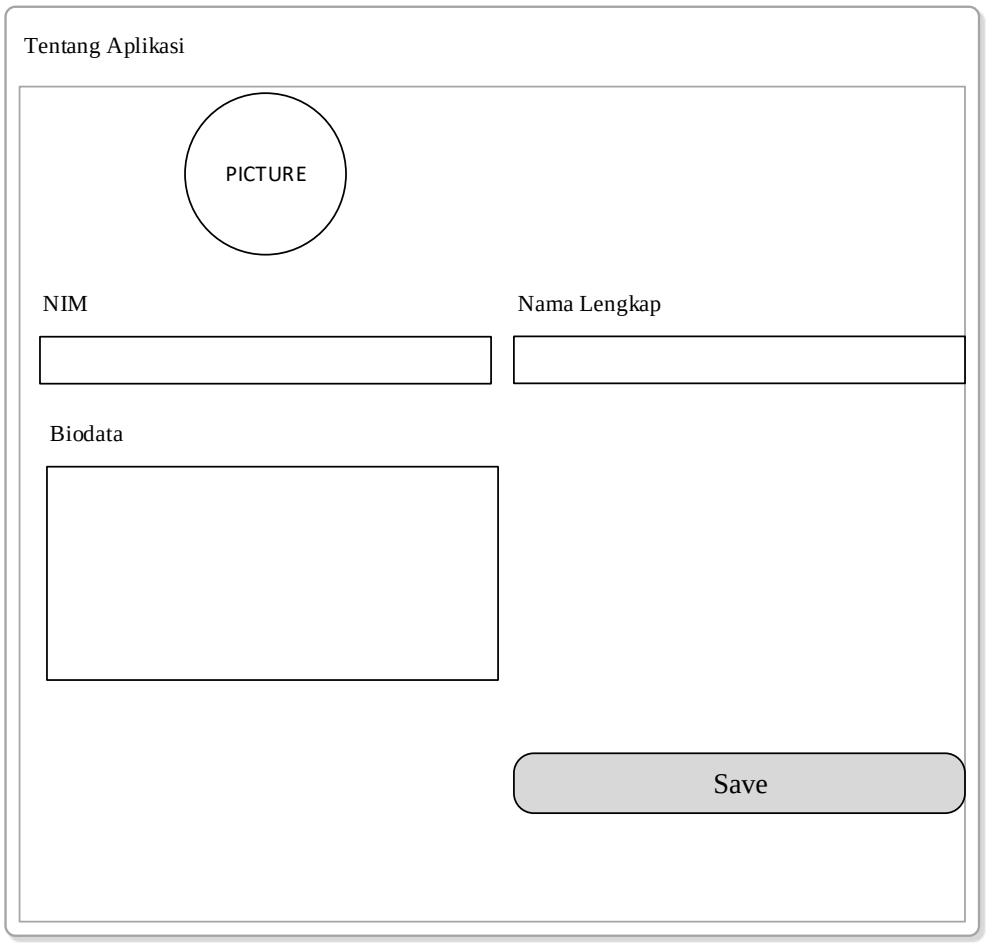
Perancangan *form* tentang, untuk lebih jelasnya, perancangan *form* tentang dapat dilihat pada Gambar 3.26. sebagai berikut:



Gambar 3.26. Perancangan *Form* Tentang

7. Perancangan *Form* Profil

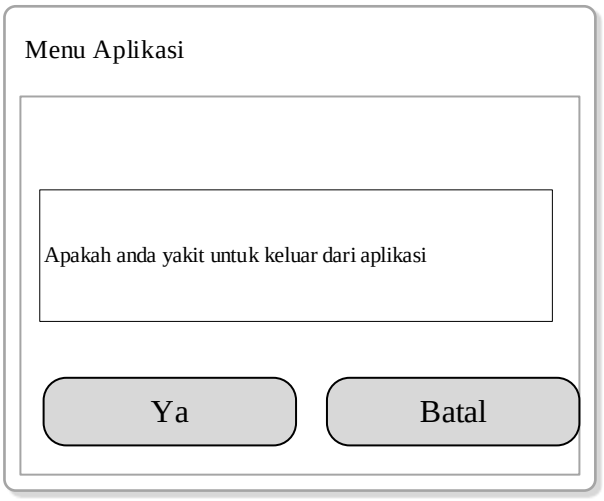
Perancangan *form* profil, untuk lebih jelasnya, perancangan *form* profil dapat dilihat pada Gambar 3.27. sebagai berikut:



Gambar 3.27. Perancangan *Form* Profil

7. Perancangan *Form* Logout

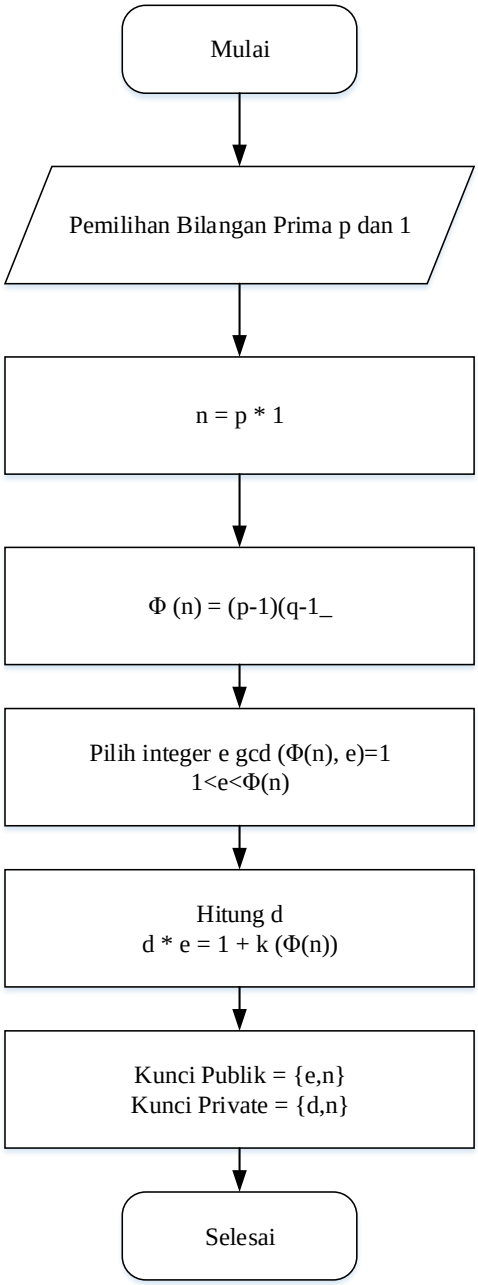
Perancangan *form* logout, untuk lebih jelasnya, perancangan *form* logout dapat dilihat pada Gambar 3.28. sebagai berikut:



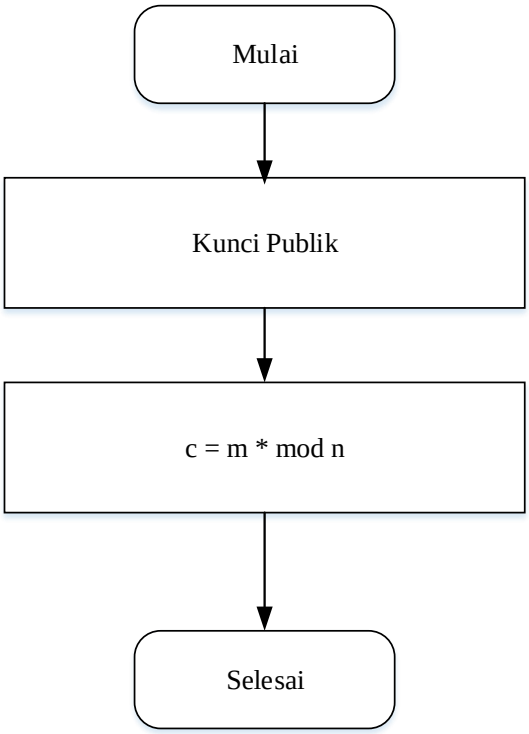
Gambar 3.28. Perancangan *Form* Logout

3.4. Flowcahrt Metode

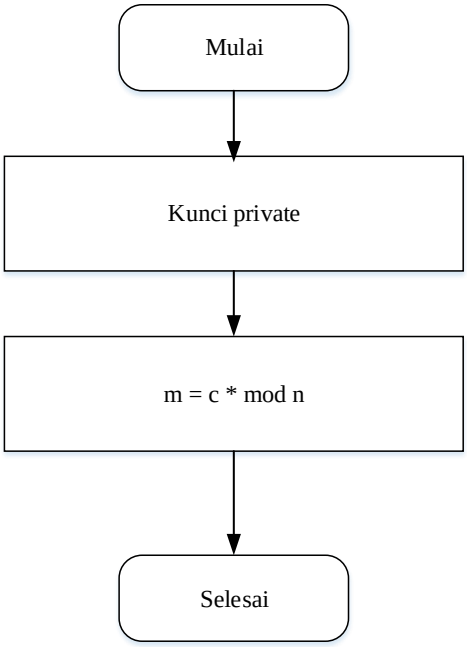
Berikut ini merupakan flowchart dari metode RSA dan flowchart dari penggunaan aplikasi sebagai berikut :



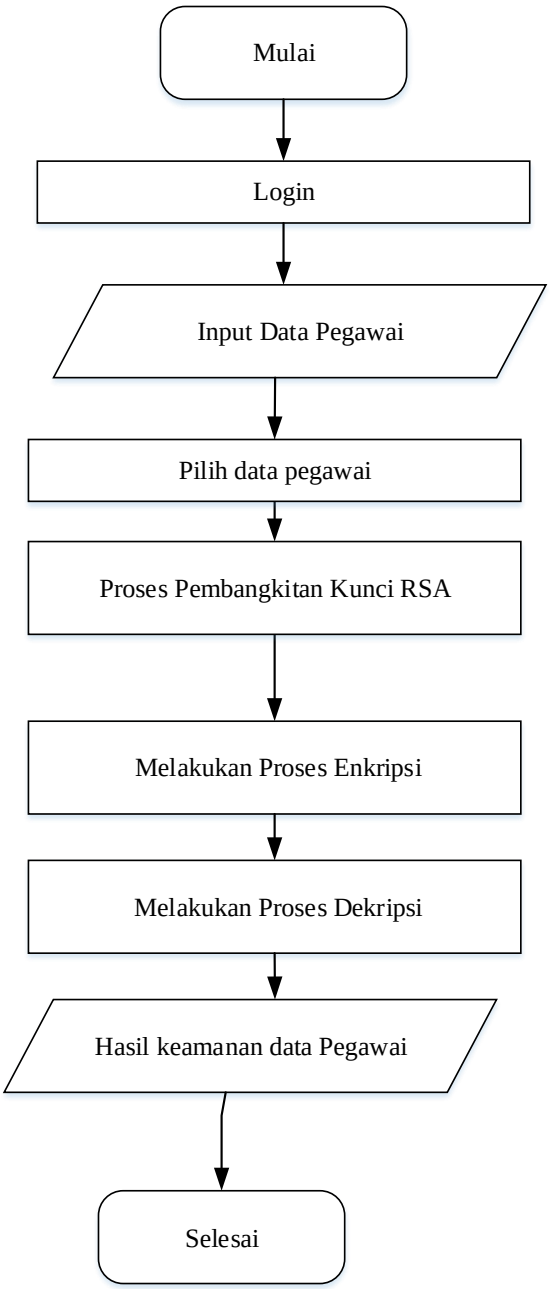
Gambar 3.29. Flowchart Pembangkitan Kunci Metode RSA



Gambar 3.30. Flowchart Enkripsi Metode RSA



Gambar 3.31. Flowchart Dekripsi Metode RSA



Gambar 3.32. Flowchart Aplikasi

BAB IV

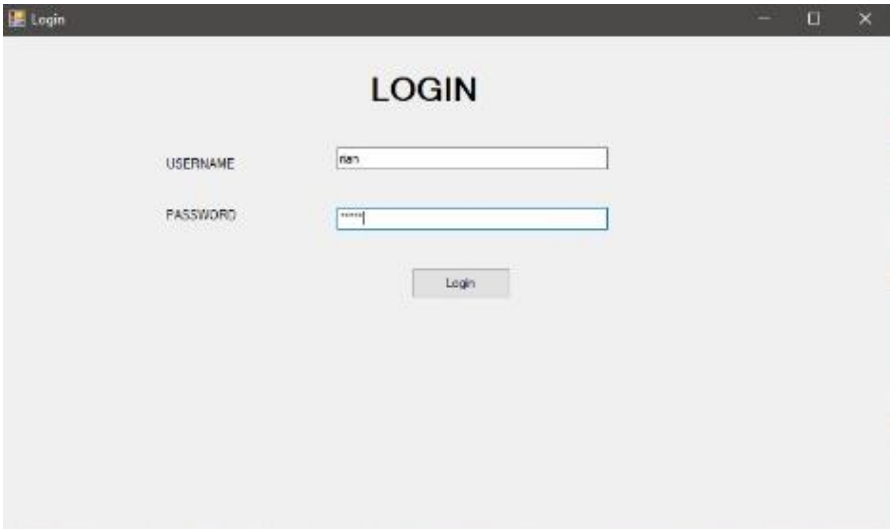
HASIL DAN UJI COBA

4.1. Hasil

Pada bab ini akan dijelaskan tampilan hasil dari aplikasi yang telah dibuat, yang digunakan untuk memperjelas tentang tampilan-tampilan yang ada pada Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA. Sehingga hasil implementasinya dapat dilihat sesuai dengan hasil program yang telah dibuat. Dibawah ini akan dijelaskan tiap-tiap tampilan yang ada pada program.

1. Tampilan Menu *Login*

Tampilan *login* merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai *form input username* dan *password* admin program. Gambar tampilan *login* dapat ditunjukkan pada gambar 4.1 :



Gambar 4.1 Tampilan *Form login*

2. Tampilan *Form* Utama

Form utama merupakan *interface* program kriptografi secara keseluruhan, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* utama. Dalam *form* utama terdapat beberapa menu yaitu, menu *file* dan menu program. Untuk lebih jelasnya tampilan *form* utama dapat dilihat pada Gambar 4.2 dibawah ini.

Gambar 4.2. Tampilan *Form* Utama

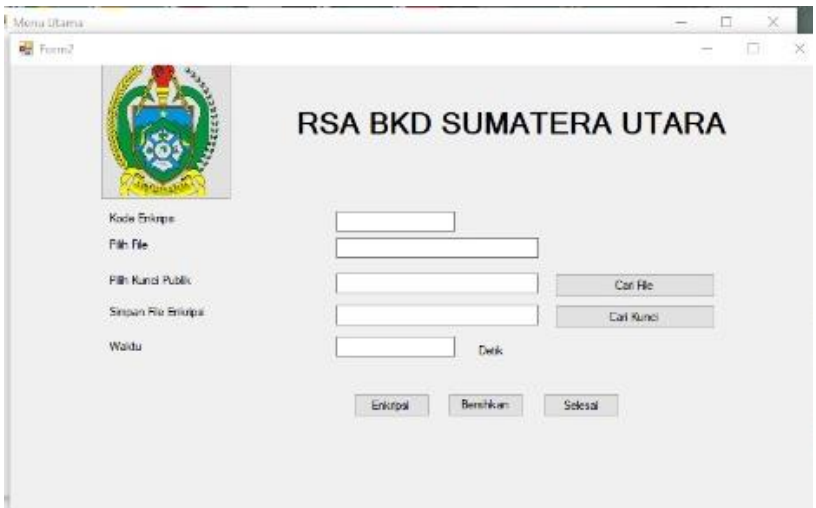
3. Tampilan *Form* Data Enkripsi

Form enkripsi ini berfungsi untuk merubah isi data *file* dalam bentuk *chipretext*, menyimpan hasil enkripsi (*chipertext*), dan keluar dari *form* data enkripsi. Berikut ini tampilan *form* data enkripsi dapat dilihat pada gambar 4.3 berikut ini:

Gambar 4.3. Tampilan *Form* Data Enkripsi

4. Tampilan *Form* Data Dekripsi

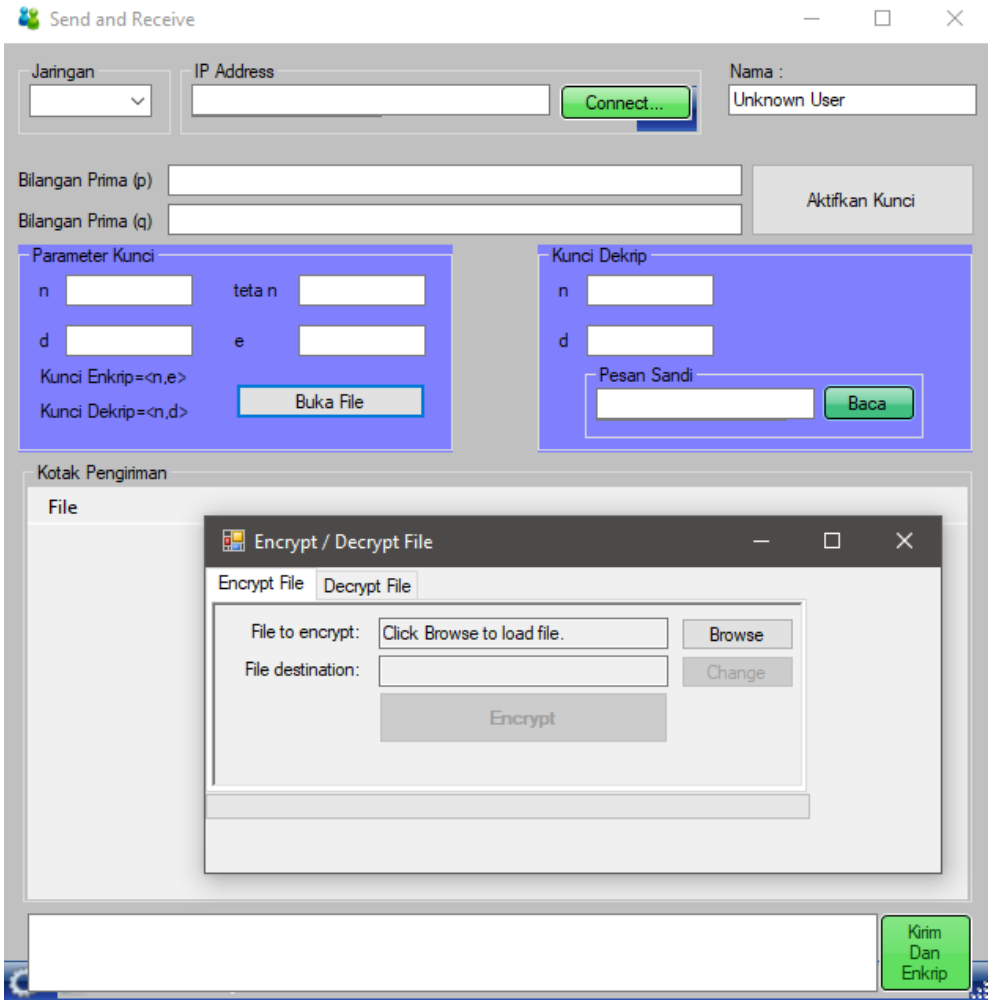
Form dekripsi ini berfungsi untuk upload data yang akan diamankan. Berikut ini tampilan *form* data dekripsi dapat dilihat pada gambar 4.4 berikut ini:



Gambar 4.4. Tampilan *Form* Data Dekripsi

4.1.1. Tampilan Hasil Enkrip

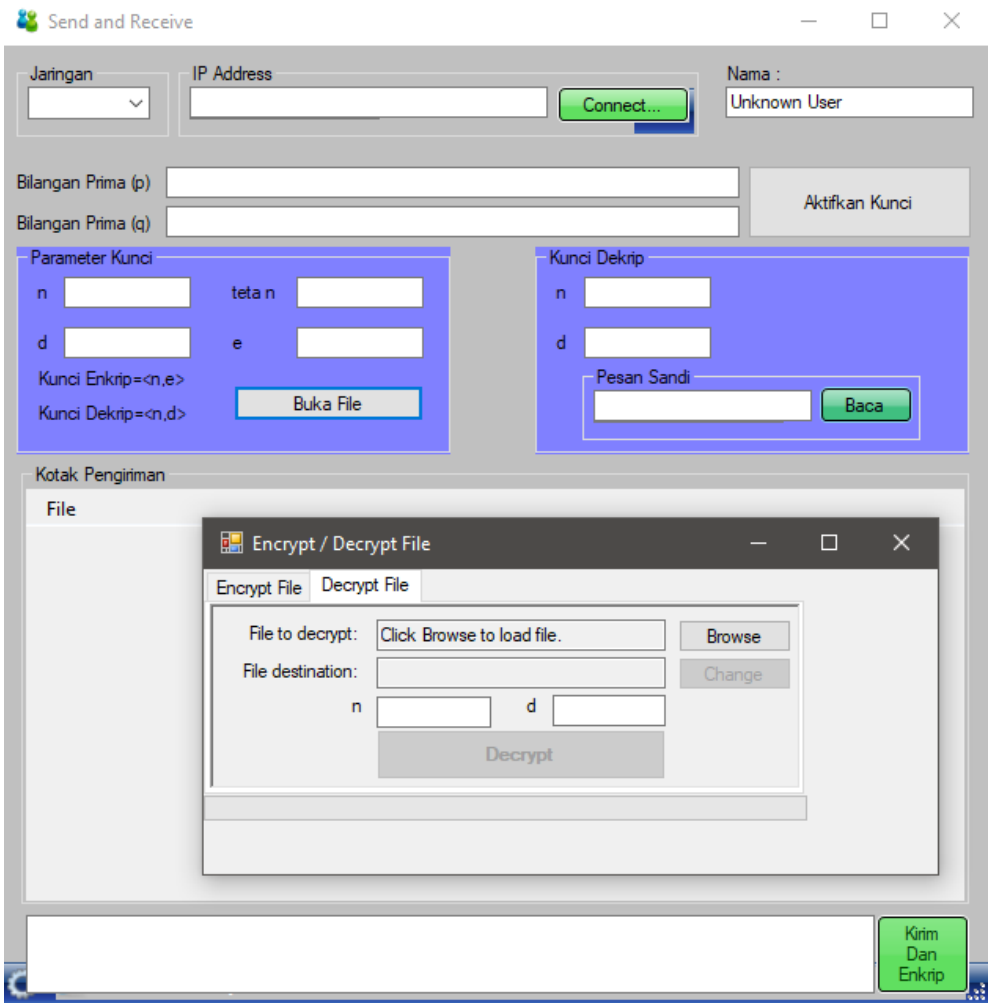
Aplikasi Aplikasi Pengamanan Distribusi Data Kepegawaian Pada Badang Kepegawaian Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA memiliki tampilan sebagai berikut:



Gambar 4.5. Tampilan *Form* Enkrip

4.1.2. Tampilan Hasil Dekrip

Aplikasi Aplikasi Pengamanan Distribusi Data Kepegawaian Pada Badang Kepegawaian Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA memiliki tampilan sebagai berikut:



Gambar 4.6. Tampilan *Form* Dekrip

4.2. Pembahasan

Pembahasan mengenai perangkat keras dan perangkat lunak dalam pembuatan aplikasi Pengamanan Distribusi Data Kepegawaian Pada Badang Kepegawaian Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA dijabarkan sebagai berikut:

1. Perangkat keras laptop dengan spesifikasi sebagai berikut:
    a. Processor Minimal Core 2 duo
    b. RAM minimal 4 Gb
    c. Hardisk minimal 80 Gb

2. Perangkat Lunak dengan spesifikasi sebagai berikut:
    a. OS Windows
    b. Visual Studio 2019
    c. Microsoft Word

4.2.1 Uji Coba

Uji coba pada Aplikasi Aplikasi Pengamanan Distribusi Data Kepegawaian Pada Badang Kepegawaian Sumatera Utara Dengan Memanfaatkan Algoritma Kriptografi Asimetris RSA menggunakan *blackbox testing* sebagai berikut:

Tabel 4.1. *Blackbox Testing Form* Enkrip

No	Form Enkrip	Hasil Uji	Validasi
1	Klik tombol connect	Aplikasi menghubungkan jaringan ke aplikasi	Sesuai
2	Klik tombol aktifkan kunci	Aplikasi menampilkan kunci e, d, n dan teta n	Sesuai
3	Klik tombol buka file dan jika melakukan enkrip maka pilih file dan klik enkrip	Aplikasi akan mengenkrip file	Sesuai
4	Klik tombol file dan kirim	Aplikasi akan mengirim file ke client	Sesuai

Tabel 4.2. *Blackbox Testing Form* Dekrip

No	Form Dekrip	Hasil Uji	Validasi
1	Klik tombol connect	Aplikasi menghubungkan jaringan ke aplikasi	Sesuai
2	Klik tombol aktifkan kunci	Aplikasi menampilkan kunci e, d, n dan teta n	Sesuai
3	Klik tombol buka file dan jika melakukan dekrip maka pilih file dan klik dekrip	Aplikasi akan mengdekrip file	Sesuai
4	Klik tombol file dan kirim	Aplikasi akan mengirim file ke server	Sesuai

4.2.2. Metode RSA

Langkah-langkah metode RSA untuk enkrip dapat dilihat sebagai berikut :

1. Enkrip Metode RSA

Berikut ini adalah enkrip dari metode RSA, enkrip metode RSA menggunakan fungsi eksponensial dalam modular n sebagai berikut :

$C_i = P_i^e \bmod n$

Keterangan :

C_i = *Ciphertext* hasil enkrip

P_i = *Plaintext* yang akan dienkrip

e = Fungsi eksponensial

mod = Sisa Bagi/Modulus

n = Hasil perkalian dua buah bilangan prima

Contoh Kasus :

a. Pembentukan Kunci :

1. Menentukan dua buah bilangan prima

Tentukan dua buah bilangan prima besar dengan ketentuan kedua bilangan prima tidak boleh sama.

$P_1 = 31$

$P_2 = 37$

2. Mencari nilai n

Untuk mendapatkan nilai n, maka gunakan rumus berikut :

$n = P_1 \times P_2$

$= 31 \times 37$

$= 1147$

3. Mencari nilai θn

Untuk mencari nilai θn gunakan rumus berikut :

$\theta n = (P_1 - 1) \times (P_2 - 1)$

$\theta n = (31 - 1) \times (37 - 1)$

$\theta n = 30 \times 36$

$\theta n = 1080$

4. Mencari nilai e

Untuk menentukan nilai e, gunakan algoritma berikut :

e = 2

While θn mod e ≠ 0

e = e + 1

End While

Artinya :

Sampai θn mod e ≠ 0, lakukan e = e + 1. Proses berhenti ketika nilai 0n dibagi dengan nilai e memiliki sisa bagi tidak sama dengan nilai 0, maka akan didapat nilai e.

e = 3

Iterasi Pertama :

θn mod e = 1080 mod 3

= 0

e = 3 + 1

e = 4

Iterasi Kedua :

θn mod e = 1080 mod 4

= 0

e = 4 + 1

e = 5

Iterasi Ketiga :

θn mod e = 1080 mod 5

= 0

e = 5 + 1

e = 6

Iterasi Keempat :

θn mod e = 1080 mod 6

= 0

e = 6 + 1

e = 7

Iterasi Kelima :

θn mod e = 1080 mod 7

= 2

Proses berhenti pada iterasi kelima, maka telah didapat nilai e = 7.

5. Mencari nilai d

Untuk mencari nilai d, maka dapat digunakan teorema *extended euclid* sebagai berikut :

$U_1 = 1$

$U_2 = 0$

$U_3 = \theta n$

$V_1 = 0$

$V_2 = 1$

$V_3 = e$

While $V_3 = 0$

$Q = Int(U_3 / V_3)$

$N_1 = U_1 - (Q \times V_1)$

$N_2 = U_2 - (Q \times V_2)$

$N_3 = U_3 - (Q \times V_3)$

$U_1 = V_1$

$U_2 = V_2$

$U_3 = V_3$

$V_1 = N_1$

$V_2 = N_2$

$V_3 = N_3$

End While

Artinya :

Sampai $V_3 = 0$, lakukan teorema *extended euclid*. Proses berhenti ketika nilai V_3 sama dengan nilai 0, maka akan didapat nilai d.

$U_1 = 1$

$U_2 = 0$

$U_3 = \theta n$

$V_1 = 0$

$V_2 = 1$

$V_3 = e$

Iterasi Pertama :

$Q = Int(U_3 / V_3)$

$= Int(1080 / 7)$

$= 154$

$N_1 = U_1 - (Q \times V_1)$

$= 1 - (154 \times 0)$

$= 1$

$N_2 = U_2 - (Q \times V_2)$

$= 0 - (154 \times 1)$

$= -154$

$N_3 = U_3 - (Q \times V_3)$

$= 1080 - (154 \times 7)$

$= 1080 - 1078$

$= 2$

$U_1 = 0$

$U_2 = 1$

$U_3 = 7$

$V_1 = 1$

$V_2 = -154$

$V_3 = 2$

Iterasi Kedua :

$Q = Int(U_3 / V_3)$

$= Int(7 / 2)$

$= 3$

$N_1 = U_1 - (Q \times V_1)$

$= 0 - (3 \times 1)$

$= -3$

$N_2 = U_2 – (Q \times V_2)$

$= 1 – (3 \times -154)$

$= 463$

$N_3 = U_3 - (Q \times V_3)$

$= 7 - (3 \times 2)$

$= 7 - 6$

$= 1$

$U_1 = 1$

$U_2 = -154$

$U_3 = 2$

$V_1 = -3$

$V_2 = 463$

$V_3 = 1$

Iterasi Ketiga :

$Q = Int(U_3 / V_3)$

$= Int(2 / 1)$

$= 2$

$N_1 = U_1 - (Q \times V_1)$

$= 1 - (2 \times -3)$

$= 7$

$N_2 = U_2 - (Q \times V_2)$

$= -154 - (2 \times 463)$

$= -154 - 926$

$= - 1080$

$N_3 = U_3 - (Q \times V_3)$

$= 2 - (2 \times 1)$

= 2 - 2

= 0

$U_1 = -3$

$U_2 = 463$

$U_3 = 1$

$V_1 = 7$

$V_2 = -1080$

$V_3 = 0$

Proses berhenti ketika $V_3 = 0$, maka telah didapat nilai d = 463.

Maka telah diperoleh kunci *private* untuk enkrip sebagai berikut :

e = 7

n = 1147

Dan diperoleh kunci *public* untuk dekrip sebagai berikut :

d = 463

n = 1147

b. Enkrip *Plaintext*

Contoh Proses Enkrip :

Plaintext : UTAMA

Enkrip Pertama :

Enkrip Pertama :

U = 85

$C_i = P_i^e \bmod n$

$= 85^7 \bmod 1147$

= 32057708828125 mod 1147

= 122

Enkrip Kedua :

T = 84

$C_i = P_i^e \bmod n$

$= 84^7 \bmod 1147$

= 29509034655744 mod 1147

= 269

Enkrip Ketiga :

A = 65

$C_i = P_i^e \bmod n$

$= 65^7 \bmod 1147$

= 4902227890625 mod 1147

= 761

Enkrip Keempat :

M = 77

$C_i = P_i^e \bmod n$

$= 77^7 \bmod 1147$

= 16048523266853 mod 1147

= 1077

Enkrip Kelima :

A = 65

$C_i = P_i^e \bmod n$

$= 65^{7} \bmod 1147$

$= 4902227890625 \bmod 1147$

$= 761$

2. Dekrip Metode RSA

Berikut ini adalah dekrip dari metode RSA, dekrip metode RSA merupakan fungsi eksponensial dalam modular n dengan menggunakan kunci *private* sebagai berikut :

$P_i = C_i^{d} \bmod n$

Keterangan :

P_i = *Plaintext* hasil dekrip

C_i = *Ciphertext* yang akan didekrip

d = Fungsi eksponensial kunci *public*

mod = Sisa Bagi/Modulus

n = Fungsi perkalian dua bilangan prima

1. Terima kunci

d = 463

n = 1147

2. Dekrip *Ciphertext*

Contoh Proses Dekrip :

Dekrip Pertama :

C = 122

$P_i = C_i^{d} \bmod n$

$= 122^{463} \bmod 1147$

= 9,651650840205358246697375194232 1e+965 mod 1147

= 85 = U

Dekrip Kedua :

C = 269

$P_i = C_i^d \bmod n$

= $269^{463} \bmod 1147$

= 9,447255068259840601634893182 32e+1124 mod 1147

= 84 = T

Dekrip Ketiga :

C = 761

$P_i = C_i^d \bmod n$

= $648^{463} \bmod 1147$

= 5,744175735220589484373442905 2717e+1301 mod 1147

= 65 = A

Dekrip Keempat :

C = 1077

$P_i = C_i^d \bmod n$

= $1077^{463} \bmod 1147$

= 8,238926470782347878069839749 4152e+1403 mod 1147

= 77 = M

Dekrip Kelima :

C = 761

$P_i = C_i^d \bmod n$

= 761^{463} mod 1147

= 1,20530257608012423327223965893 04e+1334 mod 1147

= 65 = A

Plaintext : UTAMA

4.2.3. Hasil Uji Coba

Hasil uji coba terhadap sistem secara manual dan praktek memiliki hasil sebagai berikut:

1. Koneksi dari aplikasi ke basis data SQL Server berjalan dengan baik.
2. Proses dari enkripsi teks telah berjalan dengan baik.
3. Proses dari dekripsi teks telah berjalan dengan baik.
4. Perhitungan teori dengan perhitungan aplikasi telah sesuai.
5. Penggunaan aplikasi yang sederhana.

4.3. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

4.3.1. Kelebihan Sistem

Adapun kelebihan sistem yang telah dibuat diantaranya yaitu :

1. Aplikasi yang telah dibuat dapat merahasiakan isi teks di dalam basis data modal penjualan.
2. Aplikasi yang telah dibuat menggunakan dua metode sehingga menguatkan kerahasiaan data teks.

3. Aplikasi dapat menyimpan hasil enkripsi dan dekripsi data ke dalam *database* SQL Server.

4.3.2. Kekurangan Sistem

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu :

1. Aplikasi yang telah dibuat tidak menggunakan satu metode.
2. Aplikasi yang telah dibuat tidak dapat membaca data per *database*.

Aplikasi yang telah dibuat tidak memiliki petunjuk penggunaan

BAB V

KESIMPULAN DAN SARAN

V.1. Kesimpulan

Berdasarkan hasil pambahasan dan uji coba yang telah dilakukan, dapat disimpulkan :

1. Aplikasi Telah dibangun dan dapat memanipulasi data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara dengan system penyandian Aplikasi algoritma *RSA.*
2. Sistem yang dibangun sudah mampu melakukan enkripsi dan dekripsi terhadap data Sehingga dapat Melindungi data-data Kepegawaian Pada Badan Kepegawaian Provinsi Sumatera Utara Dengan Menggunakan Metode *RSA.*
3. Sistem yang dibangun mempunyai tampilan yang sangat sederhana dan mudah digunakan oleh *user* .

V.2. Saran

Untuk menyempurnakan aplikasi ini maka diberikan saran :

1. Diharapkan untuk dikembangkan agar dalam mengunakan kata kunci pada sistem yang dibangun, boleh ada huruf yang sama didalam kata kunci. Hal ini agar saat pemilihan kata kata kunci, *user* bebas membuat kata kunci sesuai dengan keinginan *user*.

2. Diharapakan untuk dikembangkan agar proses enkripsi (*chipertext*) dengan sistem yang dibuat dapat menghasilkan data yang berbeda.
3. Melakukan perkembangan performance aplikasi untuk membuat pengguna tidak bosan dalam penggunaan aplikasi

DAFTAR PUSTAKA

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) untuk Mengamankan Data Keuangan. *JIKOMSI [Jurnal Ilmu Komputer Dan Sistem Informasi]*, *4*(2),75–85. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

Ferdy Riza (2018) Analisa Frekuensi Hasil Enkripsi Pada Algoritma Kriptografi Blowfish Terhadap Keamanan Informasi

Fitriyani A, Handayani R, & Widanengsih E. (2020). Sistem Pendukung Keputusan Pemilihan Jurusan Pada SMK YMIK Joglo Jakarta Barat Menggunakan Metode Simple Additive Weigting (SAW). *Jtksi*, *03*(01), 11–19.

Janis, J. W., Mamahit, D. J., Sugiarso, B. A., Rumagit, A. M., Elektro, T., Sam, U., & Manado, R. (2020). Rancang Bangun Aplikasi Online Sistem Pemesanan Jasa Tukang Bangunan Berbasis Lokasi. *Jurnal Teknik Informatika*, *15*(1), 1–12. https://doi.org/10.35793/jti.15.1.2020.29023

Kaban, R., Yunita, W., & Faradillah, Y. (2019). Aplikasi Pemesanan Tiket Bus Berbasis Android (Study Kasus : Pt . Als Terminal Pasar X Tanjung Beringin). *Jurnal Manajemen …*, *32*(1).

Lubis, R. S., Tulus, & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig- Zag dalam Hybrid Crypto Sistem. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, *6*(2), 185–189.

Marpaung, R., & Informasi, T. (2022). *PENYIMPANAN DATA PRIBADI DENGAN METODE*. *2*(11), 1–14.

Muharromin, M., Informatika, J. T., & Darma, U. B. (n.d.). *Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache*. 393–402.

Nugroho, A. P., & Suseno, H. B. (2020). Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES. *"QUERY: Jurnal Sistem Informasi Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES.,"* *04*(April), 9–17. http://jurnal.uinsu.ac.id/index.php/query/article/view/8007/3720

Perbawa, K. A. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game Penerapan Algoritma Linear Congruential Generator (LCG) dalam Game Edukasi Matematika Berbasis Android. *Jurnal Komputer, Informasi Dan Teknologi*, *2*(1), 47–56.

Prayudha, J., _ S., & _ I. (2019). Implementasi Keamanan Data Gaji

Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES). *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *18*(2), 119. https://doi.org/10.53513/jis.v18i2.150

Ruing, M. O. I., & Ujianto, E. I. H. (2020). *Penerapan Kombinasi Algoritma Kriptografi (Caesar, Vigenere, Zig-Zag) Dan Metode Steganografi Lsb Untuk Mengamankan Pesan Ke Dalam Citra Digital*. 1–8. http://eprints.uty.ac.id/4888/

Setiaji, A. (2020). RANCANG BANGUN APLIKASI PEMESANAN DESAIN JERSEY BERBASIS ANDROID DENGAN MENGGUNAKAN TEKNOLOGI FIREBASE (Studi Kasus : Konfeksi Minister). *Jurnal Sistem Informasi Dan Sains Teknologi*, *2*(2). https://doi.org/10.31326/sistek.v2i2.664

Sitepu, D. A., Nurhayati, & Khair, H. (2022). Implementasi Pengamanan Data Koperasi Menggunakan Algoritma Advanced Encryption Standard (AES). *CITISEE 2016 Proceedings*, *6*(1), 37–40. https://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/8__Amikom_Purwokerto_Implementasi_Pengamanan_Data_Koperasi_Menggunakan_Algoritma_Advanced_Encryption_Standard_(Aes).pdf

Suparman, B. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebasis Java Desktop. *OKTAL: Jurnal Ilmu Komputer Dan Sains*, *1*(07), 808–817. https://journal.mediapublikasi.id/index.php/oktal/article/view/777%0A https://journal.mediapublikasi.id/index.php/oktal/article/download/777/304

Waruwu, E. V., Nugroho, N. B., & Sonata, F. (2022). Penerapan Digital Signature Menggunakan Metode RSA Untuk Verifikasi Surat Keterangan Keaslian Ijazah SMA Swasta Bina Artha. *Jurnal Cyber Tech*, *1*(1).

Sandy, C. L. M., Fadlisyah, F., & Rizal, R. A. (2023). Sistem Informasi E-Voting Berbasis Web Menggunakan Metode RSA dan Base64. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(1), 200-206.

Putra, A. C., Simanjuntak, M., & Nurhayati, N. (2022). PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENGAMANKAN DATABASE PROGRAM KELUARGA HARAPAN (PKH). *JTIK (Jurnal Teknik Informatika Kaputama)*, *5*(1), 76-84.

Ardiansyah, A. F. (2023). Pemanfaatan Digital Signature pada Sertifikat Digital Berbasis Blockchain. *Authentication Authorization Accounting Pendidikan Teknologi Informasi dan Teknologi Informasi*, *1*(2), 103-107.

Muis, M. D., Sukarno, P., & Wardana, A. A. (2022). Analisis Dan Implementasi Sistem Pendeteksi Ijazah Dan Transkrip Palsu Dengan Menggunakan Ipfs Dan Smart Contract Blockchain. *eProceedings of Engineering*, *8*(5).

Lubis, R. S., Tulus, T., & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA–LUC dan Algoritma Zig-Zag dalam Hybrid Crypto Sistem. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, *6*(2), 186-189.

Listiani, I., Nasution, M. S., Sari, W. I., & Nasution, A. B. (2022). PERANCANGAN KEAMANAN DATA PASIEN DI KLINIK KECANTIKAN RATU BEAUTY STUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *4*(4), 437-443.

Fauzan, D. A., & Fathurrozi, A. (2023). Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web. *Journal of Informatic and Information Security*, *4*(1), 91-104.

Sumiah, A., & Hakim, R. R. (2020). IMPLEMENTASI METODE LINEAR CONGRUENTIAL GENERATOR PADA GAME PUZZLE BERBASIS ANDROID. *JEJARING: Jurnal Teknologi dan Manajemen Informatika*, *5*(1), 1-10.

Abi Perbawa, K., & Diana, D. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game. *Jurnal Komputer, Informasi dan Teknologi (JKOMITEK)*, *2*(1), 47-56.

Putra, B. J. M., Fuâ, A., & Yuniarti, D. A. F. (2022). Analisa dan Rancangan Sistem Informasi Pariwisata Pacitan dengan UML dan ERD. *Information System For Educators And Professionals: Journal of Information System*, *7*(1), 63-72.

Andikos, A. (2019). Perancangan aplikasi multimedia interaktif sebagai media pembelajaran pengenalan hewan pada tk islam bakti 113 koto salak. *Jurnal Sakinah*, *1*(1), 34-49.

LAMPIRAN

Lampiran 1 Surat Izin Penelitian

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Nomor : 47/II.3-AU/UMSU-09/F/2024 Medan, 13 Dzulqa'dah 1445 H
Lampiran : - 21 Mei 2024 M
Perihal : **IZIN RISET PENDAHULUAN**

Kepada Yth.

Bapak/Ibu Pimpinan
Badan Kepegawaian
Pemerintah Provinsi Sumatera Utara
Jl. Teuku Daud No. 5 Madras Hulu, Medan Polonia 20152

Di tempat

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dengan hormat, sehubungan mahasiswa kami akan menyelesaikan studi,untuk itu kami memohon kesediaan Bapak / Ibu untuk memberikan kesempatan pada mahasiswa kami melakukan riset di **Perusahaan / Instansi** yang Bapak / Ibu pimpin, guna untuk penyusunan skripsi yang merupakan salah satu persyaratan dalam menyelesaikan Program **Studi Strata Satu (S-1)**

Adapun Mahasiswa/i di Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara tersebut adalah:

Nama	**: NOPRIAN SYAHPUTRA**
Npm	**: 2009010093**
Jurusan	**: Sistem Informasi**
Semester	**: VIII**
Judul	**: Pengamanan Distribusi Data Kepegawaian Pada Badan Kepegawaian Sumatera Utara Dengan memanfaatkan Algoritma Kriptografi Asimetris RSA**
Email	**: riannopriansyahputra@gmail.com**
Hp/Wa	**: 082273329460**

Demikianlah surat kami ini, atas perhatian dan kerjasama yang Bapak / Ibu berikan kami ucapkan terimaksih

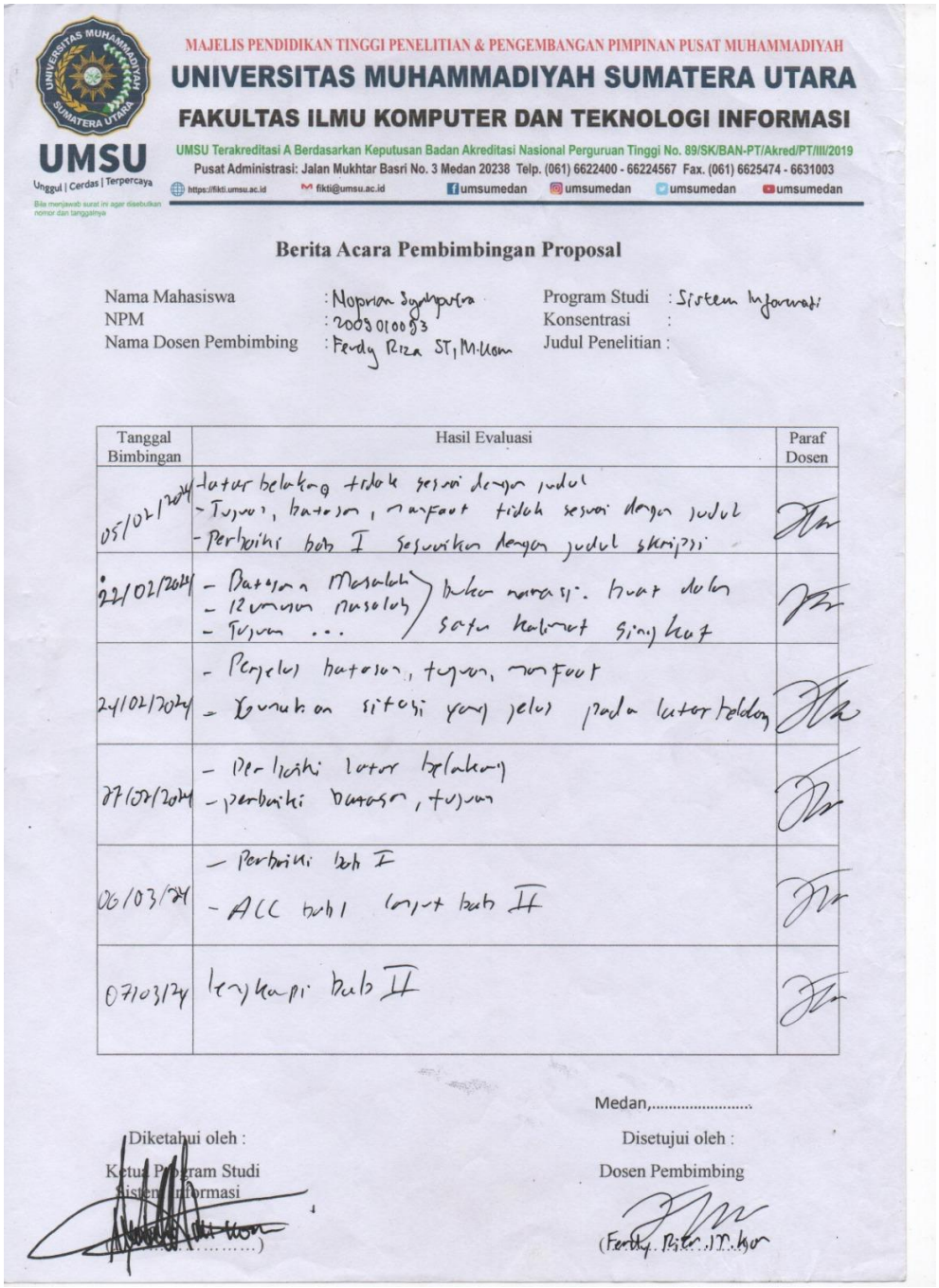
Wassalamu 'alaikum Warahmatullahi Wabarakatuh

Dekan

Dr. Al-Khowarizmi, M.Kom
NIDN : 0127099201

Cc.File

Lampiran 2 Berita Acara Bimbingan



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Unggul | Cerdas | Terpercaya

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan nomor dan tanggalnya

Berita Acara Pembimbingan Proposal

Nama Mahasiswa : Noprian Syahputra
NPM : 2003010093
Nama Dosen Pembimbing : Ferdy Riza ST, M.Kom

Program Studi : Sistem Informasi
Konsentrasi :
Judul Penelitian :

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
05/02/2024	latar belakang tidak sesuai dengan judul - Tujuan, batasan, manfaat tidak sesuai dengan judul - Perbaiki bab I sesuaikan dengan judul skripsi	
22/02/2024	- Batasan Masalah - Rumusan masalah - Tujuan ... Buka narasi. buat dulu satu kalimat singkat	
24/02/2024	- Perjelas batasan, tujuan, manfaat - Kumukan situasi yang jelas pada latar belakang	
27/02/2024	- Perbaiki latar belakang - perbaiki batasan, tujuan	
06/03/24	- Perbaiki bab I - ACC buat lanjut bab II	
07/03/24	lengkapi bab II	

Medan,.....

Diketahui oleh :
Ketua Program Studi
Sistem Informasi

(.....)

Disetujui oleh :
Dosen Pembimbing

(Ferdy Riza, ST, M.Kom)

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Berita Acara Pembimbingan Skripsi

Nama Mahasiswa : NOPRIAH SYAHPUTRA
NPM : 2009010093
Nama Dosen Penguji : INDAH PURNAMA SARI, ST. M.KOM
Program Studi : SISTEM INFORMASI
Konsentrasi :
Judul Penelitian :

Item	Hasil Evaluasi	Tanggal	Paraf Dosen
	Acc Sidang	03/07-2024	

Medan, 2 Juli 2024

Diketahui oleh :
Ketua Program Studi
Sistem Informasi

Disetujui oleh :
Dosen Penguji

(Indah Purnama Sari)

Lampiran 3 Surat izin Penerimaan

PEMERINTAH PROVINSI SUMATERA UTARA
BADAN KEPEGAWAIAN
Jalan Teuku Daud No. 5, Madras Hulu, Medan Polonia 20152
Website bapeg.sumutprov.go.id - Email bapeg@sumutprov.go.id

Medan, 30 Mei 2024

Nomor : 000.9/1939/BAPEG/V/2024
Sifat :
Lampiran : -
Hal : Penerimaan Izin Pendahuluan

Yth. Rektor Universitas Muhammadiyah Sumatera Utara
C/q. Dekan Fakultas Ilmu Komputer dan Teknologi Informasi
di –
Tempat

Sehubungan dengan surat Saudara Nomor 47/II.3-AU/UMSU-09/F/2024 Tanggal 10 Januari 2024 Hal Izin Riset Pendahuluan, maka dapat kami sampaikan bahwa kami menerima Riset untuk penyusunan skripsi yang merupakan salah satu persyaratan dalam menyelesaikan Program Studi Strata Satu (S1) di Badan Kepegawaian Provinsi Sumatera Utara atas nama :

No.	Nama	NIM	Jurusan
1.	Noprian Syahputra	2009010093	Sistem Informasi

Demikian disampaikan, atas perhatiannya diucapkan terima kasih.

a.n. KEPALA BADAN KEPEGAWAIAN
SEKRETARIS,

Ir. MUKMIN, M.AP
PEMBINA TK. I
NIP. 19670731 199503 1 001

Lampiran 4 Dokumentasi