

KONSENTRASI:
KEAMANAN KOMPUTER

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI
RIVEST SHAMIR ADLEMAN (RSA)
UNTUK KEAMANAN PADA FILE CITRA DIGITAL**

PROPOSAL TUGAS AKHIR



Oleh

AGUS MUHAMAD GAOSTUL IBAD

5170411331

**PROGRAM STUDI INFORMATIKA
FAKULTAS SAINS & TEKNOLOGI
UNIVERSITAS TEKNOLOGI YOGYAKARTA
2021**

PROPOSAL TUGAS AKHIR

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI
RIVEST SHAMIR ADLEMAN (RSA)
UNTUK KEAMANAN PADA FILE CITRA DIGITAL**

Oleh

AGUS MUHAMAD GAOSTUL IBAD
5170411331

Yogyakarta,

Yogyakarta,

Dosen Penguji Konten

Dosen Penguji Naskah

Nama.

NIK.

Nama

NIK.

Mengetahui

Ketua Program Studi Informatika

Dr. Enny Itje Sela, S.Si., M.Kom.

NIK. 111116089

ABSTRAK

Penelitian ini bertujuan untuk mengamankan informasi melalui media gambar atau citra yang mempunyai beberapa kelemahan, salah satunya adalah kemudahan melakukan manipulasi citra oleh pihak-pihak tertentu dengan bantuan teknologi yang berkembang sekarang ini. Dalam upaya untuk peningkatan pengiriman informasi melalui media citra digital dan perlindungan atas hak cipta hasil karya media digital maka algoritma kriptografi dapat diterapkan untuk pengamanan citra tersebut. Pada penelitian ini algoritma kriptografi yang digunakan yaitu algoritma kriptografi Rivest Shamir Adleman (RSA).

RSA merupakan algoritma kriptografi dengan memfaktorkan dua buah bilangan prima. Dari dua buah bilangan prima tersebut diperoleh sebuah kunci publik (digunakan untuk mengenkripsi plaintext), dan sebuah kunci privat (digunakan untuk mendekripsi ciphertext). Panjang kunci untuk mengenkripsi dapat diatur, dimana semakin Panjang bit untuk pembentukan kunci maka akan semakin sulit untuk dipecahkan karena sulitnya memfaktorkan dua buah bilangan yang sangat besar.

Tujuan penelitian ini yaitu untuk mengimplementasikan algoritma kriptografi RSA pada citra digital seperti jpeg,jpg,png dengan menggunakan Bahasa pemrograman PHP (Hypertext Preprocessor). Hasil dari implementasi algoritma kriptografi RSA ini dapat mengenkripsi dan dekripsi pada file citra digital dan menyimpan data yang telah di enkripsi sehingga kita bisa melihat ataupun menyimpan data yang asli didalam sistem yang telah dibaut, serta terhindar dari plagiarism karena filecitra digitaltersebut telah dienkripsi.

Kata kunci: Pengamanan File Citra Digital, PHP, Kriptografi, Enkripsi, Dekripsi, RSA

DAFTAR ISI

ABSTRAK	i
DAFTAR ISI	ii
DAFTAR GAMBAR	iv
DAFTAR TAbel.....	v
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Sistematika Penulisan	3
BAB II KAJIAN HASIL PENELITIAN DAN LANDASAN TEORI	5
2.1 Kajian Hasil Penelitian.....	5
2.2 Landasan Teori.....	10
2.2.1 Kriptografi	10
2.2.2 Algoritma Rivest Shamir Adleman (RSA).....	11
2.2.3 Flowchart.....	16
2.2.4 Bahasa Pemrograman PHP	16
2.2.5 Framework Bootsrap	17
2.2.6 XAMPP	17
BAB III METODE PENELITIAN.....	18
3.1 Bahan/Data.....	18
3.2 Tahapan Penelitian	19
BAB IV analisis dan desain sistem.....	21
4.1 Analisis Sistem yang diusulkan	21
4.1.1 Analisis fungsional	21
4.1.2 Analisis non fungsional	21
4.2 Desain Sistem.....	22
4.2.1 Desain logik.....	22

4.2.1.1 Flowchart	22
4.2.1.2 Unified Modeling Language (UML)	25
4.1.2.3 Data Flow Diagram (DFD).....	30
4.2.2 Desain fisik	31
BAB V PENUTUP	37
5.1 Kesimpulan	37
DAFTAR PUSTAKA.....	38

DAFTAR GAMBAR

Gambar 2. 1 Diagram Fishbone	9
Gambar 2. 2 Flowchart Langkah Pembangkitan Kunci Algoritma RSA.....	12
Gambar 2. 3 Flowchart Enkripsi Algoritma RSA.....	14
Gambar 2. 4 Flowchart Dekripsi Algoritma RSA.....	15
Gambar 2. 5 Skema PHP.....	16
Gambar 3. 1 Bagan Tahapan Penelitian	19
Gambar 4. 1 Proses Enkripsi.....	23
Gambar 4. 2 Proses Dekripsi.....	24
Gambar 4. 3 Use Case Diagram Proses Enkripsi	25
Gambar 4. 4 Use Case Proses Dekripsi.....	26
Gambar 4. 5 Activity Diagram.....	27
Gambar 4. 6 Sequence Diagram Pembuatan Kunci Publik dan Privat	28
Gambar 4. 7 Sequence Diagram Proses Enkripsi	29
Gambar 4. 8 Sequence Diagram Proses Dekripsi	29
Gambar 4. 9 DFD Level 0.....	31
Gambar 4. 10 ERD implemtasi Algoritma Kirptografi RSA.....	32
Gambar 4. 11 Relasi Tabel.....	33
Gambar 4. 12 Antarmuka Halaman Beranda	34
Gambar 4. 13 Antarmuka Halaman Enkripsi.....	35
Gambar 4. 14 Antarmuka Halaman Dekripsi.....	36

DAFTAR TABEL

Table 2. 1 Perbandingan Kajian Hasil Penelitian	8
---	---

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan data dan kerahasiaan data merupakan suatu aspek yang sangat penting dalam sistem informasi saat ini terutama pada citra digital. Upaya untuk mengamankan data yaitu menggunakan algoritma kriptografi, berbagai jenis algoritma dapat diimplementasikan untuk sistem keamanan data pada citra digital. Salah satunya yaitu algoritma kriptografi Rivest Shamir Adleman (RSA) yang digunakan untuk menjaga informasi atau data saat ini.

Berdasarkan penelitian yang dilakukan oleh (Deskiva, Z. Z. dkk., 2014) informasi yang disimpan dalam bentuk digital dan memiliki beberapa bentuk seperti teks, citra, video, audio, dan multimedia. Dalam hal ini, khususnya citra digital banyak sekali aplikasi yang dapat memanipulasi citra tersebut dengan mudah oleh oknum-oknum yang kurang bertanggung jawab dengan memberikan kesan-kesan negatif dalam citra tersebut. Hal tersebut menimbulkan kekhawatiran pada berbagai pihak dalam melakukan interaksi baik secara individu maupun kelompok, serta yang berkaitan dengan pengamanan data maupun informasi penting haruslah benar-benar diperhatikan agar data yang masih tersimpan dalam computer tetap terjaga dan aman serta terhindar dari pengguna yang melakukan penyalahgunaan data tersebut.

Berdasarkan permasalahan diatas, diperlukan cara dalam melindungi data agar terhindar dari penggunaan data yang bersifat negative oleh pengguna yang tidak bertanggungjawab. Maka dari itu, bisa menerapkan algoritma kriptografi RSA karena kriptografi RSA ini merupakan algoritma kriptografi asimetris dengan panjang kunci dalam bit dapat diatur, semakin panjang bit yang diatur maka semakin susah untuk dipecahkan kunci dalam bit tertentu tersebut, akan tetapi semakin lama proses pada dekripsinya.

Dari permasalahan yang sudah dijabarkan diatas, peneliti berusaha untuk melakukan penelitian yang nantinya mampu digunakan dalam pengamanan dalam

bentuk file citra digital serta menekan resiko manipulasi file citra digital dengan mengaplikasikan algoritma RSA yang memiliki dua kunci yaitu publik dan rahasia dengan harapan file citra digital tersebut dapat diamankan menggunakan algoritma kriptografi RSA tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan diatas maka dapat dirumuskan suatu rumusan masalah sebagai yaitu berikut:

- a. Bagaimana menerapkan algoritma kriptografi Rivest Shamir Adleman (*RSA*) untuk keamanan data pada file citra digital?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini yaitu:

- a. Enkripsi dan Dekripsi file citra digital menggunakan metode RSA yang memiliki kunci Asimetris.
- b. Data yang di Enkripsi dan Dekripsi yang ada pada file citra digital jenis jpg.png.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah mengetahui cara menerapkan algoritma kriptografi RSA untuk sebuah sistem agar dapat mengamankan data pada file citra digital.

1.5 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan dapat memberikan manfaat yaitu:

- a. Bagi Pengguna:
 1. Memudahkan dalam pengamanan data pada file citra digital.
 2. Menjamin keamanan data sehingga dapat mencegah dari pencurian data ataupun memanipulasi data.
- b. Bagi peneliti:

1. Menambah pengetahuan dan ilmu mengenai enkripsi dan dekripsi algoritma kriptografi RSA pada file citra digital.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penelitian ini terbagi dalam beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan penelitian mengenai Implementasi Algoritma Kriptografi RSA untuk keamanan pada file gambar.

BAB II KAJIAN HASIL PENELITIAN DAN LANDASAN TEORI

Pada bab ini menjelaskan mengenai penelitian – penelitian sebelumnya yang sedikit banyaknya ada kaitan dengan penelitian yang dilakukan oleh penulis saat ini.

BAB III METODE PENELITIAN

Bab ini menyajikan secara lengkap setiap langkah eksperimen yang dilakukan dalam penelitian yang antara lain meliputi bahan/data, aturan bisnis, dan tahapan penelitian

BAB IV ANALISIS DAN DESAIN SISTEM

Pada bab ini menggambarkan rancangan antar muka yang diusulkan untuk menyelesaikan masalah. diantaranya analisis sistem, desain fisik dan desain sistem. Analisis sistem yaitu berisi analisis kebutuhan non fungsional dan fungsional. Desain sistem berisi desain logic yang memuat diagram ERD, DAD dan lain lain.

BAB V PENUTUP

Pada bagian ini berisi kesimpulan sementara yang diambil dari isi metode penelitian, dan rancangan sistem.

BAB II

KAJIAN HASIL PENELITIAN DAN LANDASAN TEORI

2.1 Kajian Hasil Penelitian

Dalam melakukan penelitian ini, peneliti mengacu pada beberapa penelitian yang telah dilakukan sebelumnya, antara lain oleh (Rusri Yanti, N. dan Zebua, T., n.d. 2018) yang meneliti tentang fungsi algoritma kriptografi hill chipper untuk pengamanan file gambar dan pesan teks. Penelitian tersebut menggunakan algoritma kriptografi hill chipper, pengamanan data yang dihasilkan dari algoritma hill cipher akan mengacak ulang nilai bit data menggunakan algoritma Hill Cipher menjadi lebih kompleks secara detail, data yang akan digunakan adalah file gambar dan sampel pesan teks untuk dijadikan sebagai sampel uji coba meningkatkan keamanan data menggunakan algoritma kriptografi hill cipher. Pada tahapan ini dilakukan pengujian untuk proses pengenkripsian pesan terhadap gambar, sehingga pesan yang terisip didalam gambar akan menjadi acak dan berubah dari aslinya (enkripsi). Proses enkripsi algoritma hill cipher dilakukan per blok dari plainteks, dengan terlebih dahulu melakukan konversi plainteks menjadi bilangan desimal/angka.

Penelitian lain oleh (Rakhman, A. A. dan Kurniawan, A. W., 2015) tentang implementasi algoritma kriptografi Rivest Shamir Adleman (RSA) dan Vigenere Chipper pada file gambar bitmap 8 bit. Penelitian tersebut menggunakan algoritma RSA dan Vigenere Chiper, Citra akan diolah dengan cara mengenkripsi nilai indeks warna RGB pada masing-masing piksel dengan menggunakan algoritma kriptografi RSA terlebih dahulu kemudian dilanjutkan dengan menggunakan algoritma Vigenere Cipher. Sedangkan untuk tahap pendekripsian dilakukan dengan menggunakan algoritma Vigenere Cipher terlebih dahulu kemudian menggunakan algoritma kriptografi RSA. Selanjutnya dilakukan analisis pengaruh penerapan algoritma Rivest Shamir Adleman (RSA) dan Vigenere Cipher pada citra yang akan diamankan, meliputi analisis ruang kunci, analisis perubahan indeks warna, dan analisis waktu proses enkripsi dan deskripsi. Pengujian yang dilakukan untuk analisis tersebut,

menggunakan citra berdimensi 3840 x 2160 piksel dan ukuran file 7,91 MB dan citra berdimensi 5012 x 2819 piksel dan ukuran file 13,4 MB. Analisis ruang kunci menunjukkan bahwa citra telah berhasil didekripsikan dan secara visual pola citra kembali ke bentuk semula tanpa mengalami cacat sedikitpun. Analisis perubahan indeks warna, dilihat secara visual pada hasil palette warna membuktikan bahwa metode enkripsi yang dirancang telah berhasil digunakan untuk memperbarui nilai indeks warna citra asli. Sedangkan dari analisis waktu proses enkripsi dan dekripsi dapat disimpulkan Rata-rata lama waktu yang dibutuhkan untuk proses dekripsi lebih lama dibandingkan dengan lama waktu proses enkripsi.

Penelitian lain oleh (Marsel Fio Ipandi, Arzi Al Hafiz, Afriliansyah, , M.Aldi Febrian, Mhd. Arief Hasan, 2020) tentang penerapan algoritma kriptografi asimetris dengan metode RSA dan Blowfish untuk enkripsi dan dekripsi gambar menggunakan java neatbeans. Penelitian tersebut menggunakan metode Dalam melakukan penelitian ini, peneliti mengacu pada beberapa penelitian yang telah dilakukan sebelumnya, antara lain oleh (Faizal Zuli dan Ari Irawan pada tahun 2016) yang isinya suatu kekuatan pada kriptografi terletak di kekuatan atau kehebatan kunci dari kriptografi itu sendiri bukan dari algoritma itu sendiri,oleh karna itu blowfish termasuk cocok karna dimana kunci kerahasiaan metode ini sangat kuat dan sangat panjang, jadi tidak terlalu mudah bagi data itu sendiri bisa dibobol oleh pihak yang tidak bertanggung jawab.

Penelitian lain oleh (Muzakir, A., 2016) tentang implementasi Teknik steganografi dengan kriptografi kunci private AES untuk keamanan file gambar berbasis Anndroid. Penelitian tersebut menggunakan algoritma kriptografi AES. Dalam membangun perangkat lunak steganografi pada citra digital file gambar jpeg dengan menggunakan bahasa pemrograman java, yang mengeksploitasi sistem kekuatan penglihatan manusia, dengan menyembunyikan sebuah pesan tersembunyi atau informasi sehingga menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya. Metode yang digunakan untuk penyembunyian pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan ke dalam bit standar AES (edvance encryption standard). Sistem steganografi disini

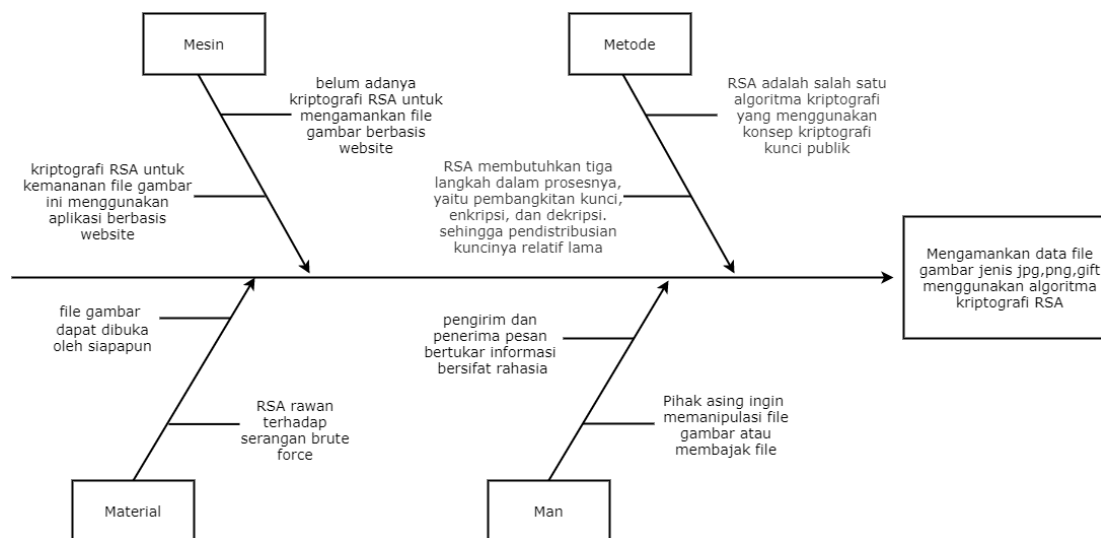
mempunyai alur proses tersendiri yaitu proses sistem enkripsi dan deskripsi pesan yang berfungsi untuk menyisipkan pesan kedalam gambar jpeg dan mengungkap kembali pesan tersebut dari gambar jpeg. Hasil akhir dari penelitian ini adalah suatu aplikasi pengolahan citra gambar yang aman, dimana sumber gambar dapat diambil dari kamera langsung atau dari file galeri ponsel. Selanjutnya gambar dari hasil pengolahan dapat langsung di share via sosial media yang telah terinstal di ponsel android.

Penelitian lainnya yang dilakukan oleh (Siringoringo, R., 2020) tentang Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File, dalam penelitian ini algoritma yang digunakan yaitu algoritma kriptografi AES dan kriptografi RSA. Sistem kriptografi secara mutlak ditentukan oleh keamanan kunci yang digunakan. Selain panjangnya kunci, proses pada saat pertukaran kunci harus juga diperhatikan agar kunci tersebut tetap aman. Algoritma kriptografi kunci publik atau sering disebut dengan algoritma kunci asimetris terkadang tidak pernah berdiri sendiri, algoritma kunci publik juga membutuhkan algoritma kunci simetris. Dalam hal ini biasanya algoritma kunci simetris tersebut digunakan untuk enkripsi dan dekripsi plainteks karena dari segi kecepatan waktu algoritma simetris cukup menguntungkan, sedangkan algoritma kunci publik berperan untuk mengenkripsikan kunci dari kunci simetris tersebut agar lebih aman pada saat pendistribusian kunci dan pesan.

Table 2. 1 Perbandingan Kajian Hasil Penelitian

No	Judul	Penulis	Algoritma yang digunakan	Hasil/Kesimpulan
1	Fungsi Algoritma Kriptografi Hill Chipper untuk Pengamanan File Gambar dan Pesan Teks	Rusri Yanti, N dan Zebua, T., n.d. 2018	Algoritma Kriptografi Hill Chipper	Telah diperoleh suatu model yang baru untuk meningkatkan keamanan data gambar dan pesan teks menggunakan algoritma kriptografi hill cipher. Berdasarkan hasil pengujian aplikasi dengan menggunakan algoritma kriptografi hill cipher, dapat memberikan masukan data secara tersandi untuk memberikan tingkat keamanan pesan
2	Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) Dan Vigenere Chipper Pada File Gambar Bitmap 8 Bit	Rakhman, A. A. dan Kurniawan, A. W., 2015	Algoritma Kriptografi Rivest Shamir Adleman (RSA) Dan Vigenere Chipper	Hasil pengujian menunjukkan secara visual citra hasil enkripsi sulit untuk dibaca atau dilihat. Hal ini disebabkan karena keteracakan pola warna dan perubahan intensitas nilai indeks warna yang dihasilkan setelah mengalami enkripsi.
3	Penerapan Algoritma Kriptografi Asimetris dengan Metode RSA dan Blowfish untuk Enkripsi dan Dekripsi Gambar menggunakan java neatbeans	Marsel Fio Ipandi, Arzi Al Hafiz, Afriliansyah, , M.Aldi Febrian, Mhd. Arief Hasan, 2020	Algoritma Kriptografi RSA dan Blowfish	Teknik yang digunakan dalam mengamankan file gambar adalah teknik algoritma RSA dan Blowfish, dimana plaintext akan diproses dengan RSA dan hasil dari ciphertext akan dideskripsikan menggunakan Blowfish.
4	Implementasi Teknik Steganografi dengan Kriptografi kunci private AES untuk keamanan file gambar berbasis Anndroid	Muzakir, A., 2016	Steganografi dan Algoritma Kriptografi AES	Aplikasi pengamanan gambar berformat jpeg dengan teknik steganografi menggunakan algoritma aes berbasis android telah berhasil dibangun sebagai aplikasi penyisipan teks gambar menggunakan perangkat mobile android.
5	Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File	Siringoringo, R., 2020	Algoritma Rijndael (AES) dan RSA	Hasil penelitian ini diperoleh sistem enkripsi dan dekripsi terhadap plainteks dan kunci simetris (sessionkey) dengan kombinasi algoritma Rijndael dan RSA. Hasil enkripsi plainteks pada sistem yang dibangun berupa kode karakter, sedangkan untuk enkripsi sessionkey berupa kode number.

Seperti terlihat pada Tabel 2.1. perbedaan dari lima referensi dengan judul yang diangkat oleh penulis terletak pada Algoritma yang digunakan , dan Objek penelitian yang akan diuji yaitu untuk citra digital menggunakan metode *Algoritma RSA* untuk enkripsi dan dekripsi file pada gambar. Dengan penelitian ini diharapkan dapat ditemukan metode terbaik untuk menyelesaikan masalah yang kompleks. Untuk lebih jelas bisa dilihat pada Gambar 2.1



Gambar 2.1 Diagram Fishbone

Pada Gambar 2.1 dapat dilihat bahwa terdapat empat kategori penyebab masalah pada penelitian Implentasi Algoritma Kriptografi RSA untuk keamanan data pada citra digital yang digambarkan dengan tanda panah yang mengarah ke tulang utama, yaitu berkaitan dengan (metode), siapapun yang terlibat dalam proses (Man), media/alat yang terlibat (material), dan mesin atau sistem (system). Setiap detail penyebab masalah tersebut digambarkan dengan tanda panah yang mengarah ke masing-masing kategori.

2.2 Landasan Teori

2.2.1 Kriptografi

Menurut (Menezes dan Oorchot, 1996), kriptografi merupakan sebuah studi teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, otentikasi entitas serta otentikasi keaslian data dan integritas data. Kriptografi tidak hanya penyediaan keamanan informasi saja, tetapi juga sebuah himpunan teknik-teknik.

Tujuan dari kriptografi yang juga merupakan aspek keamanan informasi adalah sebagai berikut (Menezes dan Oorchot, 1996) :

- a. Kerahasiaan (confidentiality) adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan, dari pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami. Istilah lain yang senada dengan confidentiality adalah secrecy dan privacy.
- b. Integritas data adalah layanan penjagaan pengubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.
- c. Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan (data origin authentication). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi

juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Tanda-tangan digital menyatakan sumber pesan.

- d. Nirpenyangkalan (non-repudiation) adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2.2 Algoritma Rivest Shamir Adleman (RSA)

Algoritma RSA diperkenalkan oleh tiga peneliti dari MIT (Massachusetts Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. RSA merupakan teknik kriptografi dengan memanfaatkan 2 bilangan prima. Dari kedua bilangan prima tersebut dapat diperoleh sebuah Public Key (digunakan untuk mengenkripsi sebuah plainteks) dan sebuah Private Key (digunakan untuk mendekripsi cipherteks) (Hariyanto dkk., 2018).

a. Pembangkitan Kunci RSA

Pada algoritma RSA terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi dan proses dekripsi. Letak kesulitan algoritma ini adalah bagaimana menemukan dua faktor bilangan prima yang besar yang akan digunakan sebagai kunci publik dan kunci privat. Dua bilangan prima besar tersebut p dan q dimana $p \neq q$.

Algoritma RSA mendasarkan proses enkripsi dan dekripsinya pada proses matematika khususnya pada konsep bilangan prima dan aritmatika modulo. Proses matematika tersebut dilakukan untuk menghasilkan kunci rahasia yang

dapat digunakan untuk proses dekripsi hanya oleh pengirim dan penerima pesan. Dasar dari algoritma ini memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Jika semakin besar bilangan yang difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan, semakin sulit pemfaktoranannya, semakin kuat pula algoritma RSA.



Gambar 2. 2 Flowchart Langkah Pembangkitan Kunci Algoritma RSA

Adapun penjelasan dari gambar 2.1 adalah sebagai berikut :

1. Pilih dua bilangan prima p dan q secara acak.
2. Hitung $n = p \cdot q$. Untuk kemudian bilangan n disebut parameter sekuriti. Sebaiknya $p \neq q$, sebab jika $p = q$ maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n .
3. Pilih bilangan e secara acak di mana e tidak memiliki faktor pembagi yang sama dengan $(p-1)(q-1)$ selain bilangan 1. Atau dengan kata lain bersifat relatif prima.
4. Hitung d sedemikian sehingga $e \cdot d \bmod (p-1)(q-1) = 1$. Dengan menggunakan sebuah algoritma yang disebut algoritma Euclid akan menghitung d sehingga, $d = e^{-1} \bmod ((p-1)(q-1))$.

5. Bilangan n dan e kita sebarikan ke publik. e ini adalah yang akan menjadi kunci publik. d menjadi kunci privat. Sementara itu bilangan p dan q dihilangkan, dan dicegah agar tidak pernah sampai bocor ke publik.

Kini sudah didapatkan sebuah kunci publik dan kunci privat. Selanjutnya berikut ini adalah algoritma untuk menyandi dan menterjemahkan pesan:

1. Untuk menyandi sebuah pesan m dengan menggunakan kunci publik e , kita melakukan operasi $m^e \bmod n$, sementara untuk membuka pesan tersandi c dengan menggunakan kunci privat, kita lakukan $c^d \bmod n$.
2. Untuk memudahkan enkripsi dan dekripsi maka pesan m dibagi menjadi beberapa blok yang kecil.

Algoritma di atas adalah algoritma yang digunakan dalam penyandian RSA, maka hanya menggunakan operasi pemangkatan bilangan dan modulus bilangan, dalam melakukan proses enkripsi dan dekripsi sebuah pesan. Kesederhanaan inilah yang menjadikan RSA menjadi populer karena relatif mudah dimengerti.

b. Enkripsi RSA

Proses enkripsi dengan algoritma RSA dilakukan dengan menghitung eksponen plaintext dalam operasi modulo n (modulo = sisa pembagian) untuk setiap blok pesan atau data sehingga dapat menghasilkan ciphertext. Eksponen yang digunakan adalah public exponent e . Operasi ini bisa dituliskan dengan persamaan berikut:

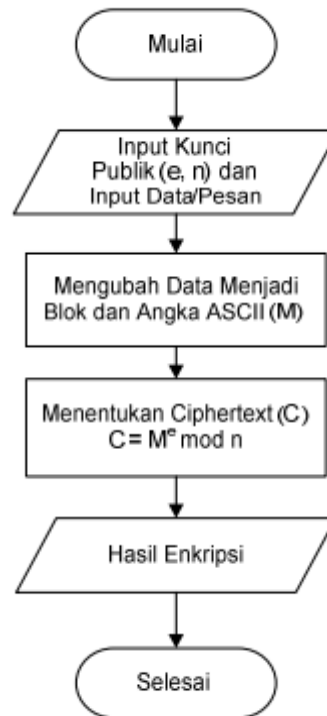
$$C = M^e \bmod n$$

C = ciphertext

M = pesan (plaintext)

e = public exponent

n = modulus



Gambar 2. 3 Flowchart Enkripsi Algoritma RSA

Penjelasan dari gambar 2.2 mengenai langkah-langkah dalam proses enkripsi algoritma RSA adalah sebagai berikut:

- i. Menginputkan kunci publik yang berupa pasangan (e, n) beserta pesan atau data yang akan dienkripsi.
- ii. Representation pesan atau data menjadi blok-blok dan diubah menjadi bilangan bulat positif M
- iii. Hitung $C = M^e \text{ mod } n$.
- iv. Dan dihasilkan ciphertext (C) yang merupakan hasil dari enkripsi.

c. Dekripsi RSA

Sedangkan pada proses deskripsi, yang dilakukan hampir sama dengan enkripsi tapi eksponen yang digunakan adalah private exponent d untuk mengembalikan pesan seperti semula. Operasi ini bisa dituliskan dengan persamaan berikut:

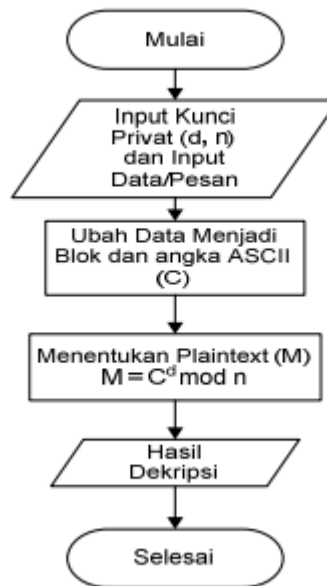
$$M = C^d \text{ mod } n$$

M = pesan (plaintext)

C = ciphertext

d = private exponent

n = modulus



Gambar 2. 4 Flowchart Dekripsi Algoritma RSA

Penjelasan dari gambar 2.3 mengenai langkah-langkah dalam proses dekripsi algoritma RSA adalah sebagai berikut:

- i. Menginputkan kunci privat yang berupa pasangan (d, n) beserta pesan atau data yang akan didekripsi.
- ii. Representation pesan atau data menjadi blok-blok dan diubah menjadi bilangan bulat positif C
- iii. Hitung $M = C^d \bmod n$
- iv. Dan dihasilkan plaintext (M) yang merupakan hasil dari dekripsi dan merupakan pesan atau data yang sebenarnya

2.2.3 Flowchart

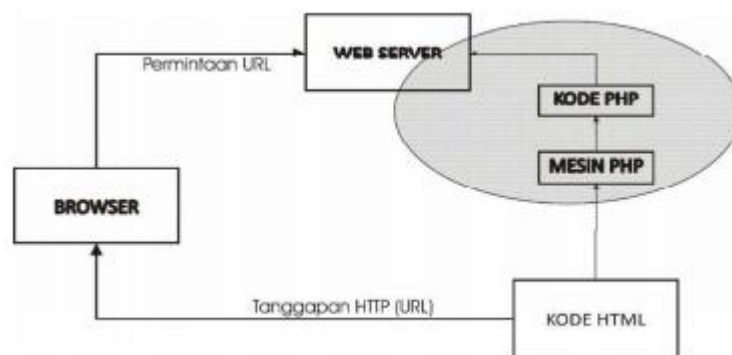
Flowchart adalah bagian-bagian yang menggambarkan langkah-langkah menyelesaikan suatu masalah. Flowchart merupakan suatu penyajian dari algoritma. Perancangan flowchart diagram bertujuan untuk menggambarkan aliran proses dalam system (Agung, H. dan Prasta, I., 2018).

2.2.4 Bahasa Pemrograman PHP

PHP merupakan singkatan dari PHP Hypertext Preprocessor. PHP merupakan bahasa berbentuk skrip yang ditempatkan dalam server dan diproses di dalam server. Hasilnya dikirim ke klien, tempat pemakai menggunakan browser (Marsudi, D., 2016).

Konsep kerja PHP diawali dengan permintaan (request) suatu halaman web oleh browser. Berdasarkan URL (Uniform Resource Locator) atau yang biasa dikenal dengan alamat internet, browser mendapatkan alamat dari web server, mengidentifikasi halaman yang dikehendaki, dan menyampaikan segala informasi yang dibutuhkan oleh web server.

Selanjutnya, web server akan mencari file yang diminta dan memberikan isinya ke web browser. Browser yang mendapatkan isinya segera melakukan proses penerjemahan kode dan menampilkan ke layar pemakai.



Gambar 2. 5 Skema PHP

2.2.5 Framework Bootstrap

Bootstrap merupakan sebuah framework css yang memudahkan pengembang untuk membangun website yang menarik dan responsif. Bootstrap adalah css tetapi dibentuk dengan LESS, sebuah pre-processor yang memberi fleksibilitas dari css biasa. Bootstrap dapat dikembangkan dengan tambahan lainnya karena ini cukup fleksibel terhadap pekerjaan design butuhkan (Otto, 2011).

2.2.6 XAMPP

XAMPP adalah sebuah software yang berfungsi untuk menjalankan website berbasis PHP dan menggunakan pengolah data MySQL yang dijalankan dikomputer secara lokal. XAMPP berperan sebagai web server pada komputer. XAMPP juga dapat disebut sebuah CPanel server virtual, yang dapat membantu Anda melakukan preview sehingga dapat memodifikasi website tanpa harus online atau terakses dengan internet.

Software XAMPP bersifat open sources yang dapat diperoleh secara gratis dari situs www.apachefriends.org. XAMPP adalah perangkat lunak yang mendukung banyak sistem operasi dan merupakan komplikasi dari beberapa program. Fungsinya adalah sebagai server yang berdiri sendiri dan terdiri atas Apache, MySQL, dan bahasa pemrograman PHP (Marsudi, D., 2016) .

BAB III

METODE PENELITIAN

3.1 Bahan/Data

a. Data yang diperoleh

Pada penelitian ini data yang diperoleh menggunakan data primer yaitu data yang diperoleh secara langsung dari sumber data tersebut yang berhubungan dengan penelitian yang dilakukan, yaitu data-data yang diperoleh dari wawancara dan survei atau pengamatan langsung, yang digunakan sebagai bahan acuan dalam pembuatan aplikasi. Contoh data primer yang dibutuhkan penulis untuk menunjang pembuatan aplikasi adalah data gambar karena data yang digunakan dalam penelitian merupakan data berupa citra atau gambar yang didapatkan dari user ketika melakukan proses enkripsi dan dekripsi.

b. Prosedur pengumpulan data

Dalam penelitian ini, pengumpulan data terkait implementasi kriptografi RSA untuk keamanan data pada file citra digital menggunakan metode, yaitu:

i. Studi Literatur

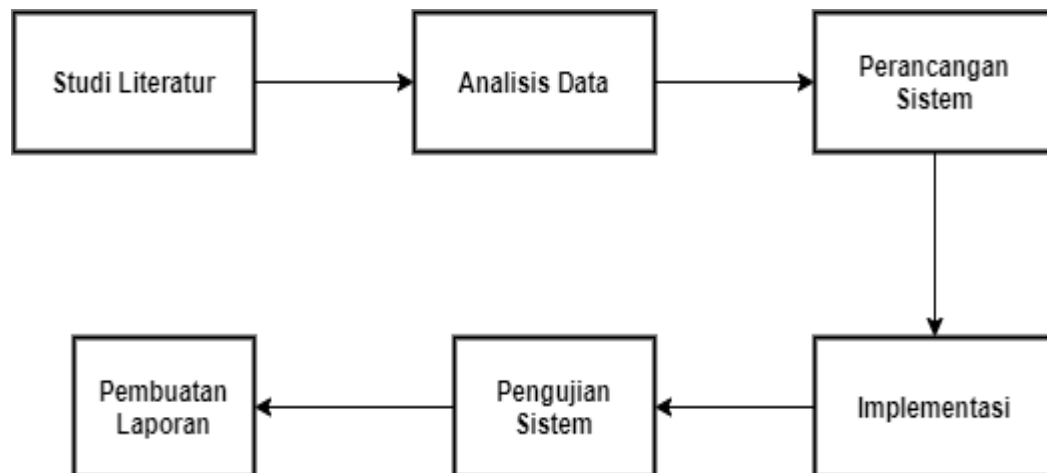
Tahap studi literatur merupakan tahapan mempelajari metode yang akan digunakan pada penelitian, yaitu mempelajari algoritma RSA. Sumber yang digunakan berupa buku jurnal, maupun bahan bacaan yang terdapat di internet. Buku “Kriptografi” karya Rinaldi Munir sebagai acuan dalam mempelajari algoritma RSA. Selain itu, penelitian yang dilakukan oleh (Rakhman, A. A. dan Kurniawan, A. W., 2015) yang berjudul Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) Dan Vigenere Chipper Pada File Gambar Bitmap 8 Bit sebagai acuan untuk mempelajari algoritma RSA dalam keamanan data untuk file gambar.

ii. Survey

Metode ini dilakukan dengan cara melakukan pengamatan dengan mengamati objek secara langsung dimana objek tersebut tentunya mendukung atau berhubungan dengan penelitian. Kegiatan yang dilakukan adalah melakukan riset mengamati langsung proses data yang dibutuhkan oleh user. Dengan metode survei ini penulis akan mencoba mengamati proses dari transaksi data file citra digital, contohnya proses yang untuk mengupload citra digital yang dimana gambar tersebut adalah karya dari user.

3.2 Tahapan Penelitian

Dalam proses implementasi kriptografi RSA untuk keamanan data pada file citra digital, ada beberapa tahapan penyelesaian masalah yang dilakukan, berikut adalah tahapan – tahapannya yang berbentuk diagram pada Gambar 3.1 dibawah ini:



Gambar 3. 1 Bagan Tahapan Penelitian

Rincian mengenai tahapan penelitian yang akan penulis gunakan akan penulis jelaskan sebagai berikut:

a. Studi Literatur

Pada tahap ini dilakukan pencarian dan pemahaman literatur serta pengumpulan informasi tentang file citra digital dan algoritma kriptografi RSA yang akan di implementasikan untuk keamanan data pada file citra digital. Literatur yang digunakan meliputi buku referensi, jurnal, buku Tugas Akhir mahasiswa jurusan Teknik Informatika serta dokumentasi dari internet.

b. Analisis Data

pada tahapan ini proses analisis yang dilakukan ada dua hal, yang pertama analisis yang diperloeh dan analisis kebutuhan, analisis data yang dikumpulkan meliputi data citra digital dan analisis kebutuhan meliputi kebutuhan dari sistem.

c. Perancangan Sistem

Pada tahap ini akan dilakukan perancangan desain mengenai implementasi algoritma kriptografi RSA yang akan dibangun berdasarkan teori yang telah dipahami.

d. Implementasi

Pada tahap ini akan dilakukan pembangunan aplikasi untuk keamanan data pada citra digital yang mana dalam pembangunan aplikasi tersebut akan diterapkan teori/algoritma yang telah dipelajari yaitu algoritma kriptografi RSA.

e. Pengujian Sistem

Setelah semua proses implementasi selesai dilakukan, tahap selanjutnya adalah pengujian yang bertujuan untuk menguji kebenaran dalam implementasi algoritma kriptografi RSA untuk keamanan data pada file citra digital.

f. Pembuatan Laporan

Dan tahapan paling akhir adalah pembuatan laporan yang bertujuan untuk dijadikan sebagai dokumentasi hasil penelitian.

BAB IV

ANALISIS DAN DESAIN SISTEM

4.1 Analisis Sistem yang diusulkan

Analisa sistem yang diusulkan dilakukan untuk menentukan gambaran sistem yang sesuai dengan kebutuhan pengguna.

4.1.1 Analisis fungsional

Adapun fitur-fitur dari implementasi algoritma kriptografi RSA untuk keamanan data pada file citra digital berbasis web ini yaitu:

- a. Pengguna dapat mengupload file citra yang akan di enkripsi maupun dekripsi
- b. Pengguna dapat mengenkripsi file citra berjenis jpg, jpeg, png
- c. Pengguna dapat mendekripsi file citra berjenis jpg, jpeg, png
- d. Pengguna dapat melihat tampilan file yang sudah di enkripsi

4.1.2 Analisis non fungsional

Kebutuhan non fungsional adalah kebutuhan yang terkait dengan basis yang digunakan dalam pembuatan sistem ini. Sistem ini akan berbasis website agar dapat diakses oleh semua admin selama terkoneksi dengan internet. Dalam hal ini, setelah penulis melakukan analisis maka kebutuhan non fungsional dari sistem ini nantinya sebagai berikut:

- a. Perangkat Keras (Hardware)

Perangkat keras yang dibutuhkan untuk membangun sistem ini yaitu:

1. Laptop ASUS KAN0CX03B604415
2. Prosesor Intel core i3 7th
3. Ram 4GB
4. Mouse

b. Perangkat Lunak (Software)

1. Visual Studio Code
2. Xampp
3. Sistem Operasi Windows 10 Home
4. Bahasa Pemrograman PHP
5. Framework Bootsrap
6. Google Chrome
7. Domain dan Hosting

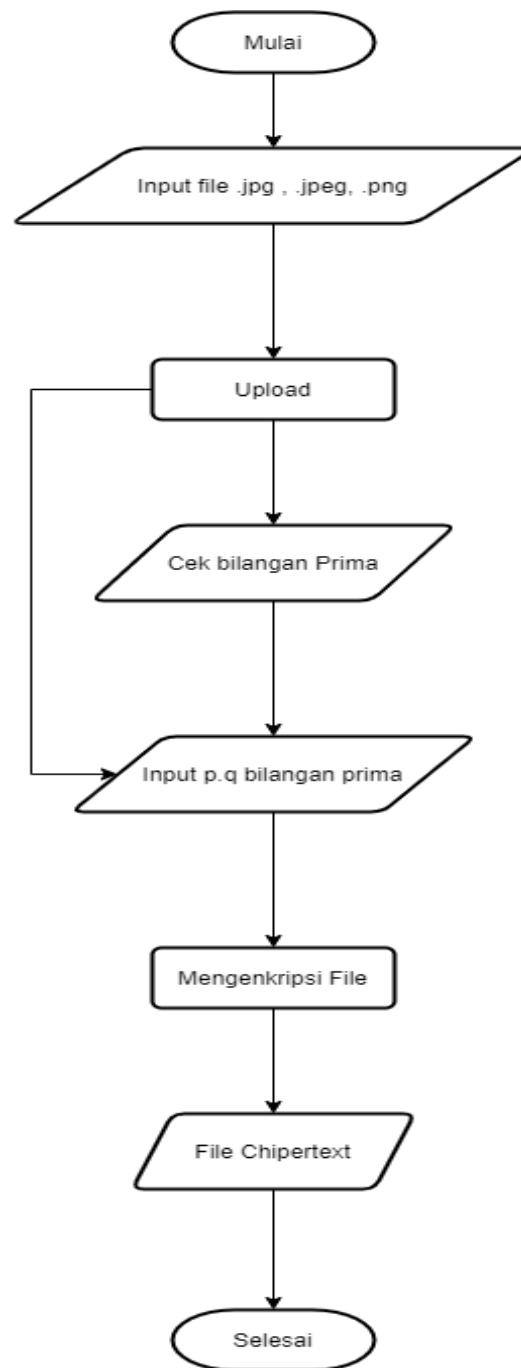
4.2 Desain Sistem

4.2.1 Desain logik

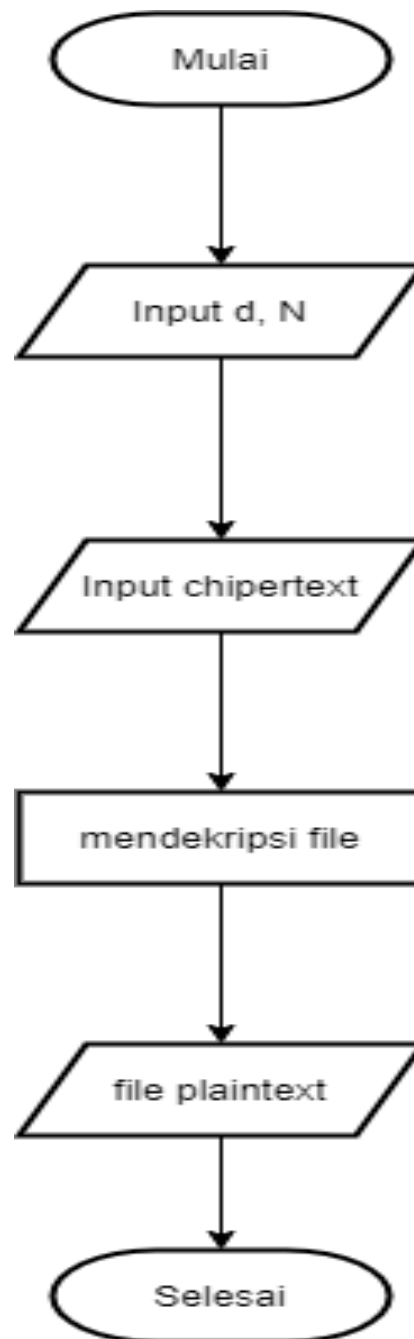
Bagian ini bisa dituliskan menggunakan diagram ER, DAD (Diagram Alir Data), DAS (Diagram Alir Sistem), flowchart, algoritma, relasi tabel, UML: class diagram, sequential diagram dan lain-lain. Tahapan rancangan sistem yang dibangun sesuai dengan teori metode pembangunan sistem yang digunakan.

4.2.1.1 Flowchart

Sistem yang diusulkan yaitu sistem yang dapat melakukan enkripsi dan dekripsi citra digital jpg, jpeg, png. Dimana input sistem adalah file citra digital, lalu sistem akan memproses bilangan prima dan input bilangan prima kemudian proses enkripsi gambar dan output nya itu file chipertext. Sistem yang diusulkan dapat dilihat pada Gambar 4.1.



Gambar 4. 1 Proses Enkripsi

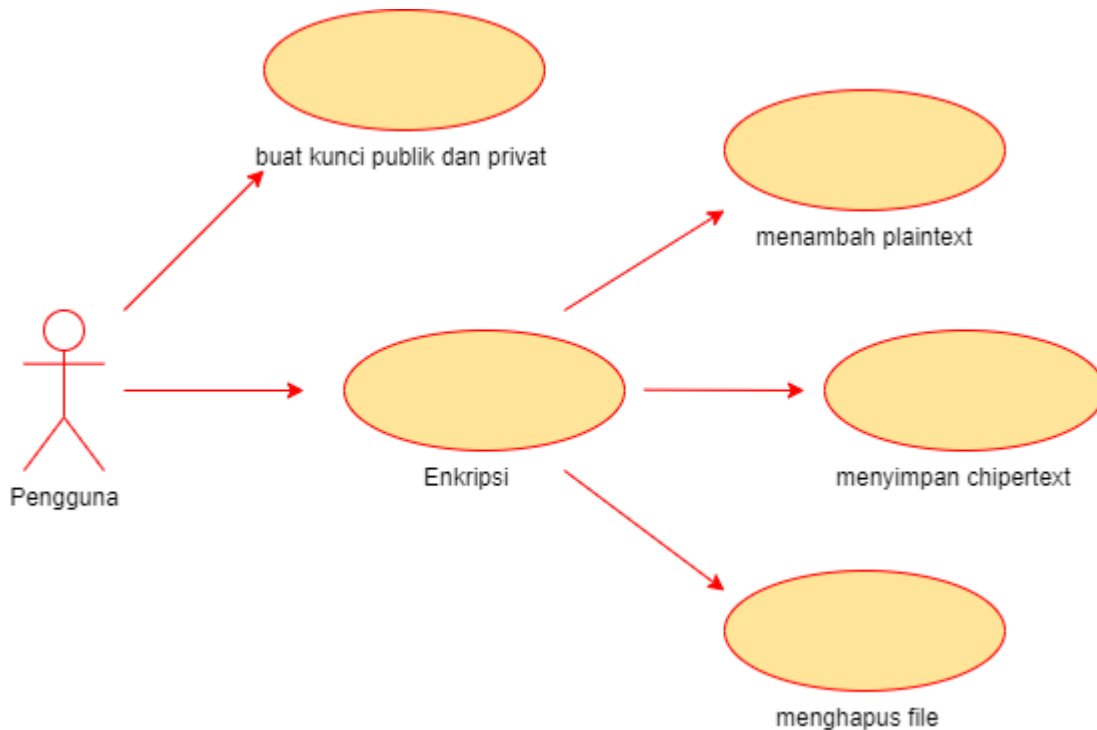


Gambar 4. 2 Proses Dekripsi

4.2.1.2 Unified Modeling Language (UML)

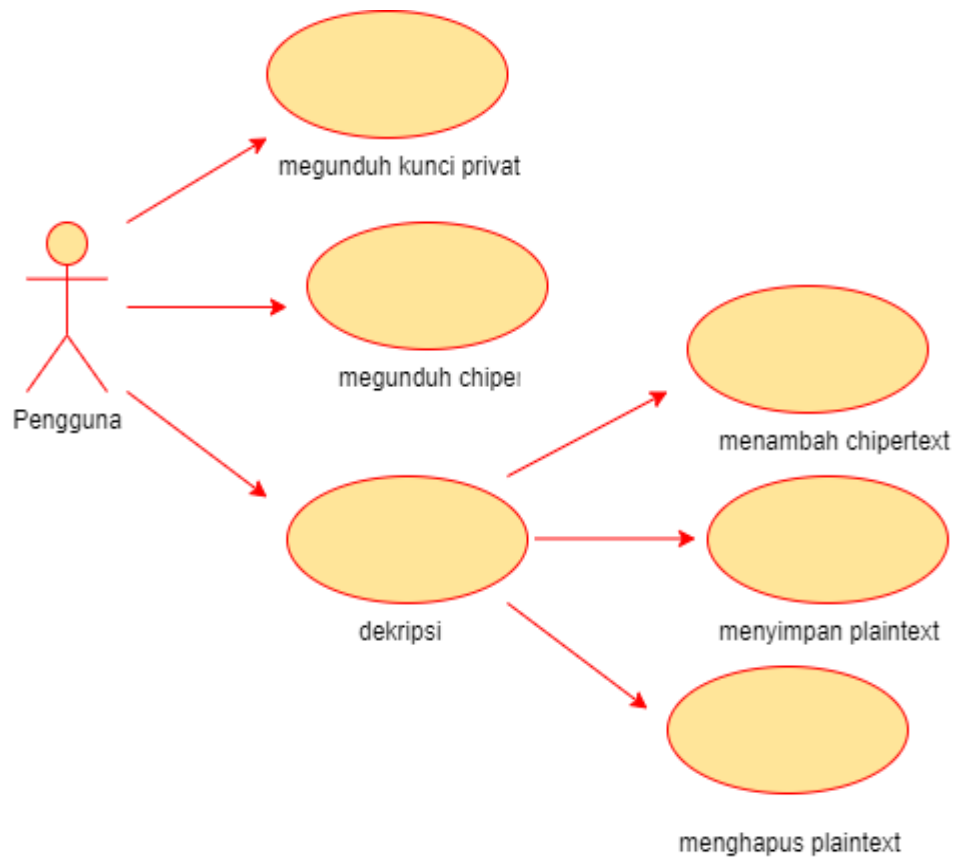
a. Use Case Diagram

Use Case Diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem yang dibangun. Sebuah use case merepresentasikan sebuah interaksi aktor atau pengguna dan penerima dengan sistem yang digunakan. Untuk lebih jelasnya bisa dilihat pada gambar 4.3.



Gambar 4. 3 Use Case Diagram Proses Enkripsi

Gambar 4.3 untuk menjalankan aplikasi RSA, pengguna dapat melakukan proses enkripsi yang diawali dengan membuat kunci public dan private. Setelah itu pengguna dapat menambah file yang akan dienkripsi, kemudian enkripsi file dimana data-data file akan diamankan. Setelah proses enkripsi selesai, pengguna dapat menyimpan file hasil enkripsi.

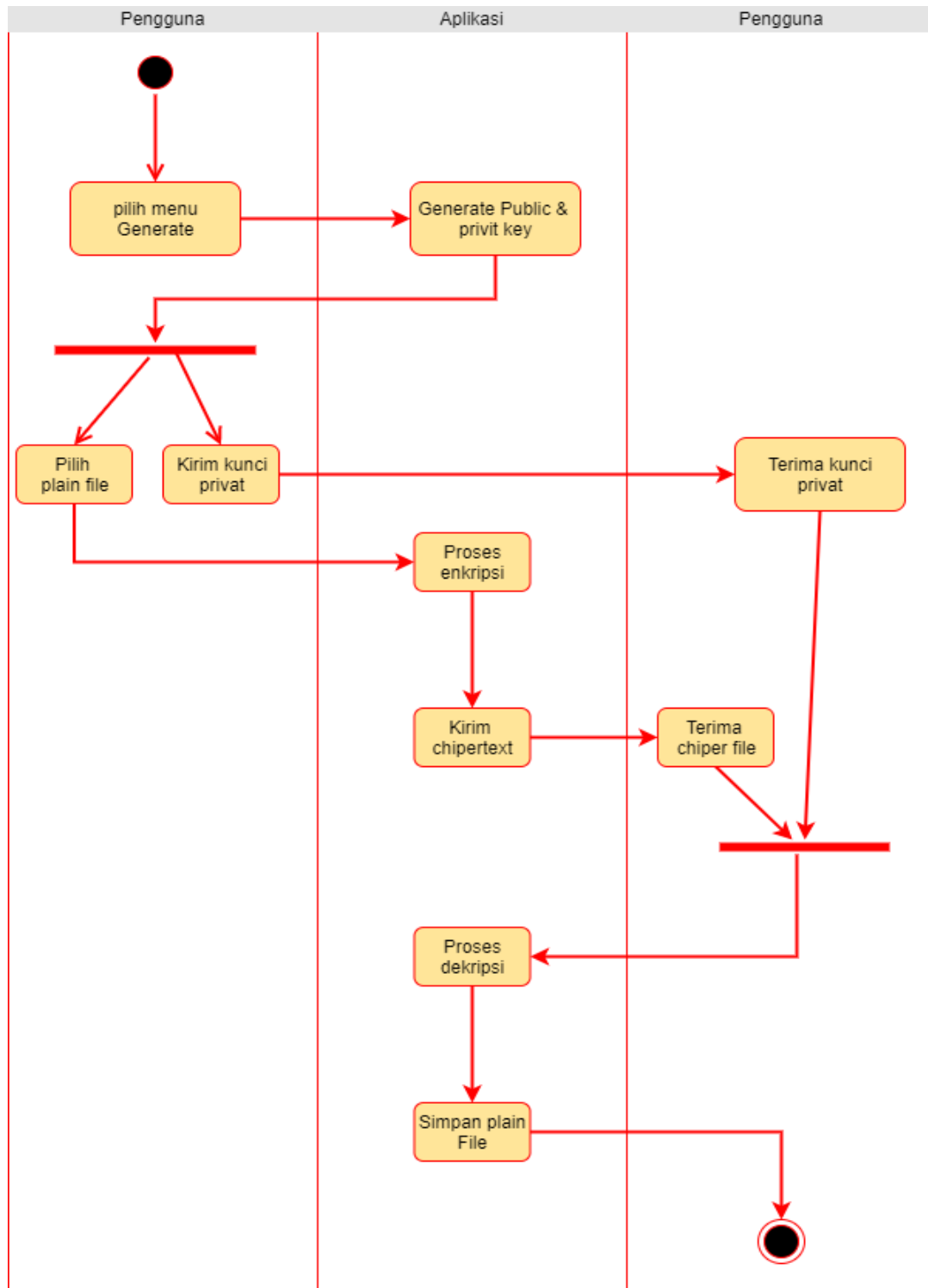


Gambar 4. 4 Use Case Proses Dekripsi

Gambar 4.4 menunjukkan bahwa pengguna dapat melakukan proses dekripsi, dimana dalam proses dekripsi pengguna dapat melakukan 3 aktifitas yaitu menambah file, menghapus file dan menyimpan file hasil dekripsi.

b. Activity Diagram

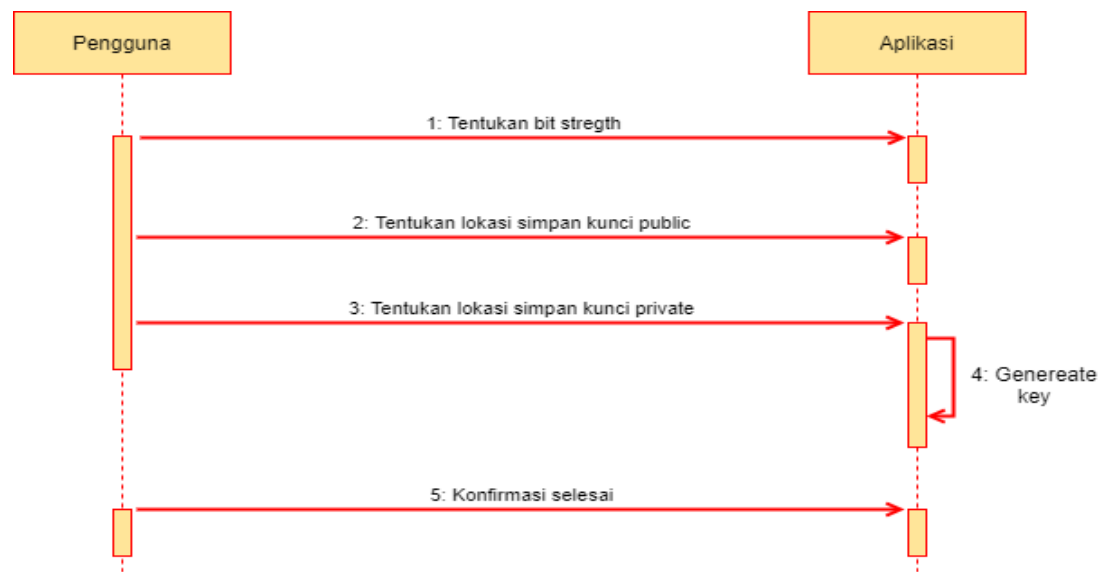
Activity diagram menggambarkan proses-proses yang terjadi mulai aktivitas dimulai sampai aktifitas berhenti. Untuk kebutuhan proses dalam sistem yang akan dibangun digambarkan pada Gambar 4.5.



Gambar 4. 5 Activity Diagram

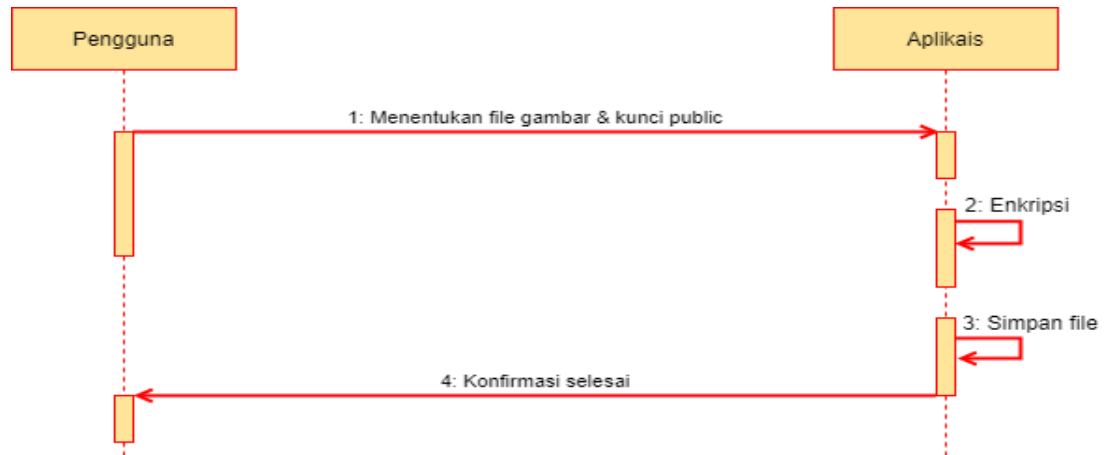
c. Sequence Diagram

Sequence diagram menggambarkan interaksi antar objek di dalam dan di sekitar sistem (termasuk pengguna, display, dan sebagainya) berupa message yang digambarkan terhadap waktu. Sequence diagram terdiri atas dimensi vertikal (waktu) dan dimensi horizontal (objek-objek yang terkait). Digambarkan pada Gambar 4.6.



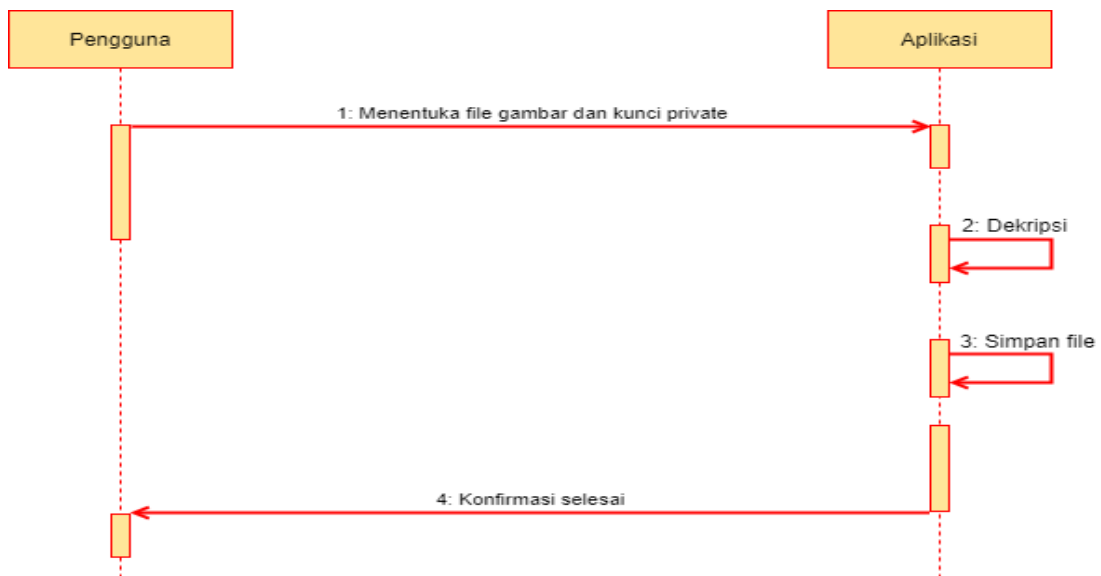
Gambar 4. 6 Sequence Diagram Pembuatan Kunci Publik dan Privat

Gambar 4.6 merupakan sequence diagram untuk proses pembuatan kunci pada aplikasi RSA untuk mengamankan citra digital. Untuk membuat kunci, pengguna diminta untuk menentukan Bit Strength kemudian menentukan lokasi penyimpanan public key. Setelah itu, penerima harus menentukan lokasi penyimpanan Pengguna Aplikasi 1: Tentukan Bit Strength 2: Tentukan Lokasi Simpan Kunci Public 3: Tentukan Lokasi Simpan Kunci Private 4: Generate Keys 5: Konfirmasi Selesai 29 private key. Setelah lokasi penyimpanan kunci telah ditentukan, selanjutnya aplikasi akan melakukan proses generate keys.



Gambar 4. 7 Sequence Diagram Proses Enkripsi

Gambar 4.7 merupakan sequence diagram untuk proses enkripsi. Tahap pertama, pengguna diminta untuk menambahkan file yang akan dienkripsi kemudian pengguna diminta untuk memilih file dan kunci public. Setelah itu, aplikasi akan melakukan proses enkripsi untuk mengenkripsi file yang telah ditambahkan tadi. Kemudian pengguna diminta untuk menentukan lokasi penyimpanan hasil enkripsi. Apabila telah selesai, aplikasi akan memberikan konfirmasi kepada pengguna.



Gambar 4. 8 Sequence Diagram Proses Dekripsi

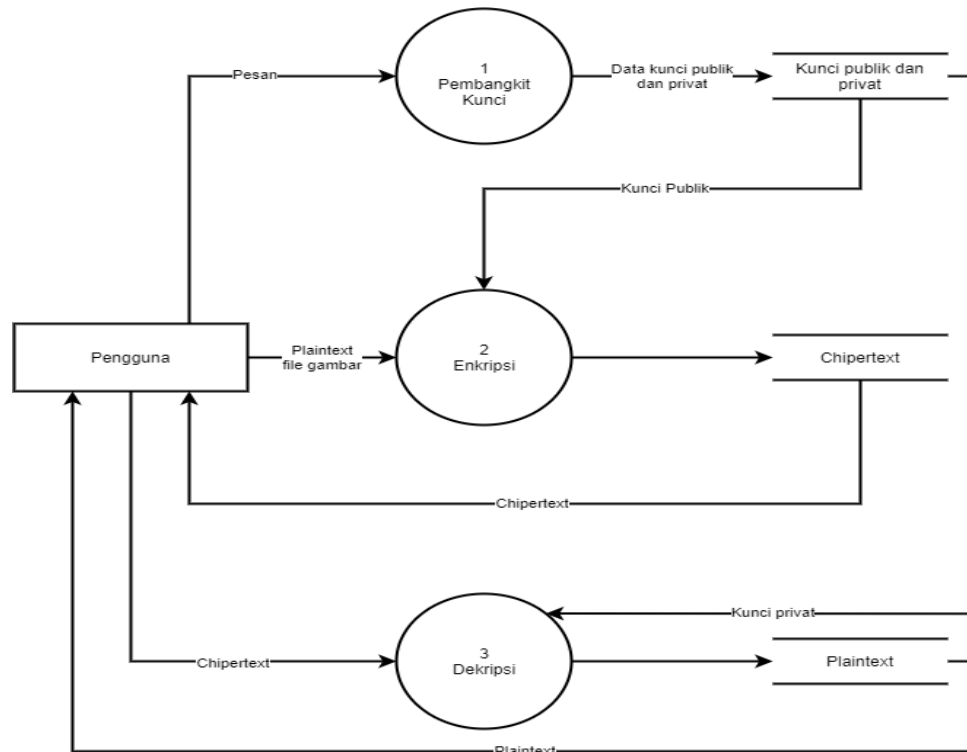
Gambar 4.8 merupakan sequence diagram untuk proses dekripsi. Tahap pertama, pengguna diminta untuk menambahkan file yang akan didekripsi kemudian pengguna diminta untuk menentukan file dan kunci private untuk mendekripsi file yang telah ditambahkan. Setelah itu, pengguna diminta untuk menentukan lokasi penyimpanan hasil dekripsi. Apabila proses tersebut telah selesai, maka aplikasi akan memberikan konfirmasi kepada pengguna.

4.1.2.3 Data Flow Diagram (DFD)

DFD (Data Flow Diagram) adalah suatu model data atau proses yang dibuat untuk menggambarkan dari mana asal data dan ke mana tujuan data yang keluar dari sistem, di mana data tersimpan, proses apa yang menghasilkan data tersebut dan interaksi antara data tersimpan dan proses yang dikenakan pada data tersebut, serta output dari data yang telah diinputkan.

a. Data Flow Diagram Level 0

DFD level 0 adalah diagram yang menggambarkan level 0 pada diagram jenjang yaitu proses Pembangkitan kunci public dan privat, proses enkripsi, dan proses dekripsi. Diagram ini menjelaskan cara kerja keseluruhan sistem rancangan, DFD level 0 dapat dilihat pada Gambar 4.9.



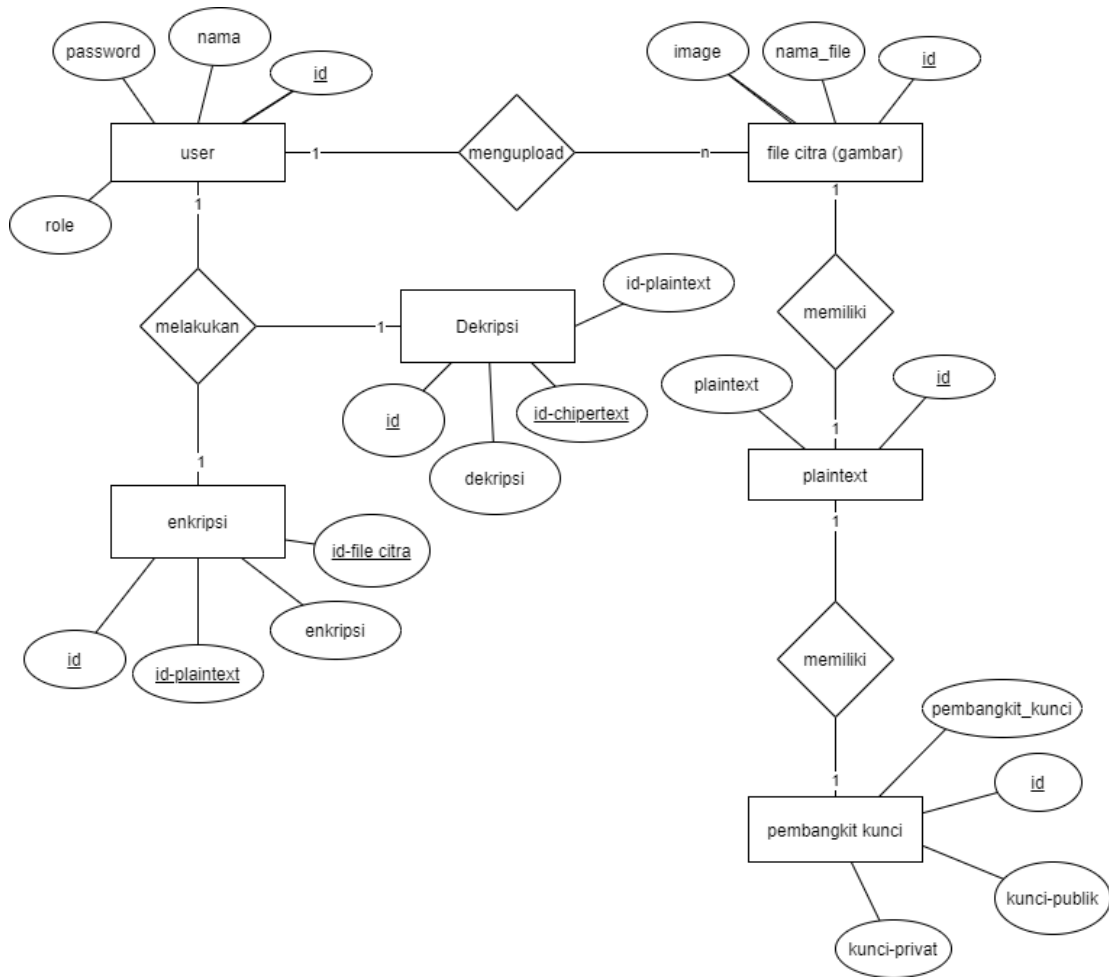
Gambar 4. 9 DFD Level 0

4.2.2 Desain fisik

Tujuan dari tahapan ini adalah mentransformasikan kebutuhan bisnis yang direpersentasikan sebagai desain logik menjadi desain fisik yang nantinya akan dijadikan acuan dalam membuat sistem yang akan dikembangkan.

4.2.2.1 Entity Relationship Diagram (ERD)

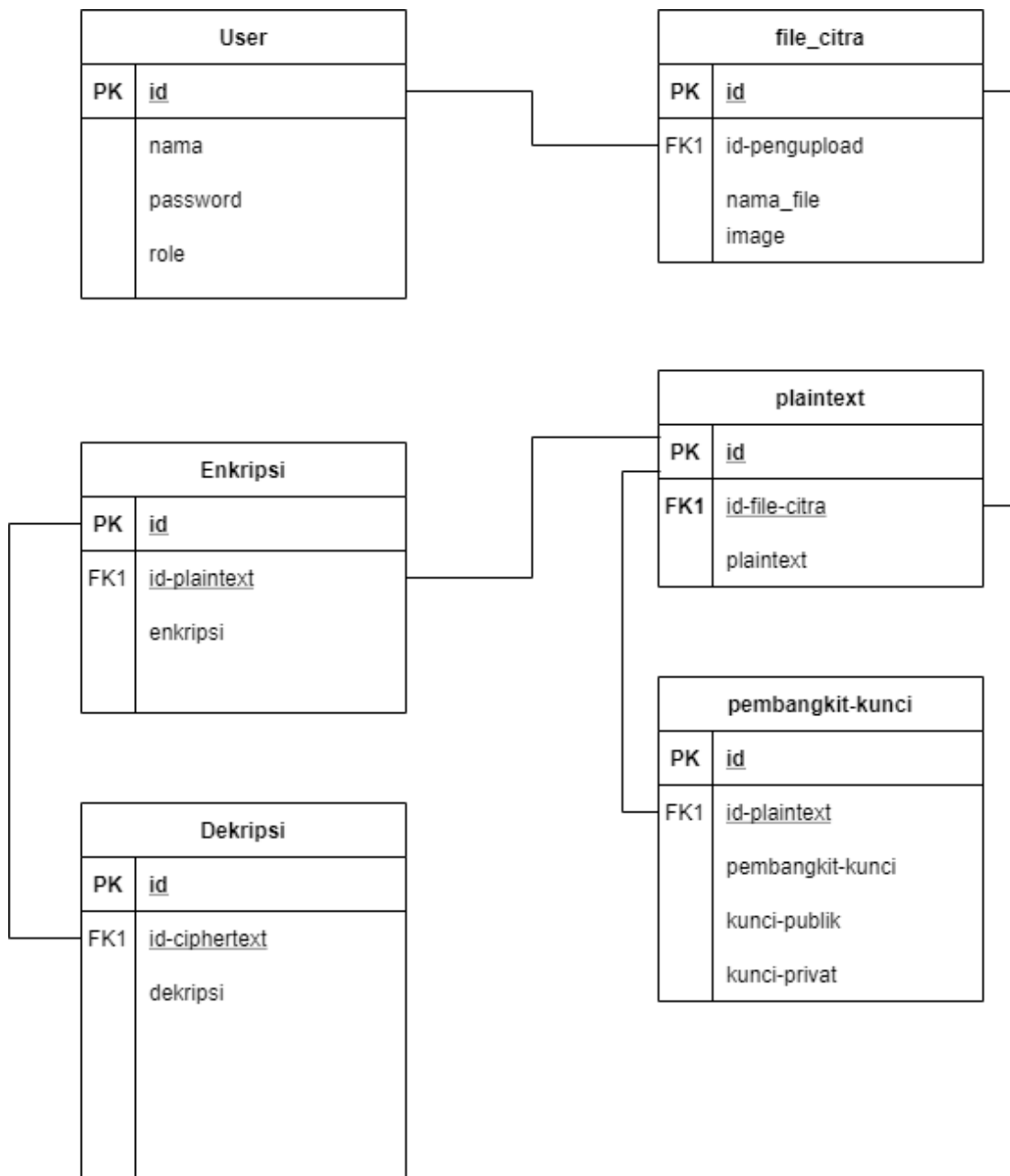
Entity Relationship Diagram yaitu diagram yang dapat mengekspresikan keseluruhan data logis struktur penggambaran basis data. Menjelaskan tentang hubungan antar entitas yang digunakan dalam pembuatan aplikasi implementasi kriptografi RSA untuk keamanan data pada citra digital berbasis website seperti Gambar 4.10. Entity Relationship Diagram digunakan karena dapat menggambarkan himpunan entitas dan relasi yang masing-masing dilengkapi dengan atribut - atribut yang merepresentasikan seluruh fakta dari dunia nyata dengan lebih sistematis.



Gambar 4. 10 ERD implemtasi Algoritma Kirptografi RSA

4.2.2.2 Relasi Tabel

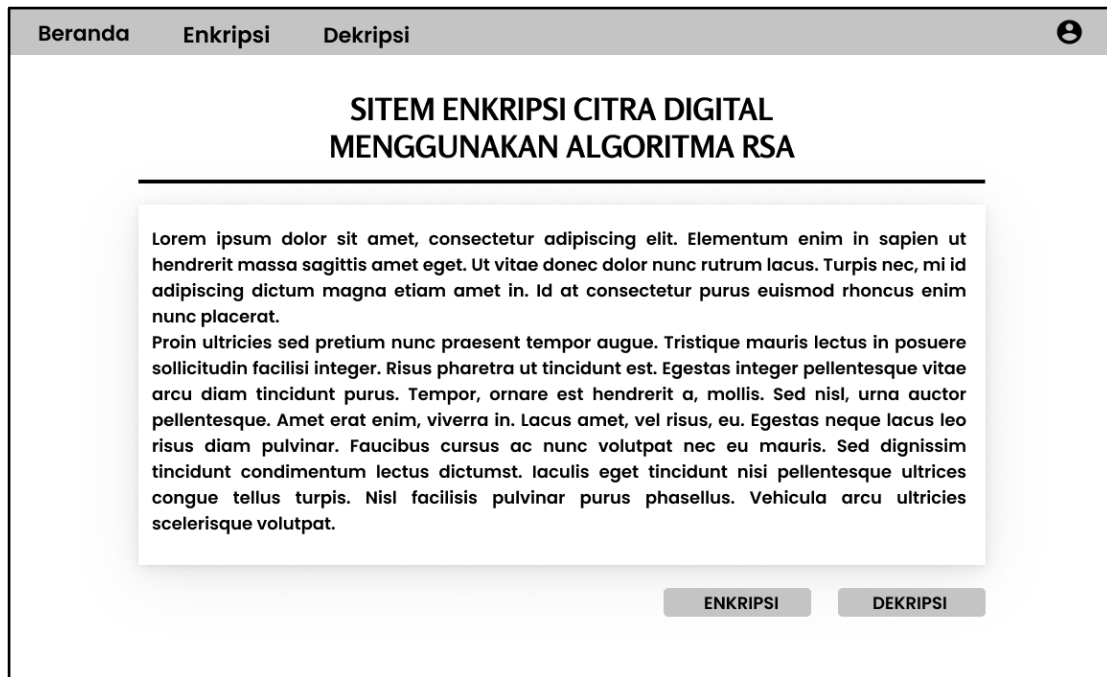
Relasi antar tabel digambarkan dengan garis-garis yang terhubung antar masing-masing tabel. Garis tersebut merupakan hubungan antara primary key dengan foreign key dari tabel. Dari rancangan tabel yang sudah dibuat, maka relasi tabel dari sistem ini bisa dilihat pada Gambar 4.11.



Gambar 4. 11 Relasi Tabel

4.2.2.3 Desain Antar Muka

Berikut adalah desain tampilan dari website yang akan dibuat sebagai dasar dari desain tampilan untuk gambaran awal pembuatan website:



Gambar 4. 12 Antarmuka Halaman Beranda


[Beranda](#) [Enkripsi](#) [Dekripsi](#)

SITEM ENKRIPSI CITRA DIGITAL MENGUNAKAN ALGORITMA RSA

Upload File Citra

Pilih

Citra Asli



Bangkitkan Kunci

Nilai P

Nilai Q

Nilai n

Kunci Publik


Kunci Private

Simpan Kunci

Kunci Publik

Proses Enkripsi

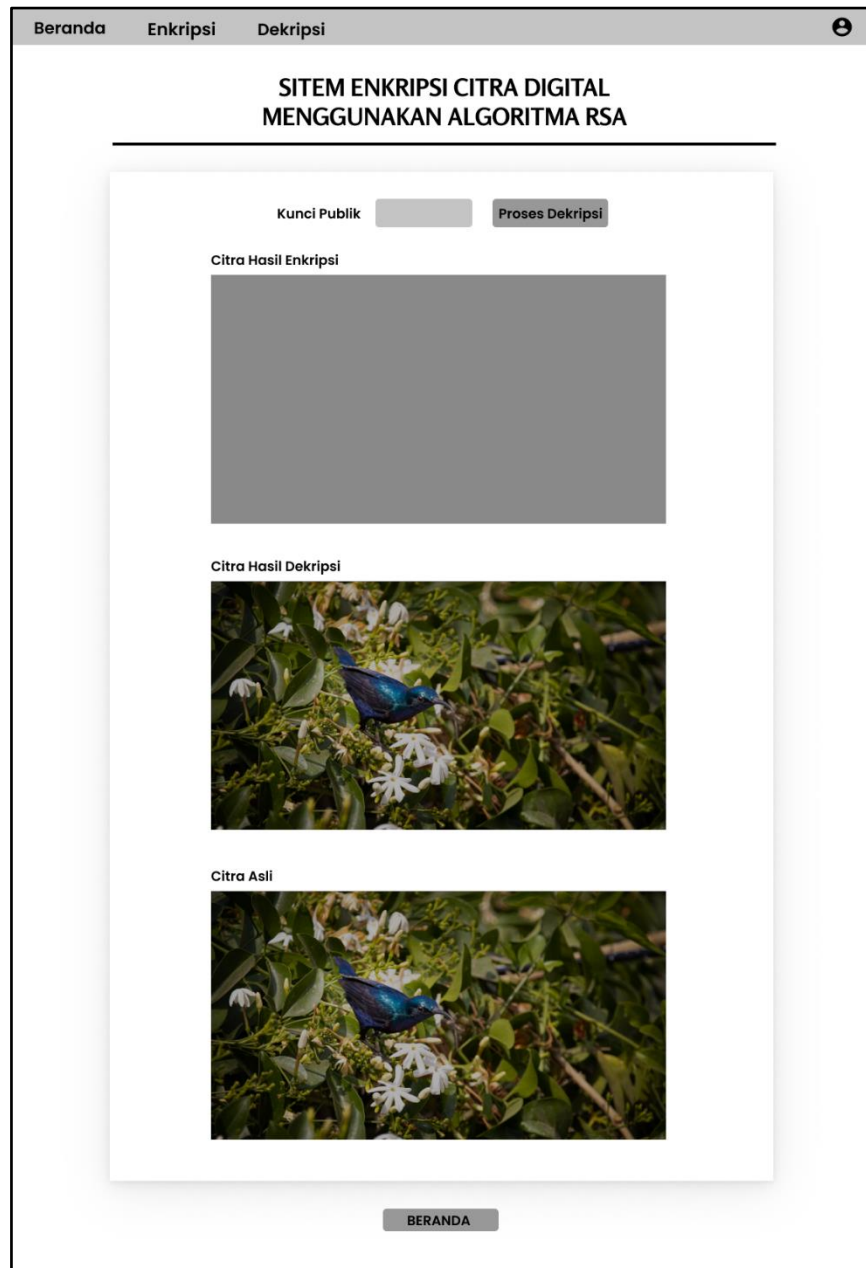
Citra Hasil Enkripsi



SIMPAN CITRA

[BERANDA](#) [DEKRIPSI](#)

Gambar 4. 13 Antarmuka Halaman Enkripsi



Gambar 4. 14 Antarmuka Halaman Dekripsi

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan dan evaluasi dari bab-bab terdahulu, dapat ditarik kesimpulan sebagai berikut:

- a. Pembangkitan kunci pada algoritma RSA menggunakan nilai p dan q yang dibangkitkan dari random bilangan prima. Sehingga didapatkan kunci publik dan kunci privat yang digunakan untuk enkripsi dan dekripsi. Semakin besar nilai kunci publik dan kunci privat akan menghasilkan enkripsi yang lebih bagus. Namun, kunci dengan nilai lebih besar diperlukan waktu sedikit lebih lama untuk proses enkripsi dan dekripsi citra digital.
- b. Hasil enkripsi dan dekripsi algoritma RSA pada penelitian ini mampu menyamarkan citra saat proses enkripsi. Serta dapat mengembalikan ke citra digital semula pada proses dekripsi.

DAFTAR PUSTAKA

- Agung, H. dan Prasta, I. (2018), *Implementasi Algoritma Rivest , Shamir , Adleman Untuk File Sharing Pada PT . Sumber Makmur Pangan Sejahtera Berbasis Web*, , 5(2), 96–102
- Deskiva, Z.Z., Studi, P., Informatika, T., Digital, C., Password, P. dan Aplikasi, P. (2014), *Implementasi Kriptografi Modern Dengan Metode*, , 44–49
- Hariyanto, Nugraha, F.R., Saepul, L. dan Irawati, D.R. (2018), *Aplikasi Enkripsi Dan Dekripsi Pada Soal Ujian Menggunakan Algoritma RSA Berbasis JAVA Desktop*, , 17(September)
- Ipandi, M.F., Hafiz, A. Al, Afriliansyah, Febrian, M.A. dan Hasan, M.A. (2020), *Penerapan Algoritma Kriptografi Asimetris Dengan Metode RSA Dan Blowfish Untuk Enkripsi Dan Dekripsi Gambar Menggunakan Java Netbeans*, , (January), 1–8
- Marsudi, D. (2016), *Politeknik Negeri Sriwijaya 4, Pembangkitan Energi Listrik*, 7(1), 4–31
- Menezes dan Oorchot (1996), *Kriptografi*,
- Muzakir, A. (2016), *Prosiding 4, Implementasi Teknik Steganografi dengan Kriptografi Kunci Private AES Untuk Keamanan File Gambar Berbasis Android*, 6
- Otto (2011), *Bootstrap*,
- Rakhman, A.A. dan Kurniawan, A.W. (2015), *Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Pada Gambar Bitmap 8 Bit, Techno.COM, 14(2), 122–134, ISSN:2356-2579*
- Rusri Yanti, N. dan Zebua, T. *Cipher Untuk Pengamanan File Gambar*,
- Siringoringo, R. (2020), *Analisis Dan Implementasi Algoritma Rijndael (AES) Dan Kriptografi RSA Pada Pengamanan File*, , 02(01), 31–42