KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH

SKRIPSI

PENERAPAN ALGORITMA *RSA* DAN *MD5* PADA KEAMANAN DATA DOKUMEN

Diajukan oleh:

1. **BAGAS KARA / 011160013**
2. **ASEP ARIFIN / 011160052**
3. **IMAM ISWAHYUDI / 011160011**

Untuk Memenuhi Sebagian dari Syarat

Mencapai Gelar Sarjana Komputer

PALEMBANG

2021

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH

SKRIPSI

PENERAPAN ALGORITMA *RSA* DAN *MD5* PADA KEAMANAN DATA DOKUMEN

Diajukan oleh:

1. BAGAS KARA / 011160013

2. ASEP ARIFIN / 011160052

3. IMAM ISWAHYUDI / 011160011

Untuk Memenuhi Sebagian dari Syarat

Mencapai Gelar Sarjana Komputer

PALEMBANG

2021

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH

HALAMAN PENGESAHAN PEMBIMBING SKRIPSI

NAMA/NPM	**: 1. BAGAS KARA / 011160013**
	2. ASEP ARIFIN / 011160052
	3. IMAM ISWAHYUDI / 011160011
PROGRAM STUDI	**: S1 INFORMATIKA**
JENJANG PENDIDIKAN	**: STRATA SATU (S1)**
JUDUL	**: PENERAPAN ALGORITMA *RSA* DAN *MD5* PADA KEAMANAN DATA DOKUMEN**

Tanggal : 21 Januari 2021

Pembimbing

Hendra Effendi, S.Kom., M.Kom.
NIDN : 0217108001

Mengetahui,

Ketua

Benedictus Effendi, S.T., M.T.
NIP : 09.PCT.13

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH

HALAMAN PENGESAHAN PENGUJI SKRIPSI

NAMA/NPM	**: 1. BAGAS KARA / 011160013**
	2. ASEP ARIFIN / 011160052
	3. IMAM ISWAHYUDI / 011160011
PROGRAM STUDI	**: S1 INFORMATIKA**
JENJANG PENDIDIKAN	**: STRATA SATU (S1)**
JUDUL	**: PENERAPAN ALGORITMA *RSA* DAN *MD5* PADA KEAMANAN DATA DOKUMEN**

Tanggal : 11 Februari 2021	**Tanggal : 11 Februari 2021**
Penguji 1	**Penguji 2**
Surahmat, S.Kom., M.Kom.	**Guntoro Barovih, S.Kom., M.Kom.**
NIDN : 0217058703	**NIDN : 0201048601**

Menyetujui,

Ketua

Benedictus Effendi, S.T., M.T.

NIP : 09.PCT.13

MOTTO : "Sesungguhnya bersama, kesulitan ada kemudahan"

"Cobalah untuk tidak menjadi seseorang yang sukses, tetapi menjadi seseorang yang bernilai"

"Tanda sejati kecerdasan bukanlah pengetahuan tapi imajinasi"

Kepada :

- Ayahanda dan Ibunda Tercinta Kami
- Saudara-saudari tersayang serta Keluarga besar kami
- Para Pendidik yang kami hormati
- Para sahabat dan teman yang selalu memberikan semangat serta dukungan untuk menyelesaikan skripsi kami
- Team 7, team santuy, sabar, tepat, team debat walau satu kelompok, team jalan-jalan malam dan kumpul gak jelas, Dah sekian.

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT atas rahmat dan karunia-Nya, yang telah memberikan kesehatan dan kesempatan sehingga penulis dapat menyelesaikan laporan skripsi dengan baik. Penulisan laporan skripsi ini bertujuan untuk memenuhi syarat dan menyelesaikan pendidikan pada jurusan S1 Informatika STMIK PalComTech Palembang, guna mencapai gelar Sarjana Komputer. Oleh karena itu, kami berharap dan memohon dukungan dan dorongannya kepada semua pihak yang membaca laporan ini. Dan tidak lupa kami ingin mengucapkan banyak terimakasih kepada:

1. Bapak Benedictus Effendi, S.T., M.T., selaku Ketua STMIK PalComTech Palembang, yang telah melakukan tugas wewenangnya dengan sangat baik selama masa waktu perkuliahan kami.
2. Bapak Hendra Effendi, S.Kom., M.Kom., selaku pembimbing skripsi kami yang telah mengarahkan dan membimbing serta membantu kami dalam pengerjaan laporan ini.
3. Ayah, Ibu, saudara-saudara kami dan seluruh keluarga yang telah memberikan dorongan semangat moral dan finansial kepada kami selama masa pendidikan kami.
4. Sahabat dan rekan-rekan yang turut membantu memberikan semangat dan dorongan yang kuat dalam menyelesaikan laporan ini.

Semua bantuan dan bimbingan arahan serta semangat yang telah diberikan kepada penulis sangat berharga, semoga Allah SWT selalu membalas kebaikan mereka. Dalam pembuatan laporan ini, penulis menyadari bahwa banyak sekali kekurangan serta juga banyak rintangan yang harus kami dihadapi dalam meneyelesaikan laporan ini.

Kami mohon maaf jika masih banyak kekurangan atas penelitian dan laporan ini. Oleh karena itu penulis menerima adanya kritik dan saran untuk mengembangkan laporan penelitian kami.

Akhir kata, kami ingin mengucapkan terima kasih atas semua yang bersangkutan. semoga laporan penelitian Skripsi ini dapat membantu dan berguna bagi semua pihak yang membutuhkan terkait dengan penelitian kami.

Palembang, 11 Februari 2021

Penulis

DAFTAR ISI

BAB IV METODE PENELITIAN

BAB V METODE PENELITIAN

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ABSTRACT

BAGASKARA, ASEP ARIFIN, IMAM ISWAHYUDI. *Application of the RSA and MD5 algorithms on document data security.*

Cryptography is the art of maintaining message security when messages are sent Form one place to another. Cryptography is also used to identify message sending with digital signatures and the authenticity of messages with a digital fingerprint (fingerprint). RSA is a cryptographic technique using 2 prime numbers. Form these two prime numbers, you can get a Publik Key (used to encrypt a plaintext) and a Privat Key (used to decrypt the ciphertext). In the RSA algorithm, there are three processes, namely, key generation, encryption process and decryption process. The difficulty of this algorithm is how to find two large prime number factors that will be used as the publik key and the privat key. Signatures are used to prove document authentication. Digital signature technology makes use of publik and privat keys. The privat key is kept by the owner, the privat key is also used to create digital signatures.

Keywords: RSA, MD5, Sieve Of Atkin (SOA), Blum-Blum shub (BBS）.

ABSTRAK

BAGASKARA, ASEP ARIFIN, IMAM ISWAHYUDI. Penerapan algoritma *RSA* dan *MD5* pada keamanan data dokumen.

Kriptografi merupakan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*fingerprint*). *RSA* merupakan teknik Kriptografi dengan memanfaatkan 2 bilangan prima. Dari kedua bilangan prima tersebut dapat diperoleh sebuah Publik *Key* (digunakan untuk mengenkripsi sebuah *plaintext*) dan sebuah Privat *Key* (digunakan untuk mendekripsi *ciphertext*), 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. Tanda tangan digunakan utntuk membuktikan otentikasi dokumen. Teknologi tanda tangan digital memanfaatkan kunci publik dan privat. Kunci privat disimpan oleh pemiliknya, kunci privat juga digunakan untuk membuat tanda tangan digital.

Kata Kunci : *RSA, MD5, Sieve Of Atkin (SOA), Blum-Blum shub (BBS).*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Di era teknologi informasi saat ini, pengiriman data dan informasi menjadi hal yang sangat penting. Dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu data maupun informasi, sehingga data tersebut dapat dikirim dengan aman. Salah satu cara untuk menjaga keamanan dan kerahasian suatu data maupun informasi adalah dengan teknik *enkripsi* dan *dekripsi* guna membuat pesan, data, maupun informasi agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali penerima yang berhak.

Sekarang banyak terjadi manipulasi data serta pencurian data ataupun kerusakan pada keaslian *file* tersebut dalam melakukan pengiriman dan penyimpanan data pada komputer sehingga rentan terhadap kebocoran data yang ingin dijaga kerahasiaanya. Teknik pengamanan data menggunakan *enkripsi* dan *dekripsi* dikenal dengan nama kriptografi sebagai sebuah ilmu atau seni untuk mengamankan pesan atau data dengan cara menyamarkan pesan tersebut sehingga hanya dapat dibaca oleh pengirim dan penerima pesan.

Didunia dengan arus informasi yang semakin global, Kriptografi telah menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan data.

Ada berbagai algoritma kriptografi yang sekarang ini telah dan sedang dikembangkan, salah satunya diantaranya algoritma kunci *simetris* ataupun *asimetris* (pembagian berdasarkan kunci).

Menurut Ardelia ‘dkk’ (2017), *RSA* adalah didasari oleh dua problem matematika yaitu masalah dalam faktorisasi bilangan berjumlah banyak. Dan masalah dari *RSA*, yaitu mencari *modulo* akar e n dari sebuah bilangan komposit (yang faktor-faktornya tidak diketahui proses *dekripsi* penuh dari sebuah *ciphertext RSA* dianggap sesuatu hal yang tidak mudah karena kedua masalah ini diasumsikan sulit. Dalam hal ini penulis melakukan sebuah penelitian bagaimana membuat perangkat *lunak* untuk mengimplementasikan *enkripsi* dan *dekripsi file* dokumen dengan metode *RSA* sebagai Kriptografi dan *MD5* sebagai *digital signature* dengan menerapkan algoritma *Sieve Of Atkins* (*SOA*) sebagai pembangkit bilangan prima dan Algoritma *Blum-Blum Shub* (*BBS*) sebagai pembangkit bilangan acaknya.

Berdasarkan latar belakang di atas maka penulis akan mengangkat sebuah judul “**Penerapan Algoritma *RSA* Dan *MD5* Pada Keamanan Data Dokumen (*Application Of RSA And MD5 Algorithm On Dokument Data Security*)”.**

1.2. Rumusan Masalah Penelitian

Rumusan masalah penelitian ini adalah “Bagaimana cara membuat prangkat *lunak* keamanan data serta keaslian data pada *file* tersebut untuk mengimplementasikan *enkripsi* dan *dekripsi file* dokumen dengan metode *RSA* dan *MD5*?”.

1.3. Ruang Lingkung Penelitian

Ruang lingkup penelitian ini adalah sebagai berikut :

a. Data yang di*enkripsi* berupa sebuah data audio, video, dan data file dokumen dengan *Format doc, excel, pdf, ppt, dan txt.*
b. Algoritma *RSA* digunakan untuk *enkripsi* dan *dekripsi* data dokumen.
c. Algoritma *Sieve Of Atkins* digunakan untuk pembangkit bilangan prima.
d. Algoritma *Blum-Blum Shub* (*BBS*) digunakan untuk pembangkit bilangan acak.
e. Algoritma *MD5* digunakan untuk tanda tangan *digital* (*Digital signature*).
f. Bahasa pemrograman *PHP* dan *database MySQL*.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah membangun sebuah aplikasi keamanan data berbasis *web* dengan menggunakan algoritma *RSA* sebagai *enkripsi* dan *dekripsi* data dokumen serta menerapkan algoritma *MD5* sebagai tanda tangan *digital* (*Digital signature*) untuk memastikan keaslian data tersebut.

1.5. Manfaat Penelitian

Penelitian ini diharapkan bermanfaat bagi tempat penelitian, akademik, dan penelitian sendiri, meliputi :

1.5.1. Manfaat Penelitian Bagi Penulis

Penulis dapat menerapkan ilmu pengetahuan yang diperoleh selama waktu perkuliahan khususnya dalam bidang pemrograman dan keamanan data.

1.5.2. Manfaat Penelitian Bagi Akademik

Sebagai referensi bagi penelitian selanjutnya dalam pembuatan laporan skripsi, khususnya mahasiswa STMIK PalComTech, dan dapat menjadi bahan perbandingan dalam penelitian bagi pihak yang berkepentingan dalam *enkripsi* dan *dekripsi* keamanan data dokumen.

1.6. Sistematik Penulisan

Penulis menggunakan pembahasan yang sesuai dengan ketentuan yang diberikan, sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi uraian latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian.

BAB II GAMBARAN UMUM PERANGKAT *LUNAK* YANG DIKEMBANGKAN

Bab ini berisi tentang perangkat *lunak* yang akan dikembangkan dalam penelitian.

BAB III TINJAUAN PUSTAKA

Bab ini berisi teori berdasarkan penulis yang terdiri dari landasan teori, penelitian terdahulu dan kerangka penelitian.

BAB IV METODE PENELITIAN

Bab ini berisi tentang waktu dan jenis penelitian, jenis dan pengumpulan data, pengembangan dan pengujian sistem.

BAB V HASIL DAN PEMBAHASAN

Bab ini memuat hasil yang diperoleh dalam penelitian dan pembahasan serta masalah yang telah ditemukan peneliti.

BAB VI PENUTUP

Bab ini berisi kesimpulan dan saran dari pembahasan dalam penelitian yang telah dilakukan

BAB II

GAMBARAN UMUM PERANGKAT *LUNAK* YANG DIKEMBANGKAN

2.1. *Enkripsi* dan *Dekripsi* pada Aplikasi

Menurut Rizal "dkk" (2011), *enkripsi* dan *dekripsi* dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Informasi ini dapat berupa nomor kartu *kredit*, catatan penting dalam komputer, maupun pass*word* untuk mengakses sesuatu. *Dekripsi* dalam dunia keamanan komputer merupakan proses untuk mengubah *chipertext* menjadi *plaintext* atau pesan asli. Jadi *Dekripsi* merupakan kebalikan dari *Enkripsi* upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri.

2.2. Fenomena Perangkat *Lunak* Yang Dikembangkan

Penerapan metode pengamanan data *enkripsi* dan *dekripsi* ini penulis menggunakan metode algoritma *RSA* dengan dukungan algoritma *Sieve Of Atkins (SOA)* sebagai pembangkit bilangan prima dan *Blum Blum Shub (BBS)* sebagai pembangkit bilangan acaknya dan disertai algoritma *MD5* sebagai *Digital Signature.* Sebelum menggunakan aplikasi pengguna harus mendaftarkan diri terlebih

dahulu sebagai *user*. Untuk mendapatkan kunci *publik* fungsinya untuk mengenkripsi *file* dan kunci *privat* fungsinya untuk mendekripsi *file*.

Setelah terdaftar *user* meng-*upload file*, sebelum melakukan *enkripsi file user* membuat *digital signature* pada *file* tersebut menggunakan kunci privat pengirim, setelah *file* terdapat *digital signature* selanjutnya *user* melakukan *enkripsi file* menggunakn kunci publik penerima yang sudah didapat pada saat melakukan pendaftaran *user*, setelah *file* ter*enkripsi user* mengirim *file* tersebut kepada penerima yang akan didekripsi oleh penerima menggunakan kunci *privat* yang dia miliki, penerima akan memeriksa *digital signature* untuk memastikan bahwa *file* tersebut memang benar

BAB III

TINJAUAN PUSTAKA

3.1 Teori Pendukung

3.1.1 Kriptografi

Menurut kurniawaan “dkk” (2017), kriptografi merupakan suatu teknik menyembunyian pesan dimana pesan tersebut hanya dapat diketahui oleh orang tertentu dimana pesan itu sering disebut dengan enkripsi). Menurut terminologi Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dengan tanda tangan *digital* dan keaslian pesan dengan sidik jari *digital* (*fingerprint*). Adapun istilah-istilah yang digunakan dalam kriptografi dalam melakukan proses kerjanya adalah sebagai berikut:

a. *Plaintext* merupakan pesan asli yang belum disandikan atau informasi yang ingin dikirimkan atau dijaga keamanannya.
b. *Ciphertext* merupakan pesan yang telah disandikan (dikodekan) sehingga siap untuk dikirimkan.
c. *Enkripsi* merupakan proses yang dilakukan untuk menyadikan *plaintext* menjadi *ciphertext* dengan tujuan pesan tidak dapat dibaca oleh pihak yang tidak berwenang

d. *Dekripsi* merupakan proses yang dilakukan untuk memperoleh kembali *plaintext* dari *ciphertext.*

e. Kunci yang dimaksud disini adalah kunci yang dipakai untuk melakukan *dekripsi* dan *enkripsi*. Kunci terbagi menjadi dua kunci pribadi (privat *key*) dan kunci umum (publik *key*).

3.1.2 Tujuan Kriptografi

Menurut A prayitno (2017), terdapat empat tujuan yang mendasarikriptografi, yaitu :

a.Kerahasiaan

Memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan data/informasi denganteknik enkripsi.

b.Integritas data

Memberikan jaminan bahwa dari setiap bagian dalam informasi tidak mengalami perubahan dari saat dibuat/dikirim hinggasaat informasitersebut dibuka.

c.Penyangkalan

Memberikan cara untuk membuktikan bahwa suatudokumen datang dari seseorang bila ia mencoba menyangkal telah memiliki dokumen tersebut.

d.Autentikasi

Memberikan dua bentuk layanan, pertama adalah mengidentifikasi keaslian suatu pesandan memberikan jaminan keotentikannya, dan

kedua adalah untuk menguji identitas seseorang bila ia akan memasuki sebuah sistem.

3.1.3 *Symmetric cryptosistem*

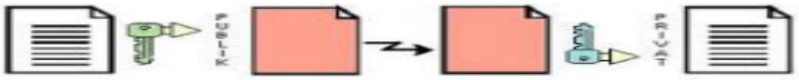
Symmetric cryptosistem atau Kriptografi *simetris* atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses *enkripsi* sama dengan kunci untuk proses *dekripsi*. Algoritma Kriptografi *simetris* dibagi menjadi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma *blok* (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu *bit* atau satu *byte* data. Sedang pada algoritma *blok*, proses penyandiannya berorientasi pada sekumpulan bit atau *byte* data (per blok).

Sumber : Basri (2016)

Gambar 3.1 Kunci *Simetris*

3.1.4 *Assymmetric cryptosistem*

Kunci *asimetris* adalah pasangan kunci-kunci Kriptografi yang salah satunya dipergunakan untuk proses *enkripsi* dan yang satu lagi untuk *dekripsi*. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci privat untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.



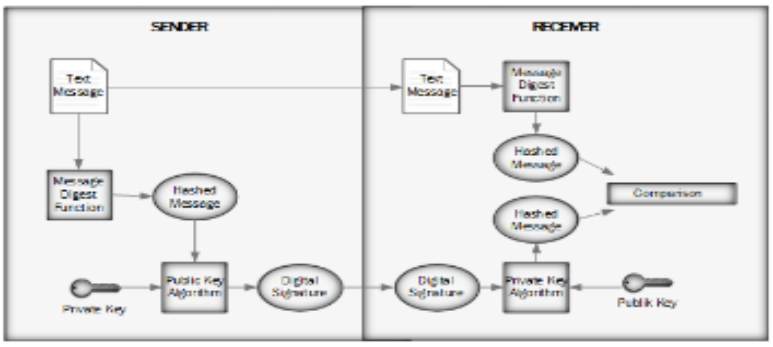
Sumber : Basri (2016)

Gambar 3.2 Kunci *Asimetris*

3.1.5 Tanda Tangan *Digital*

Menurut Junaidy (2015), tanda tangan digital atau yang lebih dikenal dengan digital signaturemerupakan salah satu solusi untuk mengatasi masalah-masalah di atas. Tanda tangan dijital memiliki fungsi sama seperti dengan tanda tangan pada dokumen biasa, yaitu untuk mengesahkan dokumen. Perbedaannya yaitu pada bentuknya, tanda tangan biasa berupa goresan simbol yang unik sedangkan tanda tangan dijital berupa kode-kode yang berisi nilai kriptografi dimana kode-kode tersebut bergantung pada pesan dan pengirim pesan.

Salah satu tanda tangan digital yang banyak digunakan adalah tanda tangan digital dengan fungsi *hash* (*hashfunction*). Fungsi hashyang digunakan adalah fungsi *hash MD5*. *MD5* atau *Message Digest* 5 adalah fungsi *hash* satu arah untuk mendapatkan nilai *hash* sepanjang 128 bit dari pesan yang ukurannya sembarang.



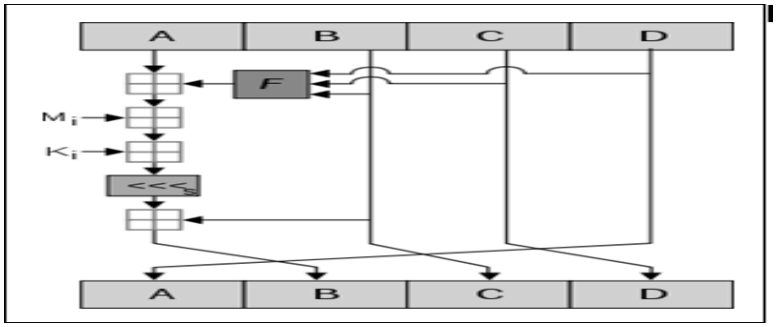
Sumber : Egi Cahyo Prabowo ‘dkk’ (2017)

Gambar 3.3 Alur Proses *Digital Signature*

3.1.6 Algoritma *MD5*

Menurut Kardi (2020), kriptografi, *MD5* (*Message-Digestalgortihm 5*) ialah fungsi *hash* kriptografi yang digunakan secara luas dengan *hash value* 128-bit. Pada standart Internet (RFC1321), *MD5* telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan,dan *MD5* juga umum digunakan untuk melakukan pengujian integritas sebuah berkas. *Message Digest 5* (*MD5*) adalah salah satu penggunaan fungsi *hash* satu arah yang paling banyak digunakan. *MD5* merupakan fungsi *hash* kelima yang dirancang oleh Ron Rivest yang di definisikan pada RFC 1321.*MD5* merupakan pengembangan dari *MD4* dimana terjadi penambahan satu ronde. *MD5* memproses teks masukkan ke dalam blok-blok bit sebanyak 512 bit, kemudian dibagi ke dalam 32 bit sub blok sebanyak 16 buah. Keluaran dari *MD5* berupa 4 buah blok yang masing-masing 32 bit yang mana akan menjadi 128 bit yang biasa disebut nilai *hash*. Simpul utama *MD5* mempunyai blok pesan dengan panjang 512 bit yang

masuk ke dalam 4 buah ronde. Hasil keluaran dari *MD5* adalah berupa 128 bit dari *byte* terendah A dan tertinggi *byte* D.



Sumber : Rosyanti Harahap (2010)

Gambar 3.4 Proses *MD5*

3.1.7 Algoritma *Rivest Shamir Adleman* (*RSA*)

Menurut Stalling (2017), algoritma *RSA* diperkenalkan oleh tiga peneliti dari *MIT* (*Masschussets 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 publik *Key* (digunakan untuk mengenkripsi sebuah *plaintext*) dan sebuah privat *Key* (digunakan untuk mendekripsi *ciphertext*). 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 tersebut p dan q dimana $p \neq q$.

Algoritma *RSA* mendasarkan proses *enkripsi* dan *dekripsi*nya 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 :

a. p dan q bilangan prima (rahasia).
b. r= p.q (tidak rahasia).
c. $\phi(n) = (p - 1)(q - 1)$ (rahasia).
d. e (kunci *enkripsi*) (tidak rahasia).
e. d (kunci *dekripsi*) (rahasia).
f. m (*plaintext*) (rahasia).
g. c (*Chipertext*) (tidak rahasia).

Contoh perhitungan *RSA*

1. pilih dua bilangan prima p dan q

   p = 7

   q = 11

2. cari nilai r dengan cara kalikan bilangan prima p dan bilangan prima q

   r = p.q

   = 7.11

   = 77

3. cari nilai n dengan cara bilangan prima p dikurang satu dan bilangan prima q dikurang satu kemudian kalikan hasil tersebut

   n = (p-1) (q-1)

   = (7-1) (11-1)

   = 60

4. cari nilai e untuk kunci publik yang akan digunakan sebagai *enkripsi file RSA* dengan cara e = 1<e<m = 1

   60 = 30.2+0

   60 = 20.3+0

   60 = 15.4+0

   60 = 12.5+0

   60 = 10.6+0

   60 = 8.7+4

   7 = 3.2+1

   e = 7

5. setelah nilai e didapat cari nilai d untuk kunci privat yang akan digunakan sebagai *dekripsi file* dengan cara d = 1+k(m)/e

   d = 1+0.60/7= 0,14

   d = 1+1.60/7= 8,71

   d = 1+2.60/7= 17,28

   d = 1+3.60/7= 25,85

   d = 1+4.60/7= 34,42

   d = 1+5.60/7= 43

6. setelah nilai e dan d didapatkan kemudian dilakukan *enkripsi dekripsi file*

   e = 7 kunci publik yang akan digunakan untuk *enkripsi*

   d = 43 kunci privat yang akan digunakan untuk *dekripsi*

   plaintext

   A = 65

   K = 75

   Enkripsi $c = M^e \bmod n$

   $65^7 \bmod 77 = 65$

   $75^7 \bmod 77 = 26$

   Dekripsi $p = C^d \bmod n$

   $65^{43} \bmod 77 = 65$

   $26^{43} \bmod 77 = 75$

3.1.8 Algoritma *Sieve Of Atkins (SOA)*

Menurut Khoiruddin “dkk” (2019), algoritma *Sieve of Atkin* adalah sebuah algoritma yang cepat dan *modern* untuk mendapatkan seluruh bilangan *prima* sampai pada suatu batas *integer* yang telah ditentukan. Algoritma ini adalah versi optimasi dari algoritma kuno *Sieve of Eratosthenes*. *Sieve of Atkin* melakukan dahulu beberapa pekerjaan persiapan dan kemudian mencoret kelipatan dari kuadrat bilangan prima, bukannya kelipatan bilangan prima. Algoritma ini diciptakan oleh A. O. L. Atkin dan Daniel J. Bernstein pada tahun 2004. Pada algoritma ini, suatu bilangan dapat disebut bilangan prima

jika bilangan tersebut memenuhi beberapa persyaratan, yaitu

1. Persamaan berikut ini harus memiliki jumlah solusi n yang ganjil:

   a.4x2 + y2 = n dimana n mod 4 =1

   b.3x2 + y2 = n dimana n mod 6 =1

   c.4x2 - y2 = n dimana n mod 12 =11

2. Bilangan tersebut haruslah square-free. Sebuah bilangan yang disebut square-free adalah bilangan yang tidak memiliki faktor prima lebih dari sekali. (Contoh: 20=2*2*5, 20 memiliki 2 buah faktor 2 sehingga bukan merupakan square-free. 21=7*3, 21 tidak memiliki faktor yang dobel dan merupakan bilangan yang square free).

Langkah 1 : Tentukan pencarian bilangan prima bilangan dari 1-n, dimana dalam penelitian ini kita akan dihasilkan bilangan prima nomor dari 1-50, yang seperti itu n = 50.

Langkah 2 : Tandai bilangan 2, 3 dan 5 sebagai bilangan prima.

Langkah 3 : Hitung persamaannya berdasarkan 3 blok berikut :

$4x^2 + y^2 \bmod 4 \Rightarrow 1 \text{ or } 5 \Rightarrow 4x^2 + y^2 < n$....(2)

$3x^2 + y^2 \bmod 6 \Rightarrow 1 \Rightarrow 3x^2 + y^2 < n$.....(3)

$3x^2 – y^2 \bmod 12 \Rightarrow 11 \Rightarrow 0 < 3x^2 – y^2 < n$…(4)

Tabel 3.1 : Persamaan Bilangan Prima

Formula 2			Formula 3			Formula 4		
x	y	n	x	y	n	x	y	n
1	1	5	1	1	4	1	1	2
1	2	8	1	2	7	2	1	11
1	3	13	1	3	12	2	2	8
1	4	20	1	4	19	2	3	3
1	5	29	1	5	28	3	1	26
1	6	40	1	6	39	3	2	23
2	1	17	2	1	13	3	3	18
2	2	20	2	2	16	3	4	11
2	3	25	2	3	21	3	5	2
2	4	32	2	4	28	4	1	47
2	5	41	2	5	37	4	2	44
3	1	37	2	6	48	4	3	39
3	2	40	3	1	28	4	4	32
3	3	45	3	2	31	4	5	23
			3	3	36	4	6	12
			3	4	43			
			4	1	49			

Langkah 4 : Dalam langkah ini, ada dua langkah yaitu :

1. Hapus nilai n yang dilakukan oleh hasil modul tidak sesuai dengan persyaratan modulo rumus 2, 3 dan 4.
2. Hapus nilai pembagian modulo bernilai 0

Penjelasan bilangan kuadrat

Angka bebas persegi adalah bilangan bulat itu tidak dapat dibagi dengan kuadrat sempurna selain 1. itu adalah, faktorisasi utama memiliki tepat satu faktor untuk masing-masing utama. Sebagai contoh, 10 = 2*5 bebas kuadrat, tapi 18 = 2*3*3 adalah tidak persegi - nomor gratis, karena 18 dapat dibagi dengan 9 = 2.

Dapat dilihat pada tabel 3.2, nilai hasil dari 25, 9, 49. Tidak dapat dibagi lagi

a. 25 => dibagi dengan 25 yang merupakan kuadrat dari 5. Contoh → 25 : 5^2 = 1

b. 45 => dibagi dengan 45 yang merupakan kuadrat dari 3. Contoh → 9 : 3^2= 1

c. 49 => dibagi dengan 49 yang merupakan kuadrat dari 7. Contoh → 49 : 7^2 = 1

Tabel 3.2 : Persamaan Bilangan Prima

$4x^2 + y^2$ mod 4 = 1 or 5	$3x^2 + y^2$ mod 6 = 1	$3x^2 - y^2$ mod 12 = 11
5 mod 4 = 1	~~4 mod 6 = 4~~	~~2 mod 12 = 2~~
~~8 mod 4 = 0~~	7 mod 6 = 1	11 mod 12 = 11
13 mod 4 = 1	~~12 mod 6 = 0~~	~~8 mod 12 = 8~~
~~20 mod 4 = 0~~	19 mod 6 = 1	~~3 mod 12 = 3~~
29 mod 4 = 1	~~28 mod 6 = 4~~	~~26 mod 12 = 2~~
~~40 mod 4 = 0~~	~~39 mod 6 = 3~~	23 mod 12 = 11
17 mod 4 = 1	13 mod 6 = 1	~~18 mod 12 = 6~~
~~20 mod 4 = 0~~	~~16 mod 6 =4~~	11 mod 12 = 11
~~25~~	~~21 mod 6 = 3~~	~~2 mod 12 = 2~~
~~32 mod 4 = 0~~	~~28 mod 6 = 4~~	47 mod 12 = 11
41 mod 4 = 1	37 mod 6 = 1	~~44 mod 12 = 8~~
37 mod 4 = 1	~~48 mod 6 =0~~	~~39 mod 12 = 3~~
~~40 mod 4 = 0~~	~~28 mod 6 = 4~~	~~32 mod 12 = 8~~
~~45~~	31 mod 6 = 1	23 mod 12 = 11
	~~36 mod 6 = 0~~	~~12 mod 12 = 0~~
	43 mod 6 = 1	
	~~49~~	

Langkah 5 : Setelah langkah - 4, daftarkan nomor pilihan yang tersisa:

Tabel 3.3 : Persamaan Bilangan Prima

$4x^2 + y^2$ mod 4 = 1 or 5	$3x^2 + y^2$ mod 6 = 1	$3x^2 - y^2$ mod 12 = 11
5 mod 4 = 1	7 mod 6 = 1	11 mod 12 = 11
13 mod 4 = 1	19 mod 6 = 1	23 mod 12 = 11
29 mod 4 = 1	13 mod 6 = 1	11 mod 12 = 11
17 mod 4 = 1	37 mod 6 = 1	47 mod 12 = 11
41 mod 4 = 1	31 mod 6 = 1	23 mod 12 = 11
37 mod 4 = 1	43 mod 6 = 1	

Langkah 6 : Hapus nomor berulang dalam daftar nomor , dan kembali - buat daftar baru.

Tabel 3.4 : Persamaan Bilangan Prima

$4x^2 + y^2$ mod 4 = 1 or 5	$3x^2 + y^2$ mod 6 = 1	$3x^2 - y^2$ mod 12 = 11
5	7	11
13	19	23
29	31	47
17	43	
41		
37		

Susun bilangan prima yang diperoleh pada langkah ini dari bilangan terkecil hingga terbesar. Berikut adalah bilangan prima antara 1-50: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

3.1.9 *Algortima Blum-Blum Shub (BBS)*

Menurut Tomoyud “dkk” (2016), *blum blum shub* merupakan algoritma pembangkit bilangan yang cukup sederhana dan efektif. *Blum Blum Shub* diperkenalkan pada tahun 1986 oleh Lenore Blum, Manuel Blum, dan Michael *Shub Blum-Blum Shub (BBS)* merupakan suatu *pseudo random number generator* yang diajukan pada tahun 1986 oleh Lenore Blum, Manuel Blum dan Michael Shub.

Algoritma ini terkenal karena ke sederhanaannya dalam proses perhitungan namun tetap menghasilkan bilangan acak yang aman. Proses pembangkitan kunci dihasilkan melalui perhitungan :xn+1= (xn)2mod N, dimana dalam hal ini, nilai N=p.q. Kedua nilai prima, p dan q, harus kongruen dengan 3 (mod 4) (hal ini akan menjamin tiap quadratic residue memiliki satu akar kuadrat yang juga merupakan quadratic residue) dan gcd(φ(p-1), φ(q-1)) juga

harus kecil (hal ini membuat panjang siklus menjadi besar).Sebagai contoh, nilai p=947, q=523 sehingga nilai n=pq=495281, kemudian nilai s=164317, sehingga nilai X0=s2 mod n=328055.

Langkah 1 : Tentukan nilai bilaangan prima P dan bilangan prima Q contoh p = 7 q = 11

Langkah 2 : Hitung nilai n dengan menghitung n = p x q

contoh n = 7x11 N = 77

Langkah 3 : Pilih lagi sebuah bilangan acak s sebagai umpan bilangan yang dipilih harus memenuhi kriteria 2<s<n, s dan n *relative* prima.

Langkah 4 : $X_0 = s^2 \bmod n$

Contoh : $X_0 = 5^2 \bmod 77$

Langkah 5 : Hasilkan bilangan bit acak dengan cara

a. Hitung $X_i = X_i\text{-}1^2 \bmod n$

b. Hasilkan Z_i = bit-bit yang diambil dari X_i. Bit yang diambil bias merupakan LSB (*Least Significant Bit*) hanya satu bit atau banyak bit j bit (j tidak melebihi log2 n.

Contoh $X_0 = 5^2 \bmod 77 = 25 = 1$

$X_1 = 25^2 \bmod 77 = 9 = 1$

$X_2 = 9^2 \bmod 77 = 4 = 0$

$X_3 = 4^2 \bmod 77 = 16 = 0$

$X_4 = 16^2 \bmod 77 = 25 = 0$

$X_5 = 25^2 \bmod 77 = 9 = 1$

$X_6 = 9^2 \bmod 77 = 4 = 0$

$X_7 = 4^2 \bmod 77 = 16 = 0$

Bilangan bit dihasilkan= 11000100 = 176

3.1.10 *PHP (Personal Hypertext Preprocessor)*

Menurut Firman ‘dkk’ (2016), *PHP* adalah salah satu bahasa pemrograman *open source* yang sangat cocok atau dikhususkan. untuk pengembangan *web* dan dapat ditanamkan pada sebuah skrip *HTML*. Berdasarkan pendapat diatas, maka dapat disimpulkan bahwa *PHP* adalah bahasa pemograman yang digunakan untuk membuat aplikasi *web*.

3.1.11 *MySQL (My Structure Query Language)*

Menurut Raharjo (2015), *MySQL* adalah suatu *software* atau program yang bersifat *open source* yang digunakan untuk membuat sebuah *database* serta menjalankan fungsi pengolah data. Berdasarkan pendapat diatas, maka dapat disimpulkan bahwa *MySQL* adalah *software open source* untuk membuat, *database* dengan cepat kapasitas lebih memori besar.

3.2 Hasil Penelitian Terdahulu

Penelitian terdahulu menjadi acuan dalam melakukan penelitian, sehingga memperkaya teori yang digunakan dalam mengkaji penelitian yang dilakukan. Dari penelitian terdahulu, penulis tidak menemukan penelitian dengan judul yang sama. Namun penulis mengangkat beberapa penelitian terdahulu sebagai referensi memperkuat bahan kajian penelitian ini dapat dilihat pada tabel 3.5

Tabel 3.5. : Penelitian Terdahulu

No	Nama judul	Nama Peneliti	Tahun dan ISSN	Hasil penelitin
1	Aplikasi *enkripsi* data *file teks* dengan algoritma *RSA* (*Rivest Shamir Adleman*)	1. Hendri syaputra 2. Hendrik fry herdiyat moko	Seminar nasional teknologi informasi & komunikasi terapan 2012 (semantika 2012) semarang, 23 juni 2012 ISBN 979-26-0255-0	Aplikasi ini dapat mengenkripsi dan *dekripsi file teks* yang ber*form*at txt dan karakternya tidak lebih dari 1000 karakter, aplkasi yang di *enkripsi* berbentuk berbaris baris dan hasil *dekripsi* berbentuk satu baris.

No	Nama judul	Nama Peneliti	Tahun dan ISSN	Hasil penelitin
2	Modifikasi pembangkit kunci algoritma *RSA* dengan menerapkan algoritma *Blum Blum Shub*(*BBS*)	1. Chandra Frenki Sianturi	Building of Informatika Technology and Science (BITS) ISSN 2684-8910 (media cetak) ISSN 2685-3310 (media online)	Pada penelitian ini kombinasi dari algoritma *Blum Blum Shub* pada *RSA* dapat diterapkan sehingga dapat digunakan sebagai pembangkit kunci pada *RSA* untuk melakukan *enkripsi* dan *dekripsi file*
3.	The Comparison of Methods for Generating Prime Numbers between *The Sieve of Eratosthenes, Atkins, and Sundaran*	1. Muhammad Khoiruddin Harahap 2. Nurul Khairina	Jurnal Publikations & In *Form*atic Enginering Research ISSN : 2541-2019 ISSN : 2541 044X	*Algoritma Sieve of Eratosthenes*, Atkins dan *Sundaran* dapat menghasilkan bilangan prima yang besar dengan akurasi yang baik, saringan *Eratosthenes*, *Atkins* dan *Sundaran* menghasilkan bilangan prima yang besar dengan akurasi yang baik, *Eratosthenes* memiliki waktu yang lebih cepat untuk menghasilkan bilangan prima pada skala besar dari dua algoritma lainnya.

No	Nama judul	Nama Peneliti	Tahun dan ISSN	Hasil penelitin
4	*Digital Signature* untuk menjaga keaslian data dengan Algoritma *MD5* dan Algoritma *RSA*	1. Budi Khutasuhut 2. Syahril Efendi 3. Zakarias Situmorang	Jurnal nasional Informatika dan teknologi jaringan ISSN : 2540-7597 (print) ISSN : 2540-7600 (online)	Algoritma *MD5* dan *RSA*, kombinasi kedua algoritma tersebut dapat memberikan peningkatan keamanan pada keaslian data, algoritma *RSA* mencegah *digital signature* dari data yang ada, hanya pengirim yang memiliki privat *key* yang dapat membangkitkan *digital signature*.

Penelitian pertama yang ditulis oleh Hendra Syaputra dan Hendrik fry herdiyat moko dengan mengambil judul : **Aplikasi *Enkripsi* Data *File* Teks Dengan Algoritma *RSA* (*Rivest Shamir Adleman*)**". Pada penelitian tersebut *Form*at *file* yang akan di *enkripsi* menggunakan *Form*at txt, pada penelitian yang akan penulis lakukan *Form*at *file* yang akan di *enkripsi* menggunkan *Form*at *doc, excel, pdf, ppt, dan txt*. Adapun persamaan dan perbedaan penelitian ini dengan penelitian kami yaitu: melakukan *enkripsi file* menggunakan algoritma *RSA* dan perbedaan yang ada dalam penelitian

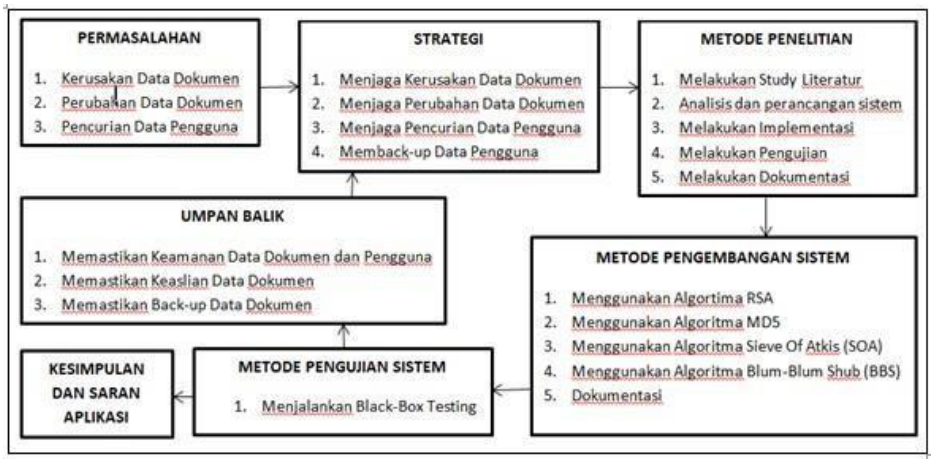
ini terletak pada jenis *form*at *file* yang akan dilakukan *enkripsi*.

Penelitian kedua yang ditulis oleh Chandra Frenki Sianturi dengan mengambil judul : "**Modifikasi Pembangkit Kunci algoritma *RSA* dengan menerapkan algoritma *Blum Blum Shub* (*BBS*)**" Pada penelitian tersebut algoritma *Blum Blum Shub* digunakan sebagai pembangkit kunci pada algoritma *RSA*, pada penelitian yang akan penulis lakukan algoritma *Blum Blum Shub* digunakan sebagai pembangkit bilangan acak pada algoritma *RSA*. Adapun persamaan dan perbedaan penelitian ini dengan penelitian kami yaitu: dalam kombinasi algoritma *Blum Blum Shub* dan algoritma *RSA* dan perbedaan yang ada dalam penelitian ini terletak pada penerapan algoritma *Blum Blum Shub* pada algoritma *RSA*.

Penelitian ketiga yang ditulis oleh Muhammad Khoruddin Harahap dan Nurul Khairina dengan mengambil judul "***The Comparison of Methods for Generating Prime Numbers between The Sieve of Eratosthenes, Atkins, and Sundaran***" Pada penelitian tersebut menjelaskan tentang perbandingan antara algoritma *Sieve of Eratosthenes*, Atkins dan *Sundaran* , pada penelitian yang akan penulis lakukan algoritma *Sieve Of Atkins* akan digunakan sebagai pembangkit bilangan prima. Adapun persamaan dan perbedaan penelitian ini dengan penelitian kami yaitu: algoritma yang digunakan dan perbedaan yang ada dalam penelitian ini terletak pada penerapan *algoritma Sieve Of Atkins* sebagai pembangkit bilangan prima pada algoritma *RSA*.

Penelitian keempat yang ditulis oleh Budi Khutasuhut, Syahril Effendi, dan Zakarias Situmorang dengan mengambil judul "***Digital Signature* untuk menjaga keaslian data dengan Algoritma *MD5* dan Algoritma *RSA***". Pada penelitian tersebut kombinasi algoritma *MD5* dan algoritma *RSA* digunakan untuk membuat *Digital Signature* untuk menjaga keaslian data. Adapun persamaan dan perbedaan penelitian ini dengan penelitian kami yaitu: dalam penggunaan algoritma *MD5* dan algoritma *RSA* sebagai *Digital Signature* dan perbedaan yang ada dalam penelitian ini terletak pada penerapan algoritma *MD5* dan algoritma *RSA* sebagai *Digital Signature* pada *enkripsi* dan *dekripsi file.*

3.3 Kerangka Pemikiran



Sumber: Peneliti Sendiri

Gambar 3.5 : Kerangka Pemikiran

Kerangka pemikiran diawali bagaimana menerapkan algoritma *RSA* dan *MD5* dengan algoritma *Sieve Of Atkins* (*SOA*) dan Algoritma *Blum-Blum Shub (BBS)* sebagai pembangkit bilangan prima dan bilangan acak pada metode *RSA*. Setelah melakukan *identifikasi* masalah peneliti menggunakan

sebuah metode penelitian, metodologi penelitian yang digunakan dalam penulisan skripsi ini adalah *studi literature*, *analisis* dan perancangan sistem, implementasi, pengujian, dokumenasi. Berikut pengujian oleh penulis terhadap aplikasi :

a. *Black box testing* digunakan untuk melakukan proses pada aplikasi untuk memastikan setiap proses yang berjalan dengan baik.

b. Sistem manual pada aplikasi yang buat dilakukan untuk memastikan *file* yang sudah di *enkripsi* dan *dekripsi.*

BAB IV

METODE PENELITIAN

4.1. Lokasi dan Waktu Penelitian

4.1.1. Waktu Penelitian

Penelitian ini dilakukan pada bulan September 2020 sampai dengan Januari 2021. Adapun jadwal penelitian dapat dilihat pada tabel 4.1

Tabel 4.1 : Waktu Penelitian

No	Kegiatan	September 2020				Oktober 2020				November 2020				Desember 2020				Januari 2021			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	*Analisis* kebutuhan perangkat *lunak*																				
2	Desain aplikasi																				
3	Pembuatan kode program																				
4	Pengujian aplikasi																				
5	Pendukung atau pememliharaan aplikasi (*Maintenance*)																				
6	Pembuatan laporan skripsi																				

4.2. Teknik Pengumpulan Data

4.2.1. *Study* Pustaka

Menurut Sugiyono (2012), studi pustaka adalah suatu metode pengumpulan data yang diambil dari perpustakaan atau instansi yang berupa karya ilmiah, jurnal, buku-buku serta dari *internet* yang berhubungan dengan penulisan ini tujuan untuk mendalami dan diperoleh keterangan yang lengkap dari penelitian.

4.2.2. *Study Literature*

Menurut Embun (2012), penelitian kepustakaan dan studi pustaka/riset pustaka meski bisa dikatakan mirip akan tetapi berbeda. Studi pustaka adalah istilah lain dari kajian pustaka, tinjauan pustaka, kajian teoritis, landasan teori, dan tinjauan teoritis. Yang dimaksud penelitian kepustakaan adalah penelitian yang dilakukan hanya berdasarkan atas karya tertulis, termasuk hasil penelitian baik yang telah maupun yang belum dipublikasikan. Studi literature yang dilakukan peneliti di dapat dari junal, artikel laporan penelitian, dan situs-situs di internet.

4.3. Alat dan Teknik Pengembangan Sistem

4.3.1. *Data Flow Diagram* (*DFD*)

Menurut Sukamto ‘dkk’ (2014:288), “*Data Flow Diagram* atau dalam bahasa Indonesia menjadi *Diagram* Alir Data (DAD) adalah refresentasi grafik yang menggambarkan aliran informasi dan trans*Form*asi informasi yang diaplikasikan sebagai data yang mengatur dari masukan (*Input*) dan keluaran (*Output*). *DFD* tidak sesuai untuk memodelkan sistem yang menggunakan pemograman berorientasi objek.”

Menurut Sukamto ‘dkk’ (2014:71), notasi-notasi *DFD* (Edward Yourdon dan Tom DeMarco) dilihat pada tabel 4.2

Tabel 4.2 Simbol-simbol *Data Flow Diagram*

No	Simbol	Nama	Keterangan
1		Proses Transformasi	Proses yang mengubah data dari input menjadi output
2		Sumber & Tujuan Data	Karyawan & organisasi yang mengirim data ke dan menerima data dari sistem.
3		Arus Data	Arus data yang masuk ke dalam dan keluar dari sebuah proses.
4		Penyimpanan Data	Penyimpanan Data

Sumber : Sukamto dan Shalahuddin (2014:71)

Menurut Sukamto dan Shalahuddin (2014:72), berikut ini adalah tahapan-tahapan perancangan menggunakan *DFD* :

a. Membuat *DFD Level* 0

Context Diagram DFD Level 0 menggambarkan sistem yang akan dibuat sebagai suatu entitas tunggal yang berinteraksi dengan orang maupun sistem lain. *DFD Level* 0 digunakan untuk menggambarkan interaksi antara sistem entitas luar.

b. Membuat *DFD Level* 1

DFD Level 1 digunakan untuk menggambarkan modul-modul yang ada dalam sistem yang aakan dikembangkan. *DFD Level* 1 merupakan hasil *breakdown DFD Level* 0 yang sebelumnya sudah dibuat.

c. Membuat *DFD Level* 2

Modul-modul pada *DFD Level* 1 dapat di *breakdown* menjadi *DFD Level* 2. Modul mana saja yang harus di *breakdown* lebih detail tergantung pada tingkat kedetilan modul tersebut. Apabila modul tersebut sudah cukup detail dan rinci maka modul tersebut sudah tidak perlu untuk di *breakdown* lagi. Untuk jumlah *DFD Level* 2 sama dengan jumlah modul pada *DFD Level* 1 yang di *breakdown*.

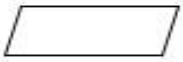
d. Membuat *DFD Level* 3

DFD Level 3, 4, 5 dan seterusnya merupakan *breakdown* dari modul pada *DFD Level* di atasnya. *Breakdown* pada *level* 3, 4 dan 5 dan seterusnya aturannya sama persis dengan *DFD Level* 1 atau *Level* 2.

4.3.2 *Entity Relationship Diagram* (*ERD*)

Menurut Sukamto ‘dkk’ (2014:50-289), “*Entitiy Relationship Diagram* (*ERD*) adalah pemodelan awal basis data yang akan dikembangkan berdasarkan teori himpunan dalam bidang matematika untuk pemodelan basis data relasional”. *ERD* memiliki beberapa aliran notasi seperti notasi Chen (dikembangkan oleh Peter Chen). Barker (dikembangkan oleh Richard Barker, Ian Palmer, Harry Ellis), notasi Crow’s Foot, dan beberapa notasi lain. Namun yang banyak digunakan adalah notasi dari Chen. Berikut adalah simbol-simbol yang digunakan pada *ERD* dengan notasi Chen dilihat pada tabel 4.3

Tabel 4.3 *Entity Relationship Diagram* (*ERD*)

Notasi	Keterangan
	Entitas, yaitu kumpulan dari objek yang dapat diidentifikasi secara unik.
	Relasi, yaitu hubungan yang terjadi antara satu atau lebih entitas. Jenis hubungan antara lain: satu ke satu, satu ke banyak, dan banyak ke banyak.
	Atribut, yaitu karakteristik dari entity atau relasi yang merupakan penjelasan detail tentang entitas.
	Garis, hubungan antara entity dengan atribut nya dan himpunan entitas dengan himpunan relasi.
	Input/output data, yaitu proses input/output data, parameter, informasi.

Sumber : Sukamto dan Shalahuddin (2014:50-289)

4.3.3 *Flowchart*

Menurut Indrajani (2015:36-38), "*Flowchart* adalah penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program." menjelaskan simbol-simbol dalam *Flowchart* dapat dilihat pada tabel 4.4

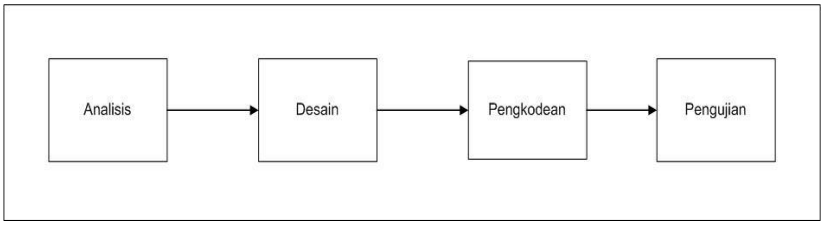
Tabel 4.4 *Flowchart Diagram*

Simbol	Kegunaan
	menghubungkan antara simbol yang satu dengan simbol yang lainnya.
	keluar/masuk prosedur atau proses dalam lembar/halaman yang lain.
	keluar/masuk proses dalam lembar/halaman yang sama.
	menunjukkan pengolahan yang dilakukan oleh komputer.
	menunjukkan pengolahan yang tidak dilakukan oleh komputer.
	kondisi yang akan menghasilkan beberapa kemungkinan jawaban/aksi.
	permulaan atau akhir dari suatu program.
	menunjukkan bahwa data di dalam simbol ini akan disimpan secara sementara.
	menunjukkan bahwa data di dalam simbol ini akan disimpan secara permanen.
	proses input dan output tanpa tergantung dengan jenis peralatannya.
	input berasal dari dokumen dalam bentuk kertas atau output dicetak ke kertas.

Sumber : Indrajani (2015:36)

4.3.4 Teknik Pengembangan Sitem

Menurut Rosa dan Shalahuddin (2013:28) Model *SDLC* air terjun (*waterfall*) sering juga disebut model sekuensial linier (*sequential linier*) atau alur hidup klasik (*classic life cycle*). Model air terjun menyediakan pendekatan alur hidup perangkat *lunak* secara *sekuensial* atau terurut dimulai dari *analisis*, desain pengkodean, pengujian, dan tahap pendukung (*support*), gambar model air terjun dapat dilihat pada gambar 4.1



Sumber : Rosa dan Shalahuddin (2013:29)

Gambar 4.1. Model *Waterfall* Rosa dan Shalahuddin

1. *Analisis* kebutuhan perangkat *lunak*

   Proses pengumpulan kebutuhan dilakukan secara intensif untuk menspesifikasikan kebutuhan perangkat *lunak* agar dapat dipahami perangkat *lunak* seperti apa yang dibutuhkan oleh *user*. *Spesifikasi* kebutuhan perangkat *lunak* pada tahap ini perlu didokumenasikan

2. Desain

   Desain perangkat *lunak* adalah proses multi langkah yang fokus pada desain pembuatan program perangkat *lunak* termasuk struktur data, arsitektur perangkat *lunak*, representasi antarmuka, dan prosedur pengodean. Tahap ini merealisasikan kebutuhan perangkat *lunak* dari tahap *analisis* kebutuhan ke representasi desain agar dapat diimplementasikan menjadi program pada tahap selanjutnya. Desain perangkat *lunak* yang dihasilkan pada tahap ini juga perlu di dokumentasikan.

3. Pembuatan kode progam

   Desain harus di realisasi ke dalam progam perangkat *lunak*. Hasil tahap ini adalah progam komputer sesuai dengan desain yang telah dibuat pada tahap desain.

4. Pengujian

   Pengujian fokus pada perangkat *lunak* secara dari segi lojik dan fungsional dan memastikan bahwa semua bagian sudah diuji. Hal ini dilakukan untuk meminimalisir kesalahan (*errors*) dan memastikan keluaran yang dihasilkan sesuai dengan yang diinginkan.

5. Pendukung (*support*) atau pemiliharaan (*Maintenance*)

   Tidak menutup kemungkinan sebuah perangkat *lunak* mengalami perubahan ketika sudah dikirim ke *user*. Perubahan bisa terjadi karena adanya kesalahan yang muncul dan tidak terdeteksi saat pengujian atau perangkat *lunak* harus beradaptasi dengan lingkungan baru. Tahap pendukung atau pemeliharaan dapat mengulangi proses pengembangan mulai dari *analisis spesifikasi* untuk perubahan perangkat *lunak* yang sudah ada, tapi tidak untuk membuat perangkat *lunak* baru.

4.5 Teknik Pengujian Sistem

4.5.1 Pengujian *Black Box*

Menurut M. Sidi mustaqbal ‘dkk’ (2015), *black box testing* berfokus pada *spesifikasi* fungsional dari perangkat *lunak. Tester* dapat mendefinisikan kumpulan kondisi *Input* dan melakukan pengujian pada *spesifikasi* fungsional program. *Black Box* Testing bukanlah solusi alternatif dari *White Box Testing* tapi lebih merupakan pelengkap untuk menguji hal-hal yang tidak dicakup oleh *White Box Testing*. *Black Box Testing* cenderung untuk menemukan hal-hal berikut:

a. Kesalahan antarmuka *(interface errors).*

b. Kesalahan pada struktur data dan akses basis data.

c. Kesalahan *perFormansi (perFormance errors).*

d. Kesalahan *inisialisasi* dan *terminasi*.

BAB V

HASIL DAN PEMBAHASAN

5.1. Hasil

Dalam pembuatan perancangan aplikasi keamanan data dokumen ini menggunakan metode *waterfall*, adapun tahapannya adalah sebagai berikut :

5.1.1. *Analisis*

5.1.1.1. Identifikasi Masalah

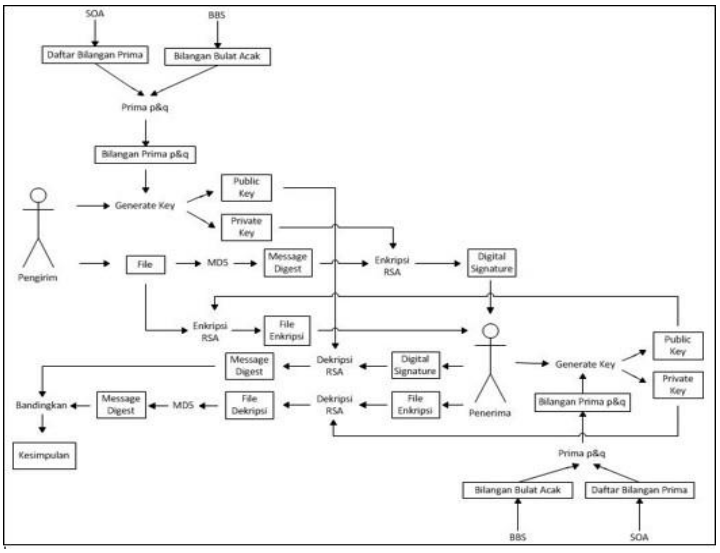
Identifikasi permasalahan yang terjadi pada rancangan aplikasi keamanan data dokumen dapat dilihat pada tabel 5.1

Tabel 5.1. Identifikasi Masalah

No	Masalah	Penyebab Masalah
1	Kerusakan Data	Pada saat pengiriman data dapat terjadi kesalahan penanda tanganan *file* atau pengesahan yang tidak cocok sehingga *file* tersebut tidak dapat ditampilkan
2	Perubahan Data	Pada saat pengiriman data dapat terjadi pembacaan data oleh orang lain ketika data sedang dikirim sehingga dapat terjadi perubahan data *file* aslinya.
3	Pencurian Data	Pada saat pengiriman data dapat terjadi pengambilan data oleh orang lain.

5.1.1.2. Alur Sistem Yang Diusulkan

Adapun alur sistem yang dapat dilihat pada gambar 5.1



Sumber : peneliti

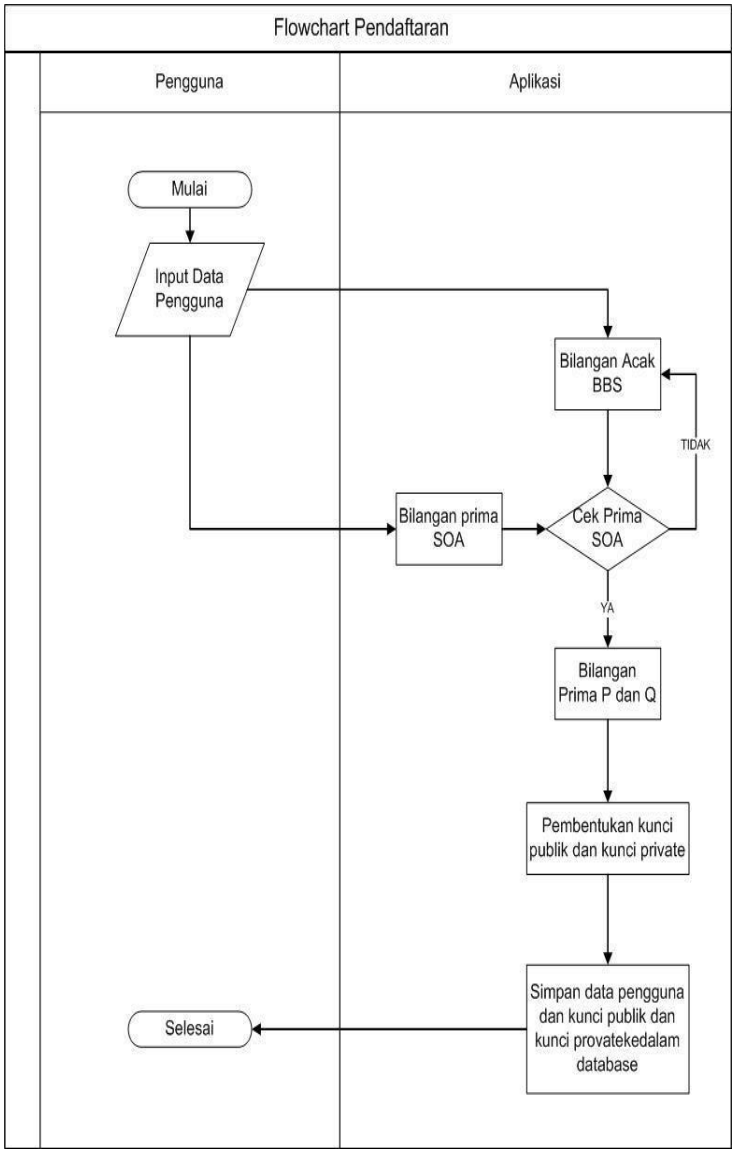
Gambar 5.1 *Flowchart* sistem yang diusulkan

Pada gambar 5.1 *Flowchart* sistem yang diusulkan terdapat 3 proses utama, yaitu proses pendaftaran, pengiriman *file* dan penerimaan *file.*

a. Pendaftaran

Pengguna melakukan *Input* data pada *Form* pendaftaran kemudian pada algoritma *Sieve Of Atkins* menampilkan deretan bilangan prima kemudian algoritma *Blum Blum Shub* melakukan pembangkitan bilangan acak yang masuk kategori pada deretan bilangan prima *Sieve Of Atkins* tersebut untuk mengambil nilai P dan Q untuk melakukan proses pembangkitan kunci publik dan kunci privat

setelah proses setelah proses tersebut selesai maka data tersebut disimpan ke dalam *database*.

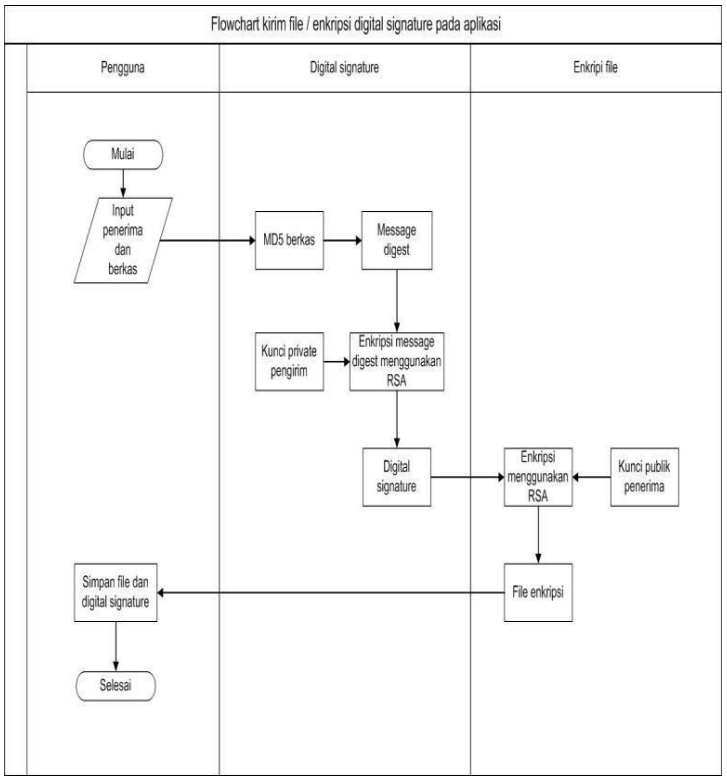


Sumber : peneliti

Gambar 5.2 *Flowchart* sistem pendaftaran pengguna

b. Pengiriman *file*

Sebelum pengguna melakukan pengiriman *file* pengguna diwajibkan untuk menanda tangani *file* tersebut terlebih dahulu fungsinya untuk memastikan pengesahan *file* yang dikirim tersebut kepada penerima. Setelah melakukan penanda tanganan pengesahan *file* pengguna melakukan *enkripsi* data bersamaan dengan tanda tangan tersebut fungsinya agar *file* tersebut sulit dibaca atau dirubah keaslian data dan pengirimnya.

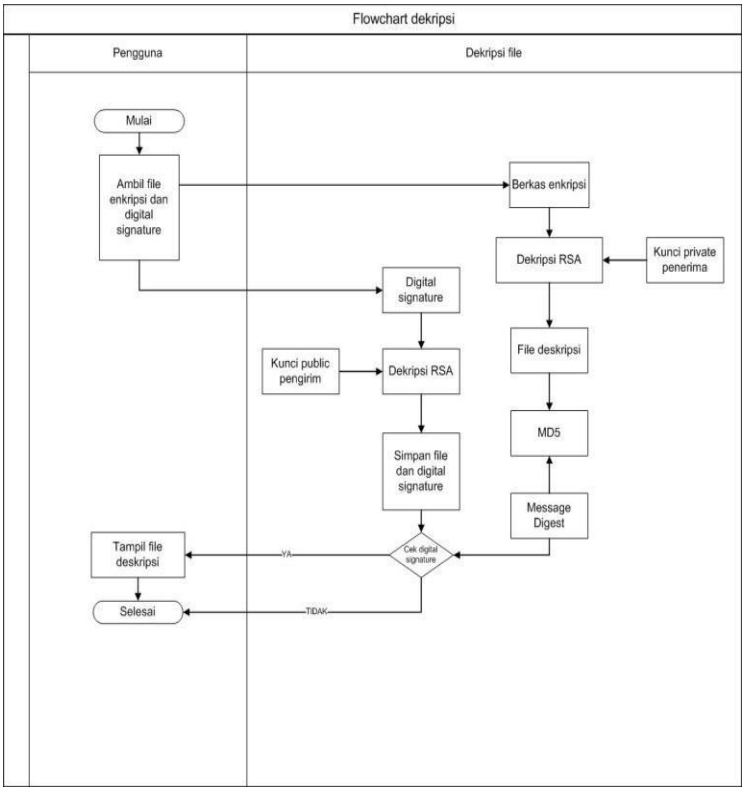


Sumber : peneliti

Gambar 5.3 *Flowchart* sistem pengiriman *file* pengguna

c. Penerimaan *file*

Selanjutnya *file* yang telah di kirim dan telah diterima oleh pengguna, penerima melakukan *dekripsi file* menggunakan kunci privat penerima, kemudian *digital signature* didekripsi menggunakan kunci publik pegirim, penerima akan memeriksa *digital signature* apakah sama dengan *digital signature* yang dibuat oleh pengirim, jika sama maka *file* tersebut dapat didekripsi dan diunduh oleh penerima.



Sumber : peneliti

Gambar 5.4 *Flowchart* sistem penerimaan *file* pengguna

5.1.1.3. *Analisis* Kebutuhan

a. *Analisis* Kebutuhan Fungsional

Kebutuhan fungsional adalah jenis kebutuhan yang berisi proses-proses apa saja yang diberikan sistem tersebut.

Kebutuhan pengguna dapat mengirim *file*, menerima *file*, membuat *digital signature* pada *file*, mengunduh dan menghapus *file*.

b. *Analisis* Kebutuhan Non Fungsional

Analisis Kebutuhan Non Fungsional dilakukan untuk mengetahui *spesifikasi* kebutuhan untuk sistem. *Spesifikasi* kebutuhan melibatkan *analisis* perangkat keras/*hardware*, *analisis* perangkat *lunak*/*software*, *analisis* pengguna/*user.*

Kebutuhan Perangkat Keras/*Hardware* yang diperlukan untuk mengimplementasikan aplikasi keamanan data dokumen adalah sebagai berikut :

1. Processor : Intel Core i3 @ 2.0 Ghz
2. Memory : 4 GB
3. Hard disk : 1000 GB

c. *Analisis* Kebutuhan Perangkat *Lunak*/*Software*

Kebutuhan perangkat *lunak*/*software* yang diperlukan untuk mendukung aplikasi yang dibangun adalah sebagai berikut :

1. *Google chrome* sebagai *browser*
2. *Xampp* dan *MySql*
3. *Virtual studio code*

d. *Analisis* Kebutuhan Pengguna/*User*

Kebutuhan fungsional pengguna dapat dilihat pada tabel 5.2

Tabel 5.2 Kebutuhan Fungsional Pengguna

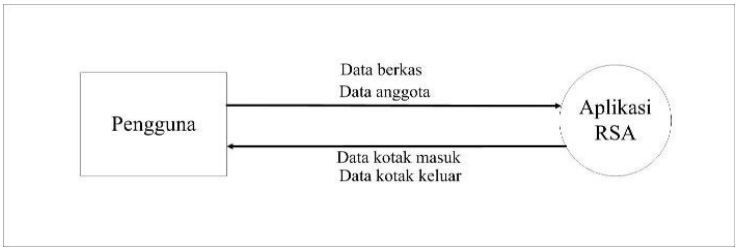
No	***Dekripsi***	**Aktifitas**	***User***
1	Kotak masuk	Lihat, unduh, hapus	Pengguna
2	Kotak keluar	Lihat, hapus	Pengguna
3	Kirim *file*	Upload, ulang, kirim	Pengguna
4	Simulasi	Upload, ulang, proses	Pengguna
5.	Ubah pass*word*	Ulang, kirim	Pengguna

5.1.2. Desain

5.1.2.1. Pemodelan Proses

a. *Data Flow Diagaram* (DFD) *level 0*

Diagaam *level* 0 digunakan untuk menggambarkan model proses sistem aplikasi keamanan data dokumen dilihat pada gambar 5.2



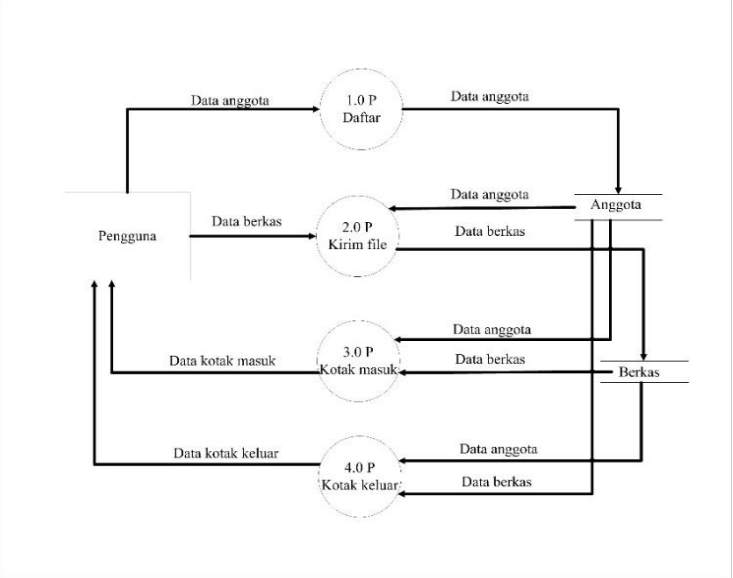
Sumber : peneliti

Gambar 5.5 *Diagram level* 0

1. Pengguna *Input* data pengguna dapat kunci publik dan kunci privat dan tanda tangan semua data tersebut disimpan ke dalam sistem.
2. Pengirim *Input* berkas *Input* penerima proses tanda tangan *digital* semua data tersebut diproses dan dihasilkan oleh sistem.
3. Penerima unduh berkas cek pengirim dan lihat berkas yang diterima semua data tersebut di proses dan ditampilkan oleh sistem.

b. *Data Flow Diagaram* (DFD) *level 1*

Diagaam *level* 0 digunakan untuk menggambarkan model proses sistem aplikasi keamanan data dokumen dilihat pada gambar 5.2



Sumber : peneliti

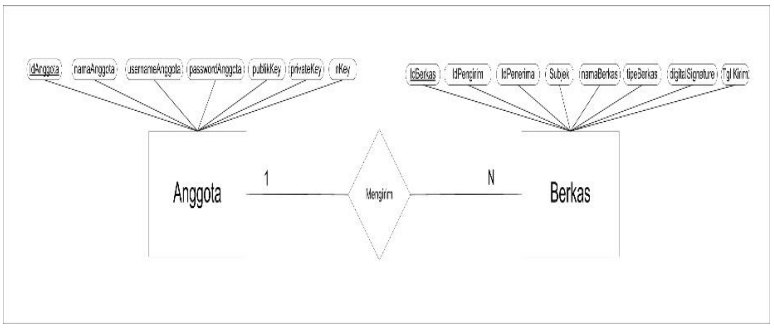
Gambar 5.6 *Diagram level* 1

1. Proses 1.0 P adalah proses dimana pengguna dapat melakukan pendaftaran dan disimpan kedalam *database*.
2. Proses 2.0 P adalah proses dimana pengguna melakukan pengiriman *file* serta meng*Input* data pengguna dan *file* berkas yang akan dikirim proses tersebut disimpan kedalam dalam kontak keluar dan *database*.

3. Proses 3.0 P adalah proses dimana pengguna dapat melihat *file*, tanda tangan, menghapus data serta mengunduh *file* yang diterima oleh pengirim yang telah masuk kedalam *database*.
4. Proses 4.0 P adalah proses dimana pengguna dapat melihat *file* serta tanda tangan dan menghapus data yang dikirim oleh pengguna yang telah masuk kedalam *database*.

5.1.2.2. ERD (Entity Relationship Diagram)

Pemodelan data adalah ERD (*Entity Relationship Diagram)*. Dapat dilihat pada gambar 5.8



Sumber : peneliti

Gambar 5.7 *ERD (Entity Relationship Diagram)*

5.1.2.3. Desain *Database*

Desain *database* adalah rancangan tabel tabel yang akan digunakan untuk kebutuhan pembangunan sistem, berikut ini adalah tabel yang akan digunakan dalam pembangunan sistem aplikasi keamanan data dokumen :

a. Tabel Pengguna

Fungsi : menyimpan data pengguna

Primary key : idAnggota

Foreign key : *username*

Tabel 5.3 Tabel Pengguna

No	Nama	Type	Panjang	Keterangan
1	IdAnggota	Int	11	*Primary key*
2	namaAnggota	varchar	50	
3	*User*name	varchar	15	*Foreign key*
4	PasswordAnggta	varchar	32	
5	Publik Key	Int	11	
6	Privat Key	Int	11	
7	NKey	Int	11	

b. Tabel Berkas

Fungsi : menyimpan data berkas

Primary key: idBerkas

Foreign key : idPengirim, idPenerima

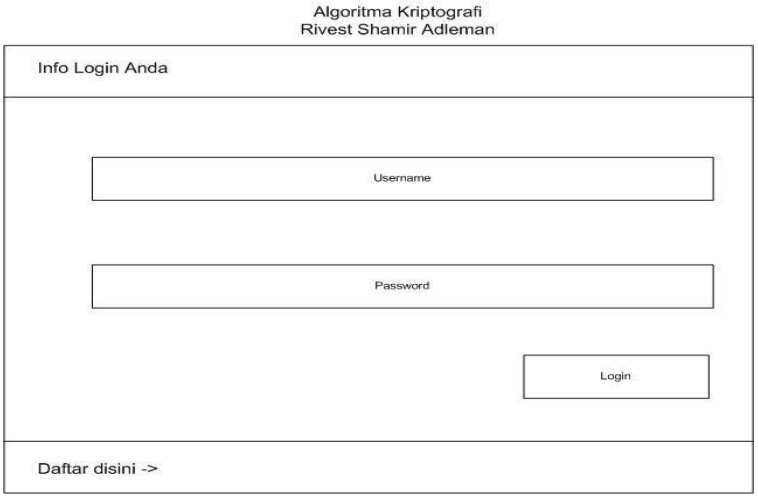
Tabel 5.4 Tabel Berkas

No	Nama	Type	Panjang	Keterangan
1	IdBerkas	Int	11	*Primary key*
2	IdPengirim	Int	11	*Foreign key*
3	idPenerima	Int	11	*Foreign key*
4	Subjek	Varchar	100	
5	namaBerkas	Varchar	32	
6	tipeBerkas	Varchar	10	
7	*digitalSignature*	Text	-	
8	Tgl Kirim	datetime	-	

5.1.2.4. Desain *Interface*

a. Desain *Form* login

Desain *Form* login ini untuk *security* akses pengguna pada *website*, serta menghindari tindakan yang tidak berkepentingan mengoperasinya. Jika *username* dan *password* yang dimasukan salah, maka kembali ke *Form* login lagi. Adapun desain *Form* login dapat dilihat pada gambar 5.8

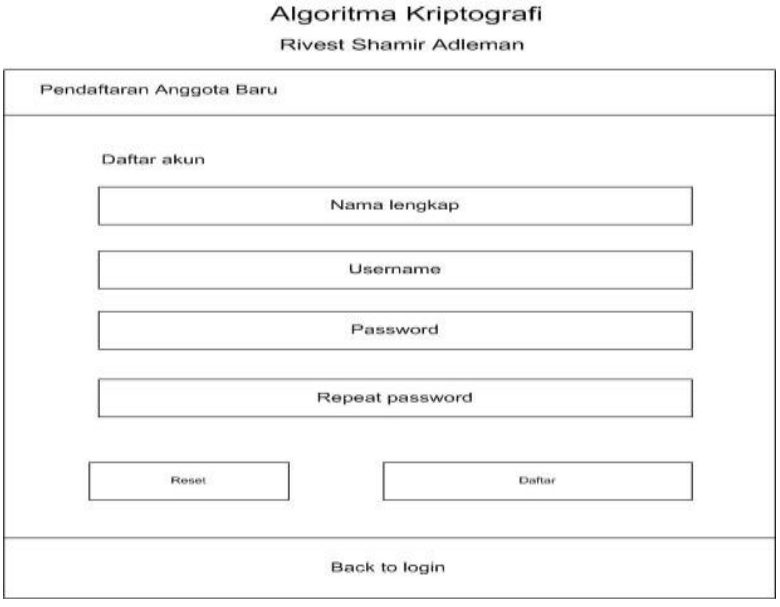


Sumber : peneleti

Gambar 5.8 Desain *Input Form* Login

b. Desain *Form* Pendaftaran

Form pendaftaran digunakan untuk menambahkan anggota, adapun desain *Form* pendaftaran dapat dilihat pada gambar 5.9

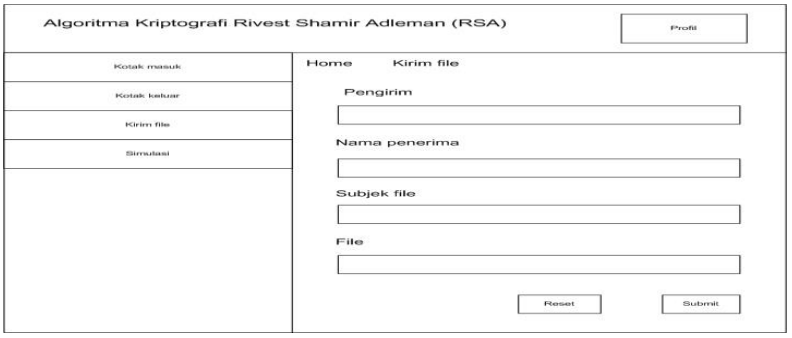


Sumber : peneliti

Gambar 5.9 Desain *Form* Pendaftaran

c. Desain *Input* Kirim *File*

Form kirim *file* digunakan untuk menambahkan data *file* yang dikirim. Adapun desain *Form* kirim *file* dapat dilihat pada gambar 5.10

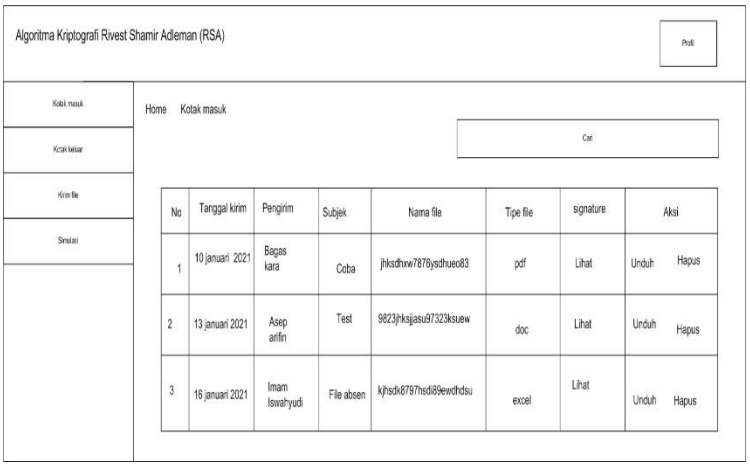


Sumber : peneliti

Gambar 5.10 Desain Kirim *File*

d. Desain *Form* Kotak Masuk

Desain *Form* kotak masuk digunakan untuk menampilkan data kotak masuk. Adapun desain *Form* kotak masuk dapat dilihat pada gambar 5.11

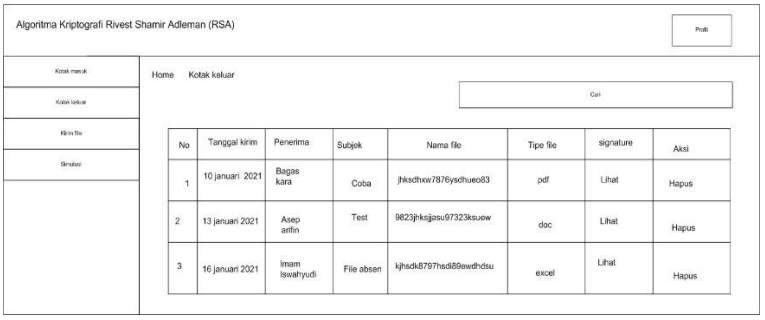


Sumber : peneliti

Gambar 5.11 Desain Kotak Masuk

e. Desain Kotak Keluar

Desain *Form* kotak keluar digunakan untuk menampilkan data kotak keluar. Adapun desain *Form* kotak keluar dapat dilihat pada gambar 5.12

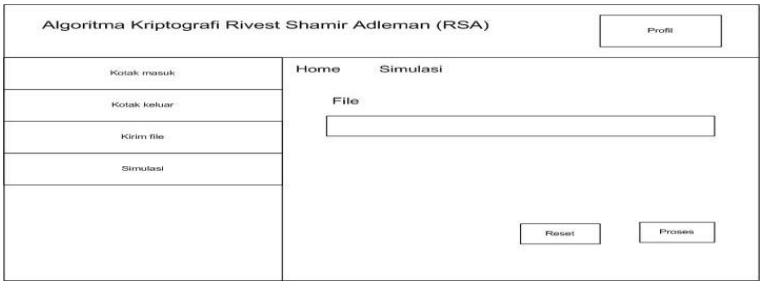


Sumber : peneliti

Gambar 5.12 Desain Kotak Keluar

f. Desain Simulasi

Desain simulasi digunakan untuk menampilkan hasil dari algoritma *Sieve Of Atkin, Blum-Blum Shub*, bilangan prima P dan Q, kunci publik, kunci privat, *digital signature*, hasil endkripsi, dan hasil *dekripsi*, Adapun desain *Form* simulasi dapat dilihat pada gambar 5.13



Sumber : peneliti

Gambar 5.13 Desain Halaman Simulasi

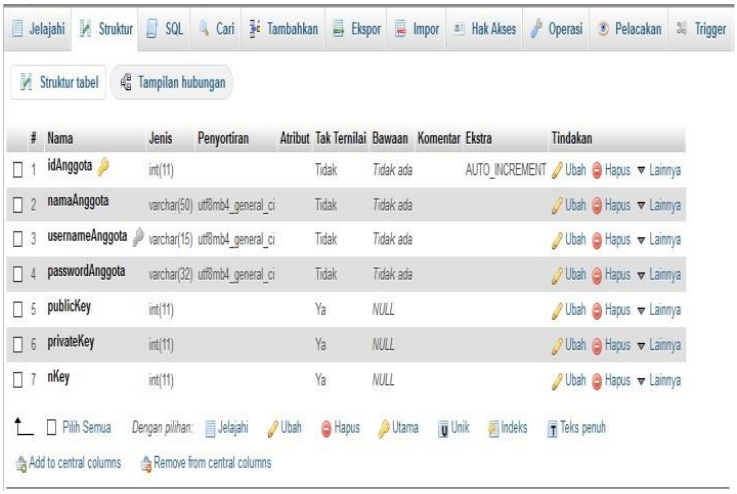
5.1.3. Implementasi/Pengkodean

5.1.3.1. Implementasi *Database*

Implementasi *database* adalah rancangan *database* yang terdiri *table-table* yang digunakan membangun sebuah aplikasi keamanan data dokumen. *Database* ini akan difungsikan sebagai tempat penyimpanan data. Berikut *table-table* yang tersimpan dalam sebuah *database* :

a. Implemntasi Tabel *Database* Pengguna

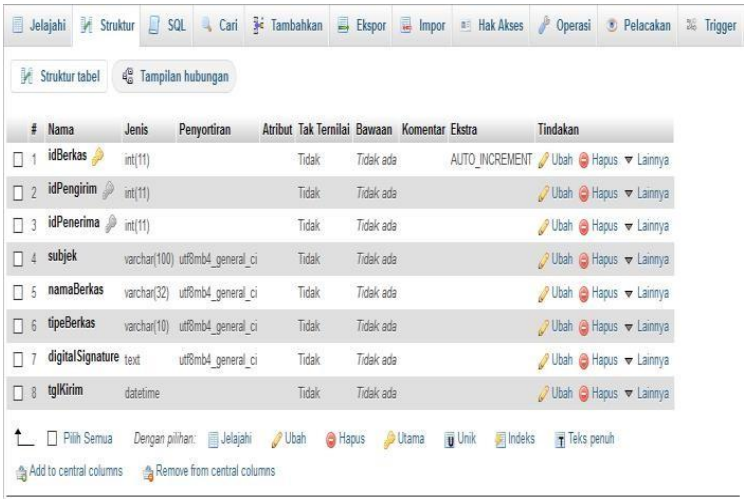
Tabel penguuna berfungsi untuk menyimpan data hak akses yang akan dizinkan melakukan pengolahan data pada aplikasi keamanan data. Tabel ini akan menyimpan data *username* dan *password* dari masing-masing *user* yang diberikan hak akses untuk masuk kedalam sistem.



Gambar 5.14 Implementasi *Database* Pengguna

b. Implentasi Tabel *Database File*

Tabel *file* berfungsi untuk menyimpan data *file* yang dikirim.

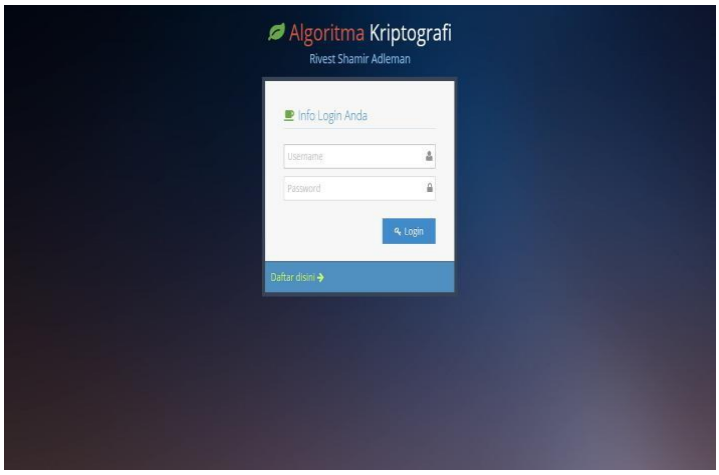


Gambar 5.15 Implementasi *Database File*

5.1.3.2. Implementasi *Interface*

a. Implementasi *Interface* Halaman Login

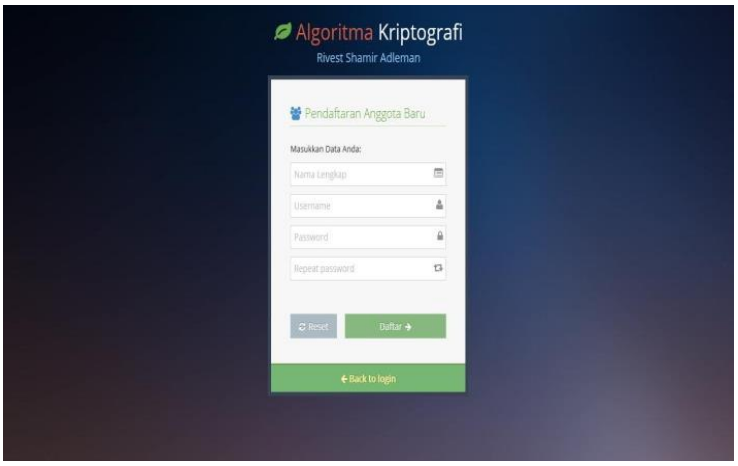
Halaman *Form* login untuk login ke aplikasi.



Gambar 5.16 Implementasi Interface Login

b. Implementasi *Interface Input* Anggota

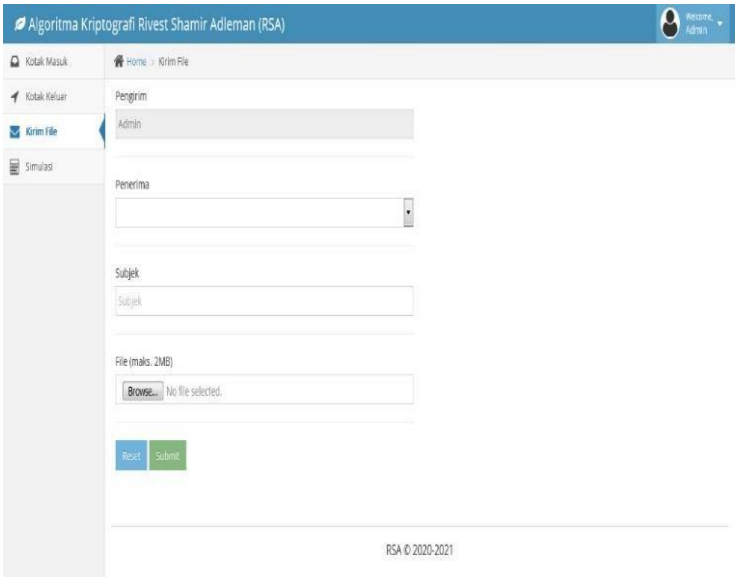
Halaman *Form Input* anggota digunakan untuk menambahkan data anggota kedalam tabel anggota.



Gambar 5.17 Implementasi *Form* Pendaftaran

c. Implementasi Kirim *File*

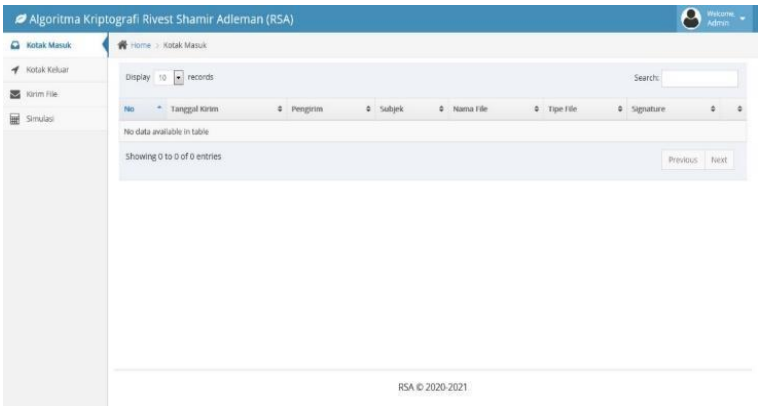
Halaman kirim *file* digunakan untuk mengirim sebuah *file* ke penerima.



Gambar 5.18 Implementasi *Form* Kirim *File*

d. Implementasi Kotak Masuk

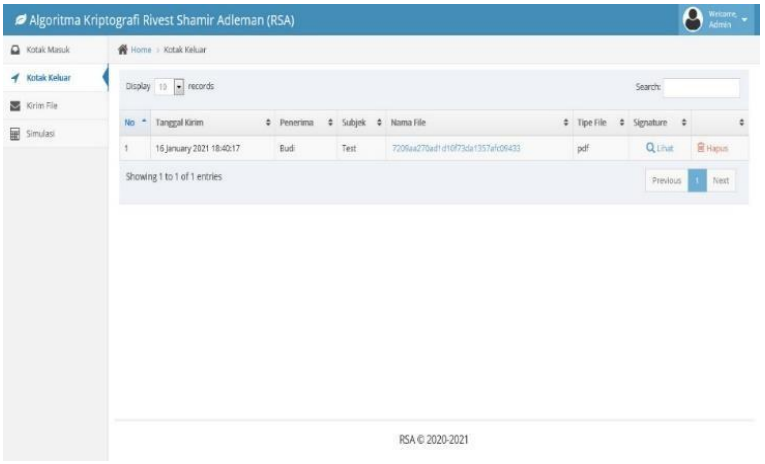
Implementasi kotak masuk digunakan untuk menampilkan data yang tersimpan didalam tabel berkas.



Gambar 5.19 Implementasi *Form* Kotak Masuk

e. Implementasi Kotak Keluar

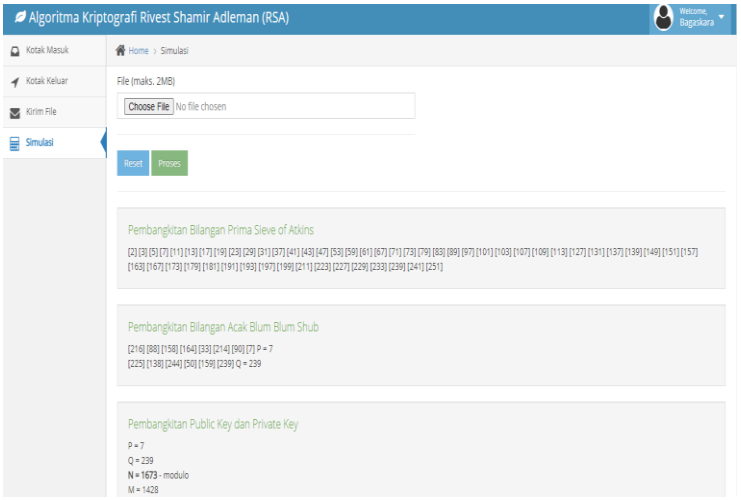
Implementasi data kotak keluar digunakan untuk menampilkan data *file* yang sudah dikirim yang tersimpan didalam tabel berkas.



Gambar 5.20 Implementasi *Form* Kotak Keluar

f. Implementasi Simulasi

Implementasi simulasi digunakan untuk mengetahui bilangan prima P dan bilangan prima Q, kunci publik, kunci privat, tanda tangan *digital*, hasil *enkripsi*, dan hasil *dekripsi*.



Gambar 5.21 Implementasi *Form* Simulasi

5.1.4. Pengujian

5.1.4.1. Pengujian *Black Box*

Pengujian sistem menggunakan teknik pengujian *Black Box testing*. Pengujian ini memperoleh kondisi *Input* seluruh keperluan fungsional program. Berikut hasil pengujianya :

Tabel 5.5 Tabel Pengujian *Black Box*

No	*Form* yang diuji	Keterangan	Harapan	Hasil
1	Pengujian pada *Form login*	Pada *Form login* pengguna harus memasukan *username* dan *password* kemudian klik tombol *login.*	Pengujian pada saat *login* "sukes" anda masuk ke menu utama. Jika salah maka kembali ke menu login dan kembali memasukan *username* dan *passwaord.*	**Berhasil**
2	Pengujian pada kontak masuk	Pada *Form* kontak masuk pengguna dapat melihat *file* yang telah dikirim oleh pengguna lain.	Pengujian pada saat pengguna melihat kontak masuk maka akan menampilkan *file* yang telah dikirim oleh pengguna lain.	**Berhasil**
3	Pengujian pada *Form* kontak keluar	Pada *Form* kontak keluar pengguna dapat melihat *file* yang telah dikirim.	Saat pengguna melihat *Form* kontak keluar dapat menampilkan *file* yang telah dikirim.	**Berhasil**

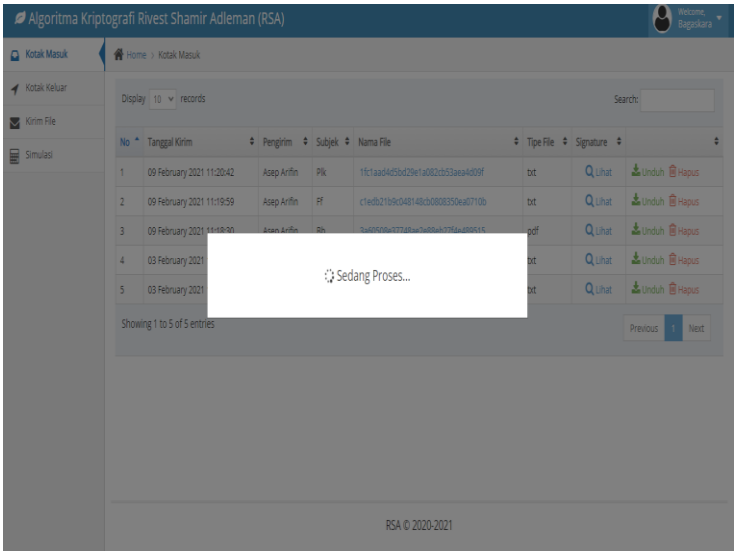
No	*Form* yang diuji	Keterangan	Harapan	Hasil
4	Pengujian pada *Form* kirim *file*	Pada saat pengguna mengirim sebuah *file* pengguna mengupload *file* dan membuat *digital signature.* Kemudian *file* tersebut di *enkripsi* dan dikirim ke pengguna lain.	Ketika *file* telah terdapat *digital signature* dan *file* tersebut ter*enkripsi* pengguna mengirim *file* tersebut berhasil terkirim.	**Berhasil**
5	Simulasi	Pada *Form* ini dilakukan simulasi untuk melihat bilangan prima p, bilangan prima q, nilai n, kunci publik, kunci privat, *digital signature*, hasil *enkripsi*, dan hasil *dekripsi*..	Pada *Form* ini dilakukan simulasi untuk melihat bilangan prima p, bilangan prima q, nilai n, kunci publik, kunci privat, *digital signature*, hasil *enkripsi*, dan hasil *dekripsi*.	**Berhasil**

No	*Form* yang diuji	Keterangan	Harapan	Hasil
6	Pengujian pada *Form* ganti pass*word*	Pada *Form* ini pengguna dapat mengganti pass*word* dengan memasukan pass*word* lama dan pass*word* yang baru.	Pengguna mengganti *password* dengan memasukan *password* lama dan *password* baru maka *password* dapat diganti.	**Berhasil**
7	Pengujian pada *Form* daftar anggota	Pada *Form* ini *user* mendaftarkan sebagai anggota dengan memasukan nama lengkap, *user*name, pass*word*, ulang pass*word*.	Pengguna mendaftar sebagai anggota dengan memasukan nama lengkap, *user*name,pass*word*, Maka akan terdaftar sebagai anggota..	**Berhasil**

5.1.4.2 Pengujian *Algoritma*

a. Kotak masuk / *dekripsi file*

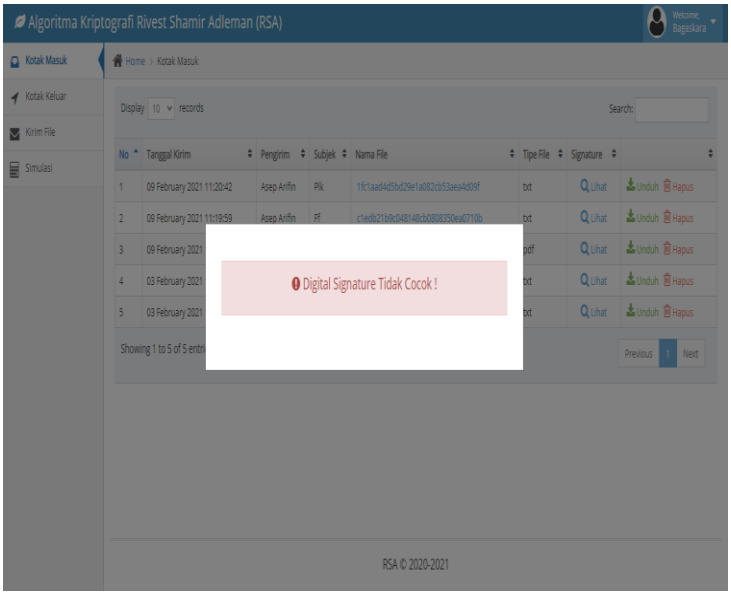
Pada kotak masuk *file* akan didekripsi menggunakan kunci privat penerima, jika *file* tidak mengalami perubahan data *file* maka *file* yang sudah didekripsi dapat di unduh, adapun tampilan *Form* uji coba kotak masuk dapat dilihat pada gambar 5.22



Gambar 5.22 Tampilan Uji Coba Kotak masuk

b. Perubahan data pada *file* yang telah dikirim

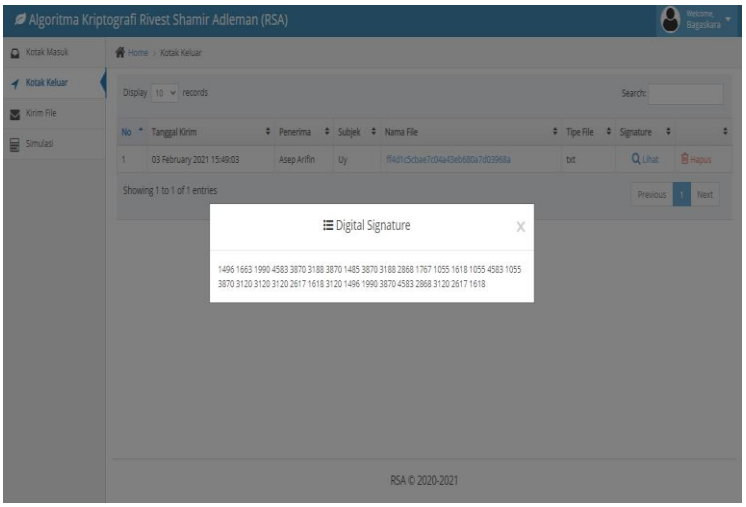
Pada kotak masuk penerima akan mendekripsi *file* menggunakan kunci privat, jika yang dikirim mengalami perubahan data maka *file* tersebut tidak dapat didekripsi dan diunduh, adapun tampilan *Form* perubahan data *file* dapat dilihat pada gambar 5.23



Gambar 5.23 Tampilan Perubahan Data *File*

c. Kotak keluar

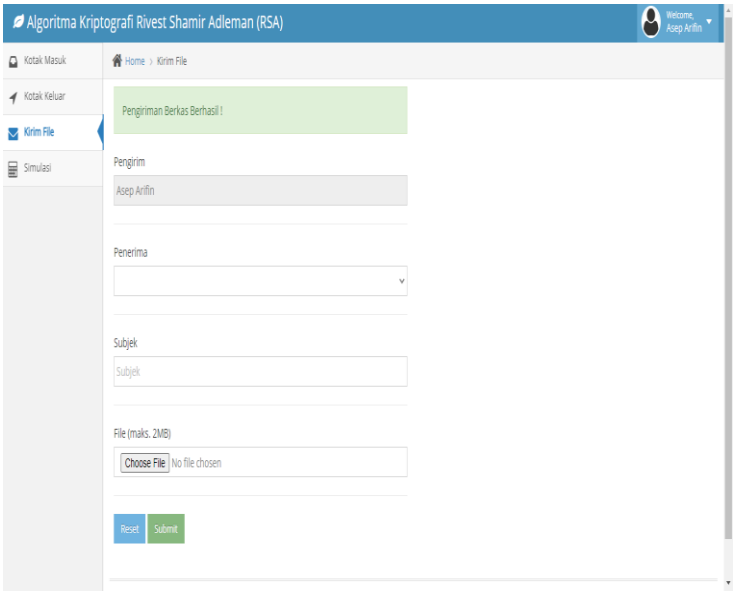
Pada kotak keluar pengguna dapat melihat *digital signature* dan *file* yang sudah dikirm, adapun tampilan *Form* kotak keluar dapat dilihat pada gambar 5.24



Gambar 5.24 Tampilan Kotak Keluar

d. Kirim *file*

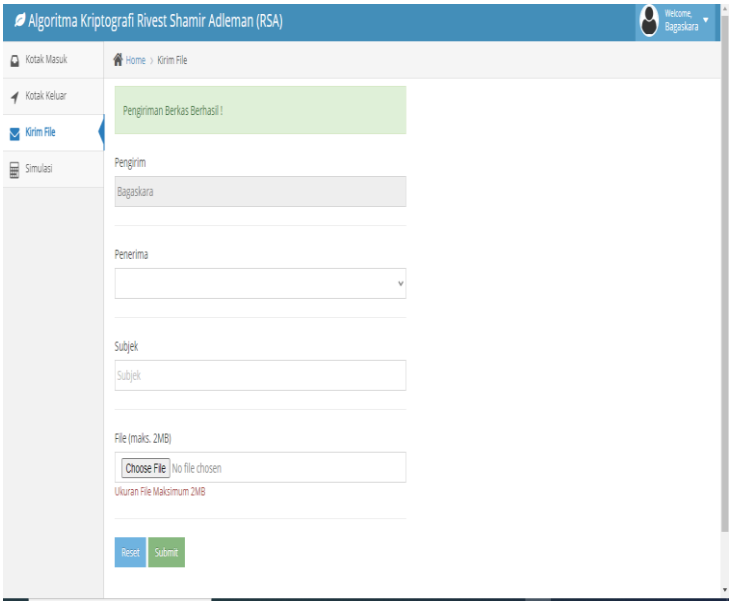
Pada kirim *file* pengguna mengirim sebuah *file* yang akan dienkripsi menggunakan kunci publik penerima, adapun tampilan *Form* kirim *file* dapat dilihat pada gambar 5.25



Gambar 5.25 Tampilan Kirim *File*

e. Kirim *file* diatas 2 MB

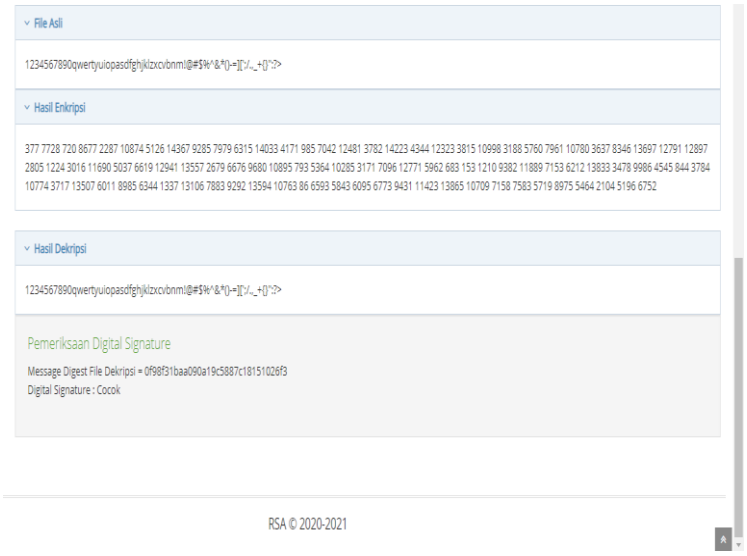
Pada halaman kirim *file*, pengguna dapat mengirim *file* yang ukuran filenya diatas 2 MB, *file* tersebut akan berhasil terkirim tetapi membutuhkan proses waktu yang cukup lama untuk enkrispi *file* tersebut, adapun tampilan *Form* kirim file dapat dilihat pada gambar 5.26



Gambar 5.26 Tampilan Uji Coba Kirim *File*

f. Hasil *Enkripsi* dan *Dekripsi File*

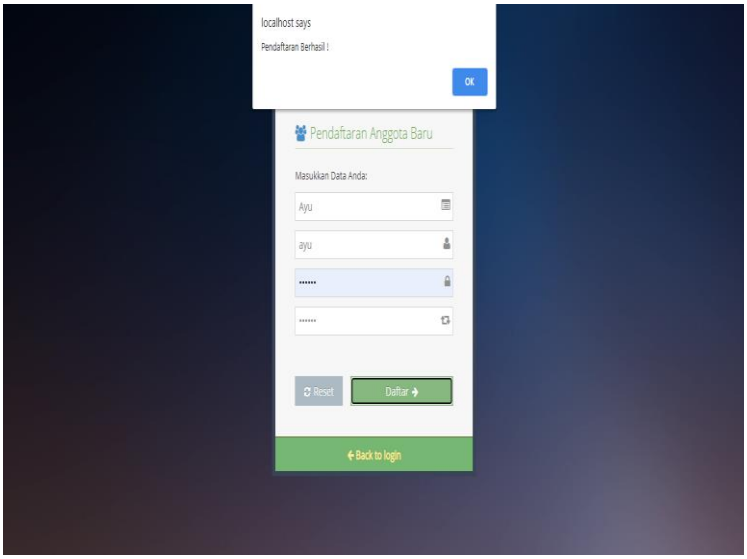
File yang sudah dienkripsi dan *dekripsi* dapat dilihat pada tampilan gambar 5.27



Gambar 5.27 Tampilan Hasil Enkrispi Dekrispi *File*

g. Halaman pendaftaran

Pada halaman pendaftaran ini pengguna akan mendaftar sebagai anggota, jika pendafataran sebagai anggota berhasil maka data diri, kunci publik dan privat yang didapat dari pembangkit kunci menggunakan *algoritma Sieve Of Atkins* dan *Blum Blum Shub* akan di simpan pada *database* tabel pengguna, adapun tampilan *Form* halaman pendaftaran dapat dilihat pada gambar 5.28



Gambar 5.28 Tampilan Halaman Pendaftaran

BAB VI

PENUTUP

6.1 Kesimpulan

Berdasarkan uraian yang telah dijelaskan dalam skripsi dengan menerapkan algoritma *RSA* dan *MD5* diperoleh kesimpulan sebagai berikut.

1. Penerapan algoritma *RSA* dan *MD5* pada keamanan data dokumen dapat diterapkan dengan baik.
2. Algoritma *RSA* dapat digunakan dalam menjaga data file yang asli karena sulitnya menetukan nilai N yang terbentuk dari dua bilangan prima sehingga tingkat kemanan algoritma Kriptografi *RSA* cukup tinggi.
3. Pembangkit bilangan prima dan bilangan acak mengguna *Algoritma Sieve Of Atkins (SOA)* dan *Algoritma Blum-Blum Shub (BBS)* pada *RSA* dapat diterapkan dengan baik.
4. Penggunaan algoritma *MD5* untuk *digital signature* dapat digunakan pada kemanan data dokumen.
5. Aplikasi perangakat lunak kemanan data yang dibuat hanya bisa untuk menjaga keaslian data file tidak dapat mengamankan data file dari serangan *cyber* atau pencurian data oleh orang lain.
6. Pada kunci publik bisa terjadi kesamaan dikarenakan nilai dari bilangan prima terlalu kecil sehingga diperlukan lebih banyak bilangan prima untuk mendapatkan kunci publik yang berbeda.

6.2 Saran

Berdasarkan uraian dan kesimpulan yang telah dijelas dalam skripsi mengenai penerpan algoritma *RSA* dan *MD5*, penulis memberikan beberapa saran sebagai berikut.

1. Perlu diperhatikan dalam membuat kunci pada pembangkit kunci *RSA* dengan menerapakan algoritma lain sebagai pembangkit kunci pada algoritma *RSA*.
2. Dapat menerapkan algoritma pembangkit bilangan selain *Algoritma Sieve Of Atkins (SOA)* dan *Algoritma Blum-Blum Shub (BBS)* pada *RSA*.
3. Pembuatan aplikasi kemanan data diharapkan dapat dibuat selain berbasis *web* misalnya berbasis *mobile*.
4. Diharapkan untuk pengembangan perangkat lunak aplikasi keamanan data dokumen dapat diterapkan untuk pengaman *cyber* atau pencurian data oleh orang lain melalui jaringan internet.
5. Didalam membangkitkan kunci pada algoritma *RSA* diperlukan limit banyaknya bilangan prima sehingga dalam pembentukan kunci publik dan kunci privat tidak terjadi kesamaan kunci.

DAFTAR PUSTAKA

Ardelia Nidya Agustina, Aryanti, Nasron. (2017). *Pengamanan Dokumen Menggunakan Metode RSA (Rivest Shamir Adleman) Berbasis Web*.

Arif Prayitno, Nurdin Nurdin. (2017). *Analisa dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Chiper Transposition*. Vol 3. No 1. (2017).

Astriab Firman, Hans F. Wowor, XaVerius Najoan. (2016). *Sistem Informasi Perpustakaan Online Berbasis Web.* Jurnal Teknik dan Komputer. Vol. 5. No. 2. Januari-Maret, ISSN 2301-8402.(2016).

A. S., Rosa dan Shalahuddin, M. (2013). *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Informatika. Hlm. 26, 30-34, 38-39, 117-118. (2013).

Basri. (2016). *Kriptografi Simetris dan Asimetris Dalam Perspektif Keamanan Data dan Kompleksitas Komputer*. Jurnal Ilmiah Komputer. Vol. 2. No. 2. (2016).

Budi Khutasuhut, Syahril Efendi, Zakarias Situmorang. (2019). *Digital Signature untuk Keaslian Data dengan Algoritma MD5 dan Algoritma RSA*. (2019). Jurnal Nasional Informatika dan Teknologi JaringaN. ISSN 2540-7600. (2019)

Chandra Franki Sianturi. (2020). *Modifikasi pembangkit kunci algoritma RSA dengan menerapkan algoritma Blum Blum Shub(BBS).* Building of Informatika Technology and Science (BITS) ISSN 2684-8910 (media cetak) ISSN 2685-3310 (media online). (2020).

Egi Cahyo Prabowo. (2017). *Penerapan Digital Signature dan Kriptografi pada Otentikasi Sertifikat Tanah Digital.* Jurnal Vol. 6. No. 2. Oktober (2017).

Embun, B. (2012). *Banjir Embun. Retrieved from Penelitian Kepustakaan:http://banjirembun.blogspot.co.id/2012/04/penelitian-kepustakaan.html.* (2012).

Hendri syaputra, Hendrik Fry Herdiyat Moko. (2012). *Aplikasi enkripsi data file teks dengan algoritma RSA (Rivest Shamir Adleman).* Jurnal Teknologi Informasi dan Informasi Terapan (2012).

Indrajani. (2015). *Database Design* (*Case Study All in One*). Jakarta: PT Elex Media Komputindo. (2015).

Junaidy B. Sanger. (2015). *Desain dan Implementasi Mekanisme Tanda Tangan Digital Dalam Pertukaran Data Dengan Hash MD5 dan Enkripsi/Dekripsi Menggunakan Algoritma RSA.* Jurnal Lasallian Vol. 12 No. 2 September (2015).

Kurniawan, S. T., Dedih, & Supriyadi. (2017*). Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks*

Berbasis Android. Jurnal Online Informatika, 102-109, ISSN : 2527-1682, Vol.2 No. 2.

Kardi Yusuf. (2020). *Penerapan Algoritma MD5 Sebagai Pengaman Akun pada Aplikasi Web Emusrenbang* Kota Binjai. Jurnal Vol. 4. No. 1. Januari (2020).

Muhammad Khoiruddin Harahap. (2019). *The Comparison Of Methods For Generating Prime Number Between The Sieve Of Erotosthenes, Atkin, and Sundaran.* Jurnal E-ISSN : 2541-2019 P-ISSN : 2541-044X. (2010).

Mustaqbal, Sidi, M., Firdaus, R., & Rahmadi, H. (2015). *Pengujian Aplikasi Menggunakan Black Box Testing Boundary Value Analysis (Studi Kasus: Aplikasi Prediksi Kelulusan SNMPTN)*. Jurnal Ilmiah Teknologi Informasi Terapan 1 (3), 31-36. (2015).

Rizal, Ansar, Suharto. (2011). *Implementasi Algoritma RC4 untuk Keamanan Login Pada Sistem Pembayaran Uang Sekolah*. Dielektrika, ISSN 2086-9487 Vol. 2 No. 2.

Rosyanti Harahap. (2010). *Sistem Pengamanan Data Teks Menggunakan Algoritma Message Disgest -5.* Jurnal (2010).

Raharjo, Budi. (2015). *Belajar Otodidak MySql. Bandung: Informatika.*(2015).

Sugiyono. (2012). *Metode Penelitian Kuantitatif Kualitatif dan R&B. Bandung: Alfabeta.* (2012).

Sukamto,R.A.,dan Shalahudin, M. (2011). *Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur Dan Berorientasi Objek)*. Bandung Modula Bandung. (2011).

Tomoyud Sintosaro Waruwu. (2016). *Kombinasi Algoritma One Time Pad Chiper dan Algoritma Blum Blum Shub Dalam Pengaman File.* Jurnal Mahasa Informasi Vol. 1. No. 1 (2016)