DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

Halaman

ABSTRAK

TANTO RAMADHAN

PERANCANGAN SISTEM KEAMANAN INFORMASI DATA MENGGUNAKAN METODE RSA (ron rivest adi shamir dan adleman)

2019

Kriptografi merupakan salah satu metode mengamankan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data serta keaslian pengirim. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum seperti LAN atau Internet. Kriptografi biasanya dalam bentuk Enkripsi dan Deskripsi. Untuk menyembunyikan tulisan, biasanya mengguakan algoritma. Algoritma yang dipakai dalam aplikasi ini adalah Algoritma RSA. Dalam hal ini, penulis berkeinginan mengangkat topik enkripsi dan deskripsi menjadi sebuah penulisan ilmiah skripsi dengan menggunakan visual studio yang berkembang saat ini. Diharapkan dengan adanya aplikasi ini, mahasiswa serta dosen dapat melakukan uji coba Enkripsi menggunakan algoritma RSA.

Kata Kunci: Kriptografi, RSA.

PERANCANGAN SISTEM KEAMANAN INFORMASI DATA MENGGUNAKAN METODE RSA (Ron Rivest, Adi Shamir)

Disusun serta Diajukan Untuk Memenuhi Persyaratan Ujian Akhir
Memperoleh Gelar Sarjana Pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi Medan

SKRIPSI

OLEH

NAMA : TANTO RAMADHAN
N.P.M : 1414370412
PROGRAM STUDI : SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

PERANCANGAN SISTEM KEAMANAN INFORMASI DATA MENGGUNAKAN METODE RSA

DISUSUN OLEH

NAMA : TANTO RAMADHAN
N.P.M : 1414370412
PROGRAM STUDI : SISTEM KOMPUTER

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 11 November 2019 :

Dosen Pembimbing I	Dosen Pembimbing II
Andysah Putera S S.Kom., M.Kom ,Ph.D	Dr. Muhammad Iqbal S.Kom., M.Kom

Mengetahui,

Dekan Fakultas Sains dan Teknologi	Ketua Program Studi
Sri Shindi Indira, S.T., M.S.C	Eko Hariyanto, S.Kom., M.Kom

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Tanto Ramadhan
NPM	: 1414370412
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Keamanan
Judul Skripsi	: Perancangan Sistem Keamanan Data Menggunakan Metode RSA (Ron Rivest, Adi Shamir)

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat
2. Sayat tidak akan menuntut perbaikan nilai indeks Prestasi Kumulatif (IPK) setelah ujian Sidang Meja Hijau
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga, dan saya tidak akan menuntut akibat publikasi tersebut

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih

Medan, 20 November 2019

Yang membuat pernyataan

Tanto Ramadhan

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

Saya yang bertanda tangan di bawah ini :

Nama Lengkap	: tanto ramadhan
Tempat/Tgl. Lahir	: medan 16-02-1996 / 16 Desember 1996
Nomor Pokok Mahasiswa	: 1414370412
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 141 SKS, IPK 3,11
Nomor Hp	: 087867368957
Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	Perancangan Sistem Keamanan Informasi Data menggunakan Metode RSA (Ron Rivest, Adi Shamir)

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

Coret Yang Tidak Perlu

Rektor I,

(Ir. Bhakti Alamsyah, M.T., Ph.D.)

Medan, 04 Oktober 2019
Pemohon,

(Tanto Ramadhan)

Tanggal : .....
Disahkan oleh :
Dekan

(Sri Shindi Indira, S.T., M.Sc.)

Tanggal : .....
Disetujui oleh :
Dosen Pembimbing I :

(Andysah Putera Utama Siahaan, S.Kom., M.Kom., Ph.D.)

Tanggal : .....
Disetujui oleh:
Ka. Prodi Sistem Komputer

(Eko Hariyanto, S.Kom., M.Kom)

Tanggal : .....
Disetujui oleh:
Dosen Pembimbing II:

(Dr Muhammad Iqbal, S.Kom., M.Kom.)

No. Dokumen: FM-UPBM-18-02	Revisi: 0	Tgl. Eff: 22 Oktober 2018

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas	: Universitas Pembangunan Panca Budi
Fakultas	: SAINS & TEKNOLOGI
Dosen Pembimbing I	: Andysah Putera Utama Siahaan, SKom., M.Kom
Dosen Pembimbing II	: Muhammad Iqbal, SKom., M.Kom
Nama Mahasiswa	: TANTO RAMADHAN
Jurusan/Program Studi	: Sistem Komputer
Nomor Pokok Mahasiswa	: 1414370412
Penjang Pendidikan	:
Judul Tugas Akhir/Skripsi	: Perancangan Sistem Keamanan Informasi Data Menggunakan Metode RSA

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
10/2	Revisi Bab I		
20/2	Revisi Bab II		
25/2	Revisi Bab II, III		
4/3	Revisi Bab IV		
13/3	Acc Seminar		
16/10	Acc Sidang		
11/11	Acc Jilid		

Medan, 23 Januari 2019
Diketahui/Disetujui oleh
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

Coret yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI

FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

---

iversitas	: Universitas Pembangunan Panca Budi
kultas	: SAINS & TEKNOLOGI
sen Pembimbing I	: Andysah Putera Utama Siahaan, SKom . M.Kom.
sen Pembimbing II	: Muhammad Iqbal , Skom.M.kom
ma Mahasiswa	: TANTO RAMADHAN
rusan/Program Studi	: Sistem Komputer
mor Pokok Mahasiswa	: 1414370412
njang Pendidikan	:
dul Tugas Akhir/Skripsi	: Perancang sistem keamanan informasi Data menggunakan Metode RSA

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
27/7	Acc Seminar		
3/7	Acc Bab I		
2/7	Acc Bab II		
9/7	Acc		
5/8	Acc Bab III		
8/8	Acc Bab IV & V		
21/8	Acc Seminar		
6/9	Acc		
11	Acc		

Medan, 22 Juli 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

yang untuk peru

Telah Diperiksa oleh LPMU
dengan Plagiarisme.....59.....%
31 OKTOBER 2019
AN Ka. LPMU
Cahyo Prayogo, SE,MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 21 Oktober 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima berkas persyaratan dapat di proses
Medan, 31/10/2019
Ka. BPAA
an.
TAGUH WAHYONO, SEI, MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: TANTO RAMADHAN
Tempat/Tgl. Lahir	: MEDAN / 16 DESEMBER 1996
Nama Orang Tua	: ASNAN
N. P. M	: 1414370412
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 087867368957
Alamat	: JL. ISTIQOMAH GG. RUKUN

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Perancangan Sistem Keamanan Informasi Data menggunakan Metode RSA (Ron Rivest, Adi Shamir)**, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	~~250.000~~ ~~400.000~~
2.	[170] Administrasi Wisuda	: Rp.	1,500,000
3.	[202] Bebas Pustaka	: Pp.	100.000
4.	[221] Bebas LAB	: Rp.	
Total Biaya		: Rp.	~~2,100,000~~ 1.855.000
5. Uang Kuliah 50% dr Thn A			3.250.000
			5.105.000

Ukuran Toga : L

Diketahui/Disetujui oleh :
Sri Shindi Indira, S.T.,M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya
TANTO RAMADHAN
1414370412

Catatan :

- 1.Surat permohonan ini sah dan berlaku bila :
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2.Dibuat Rangkap 3 (tiga), untuk : Fakultas - untuk BPAA (asli) - Mhs.ybs.

UKM CENTER PANCA BUDI
31/10-19

TANDA BEBAS PUSTAKA
No. 923/PERP/BP/2019
Tidak ada sangkut paut dengan Perpustakaan
Medan, 30 OCT 2019
UNIVERSITAS PEMBANGUNAN PANCA BUDI UNPAB INDONESIA UPT. PERPUSTAKAAN
an.
SALNIA S.IP

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571
Medan - 20122

KARTU BEBAS PRAKTIKUM

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama	:	TANTO RAMADHAN
N.P.M.	:	1414370012
Tingkat/Semester	:	Akhir
Fakultas	:	SAINS & TEKNOLOGI
Jurusan/Prodi	:	Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.

Medan, 21 Oktober 2019
Ka. Laboratorium

Fachrid Wadly, S.Kom

Plagiarism Detector v. 1092 - Originality Report:

Analyzed document: 30/10/2019 17:33:01

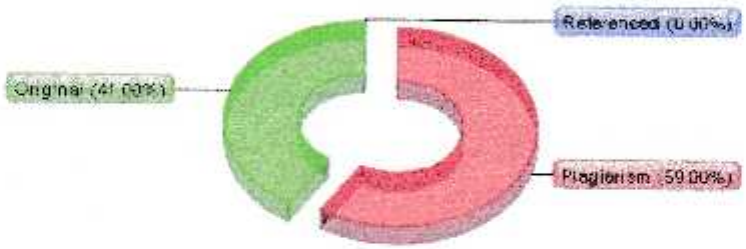
"TANTO RAMADHAN_1414370412_SISTEM KOMPUTER.docx"

Licensed to: **Universitas Pembangunan Panca Budi_License4**

UNIVERSITAS PEMBANGUNAN PANCA BUDI

LEMBAGA PENJAMIN MUTU UNIVERSITAS UNPAB UNIVERSITAS PEMBANGUNAN PANCA BUDI

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 23	wrds: 2458	https://pastebin.com/FNPwTtbP
% 12	wrds: 1257	http://archive.org/stream/Binary_Tutorial_/Binary_Tutorial_djvu.txt
% 12	wrds: 1249	https://tony-h.blogspot.com/2010

[Show other Sources:]

Processed resources details:

308 - Ok / 43 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
Wiki Detected!	[not detected]	[not detected]	[not detected]

BAB I

PENDAHULUAN

1.1 Latar Belakang

Database menempati posisi penting dalam masyarakat berbasis informasi dan pengetahuan. Dapat dikatakan bahwa database merupakan pokok penunjang perkembangan teknologi informasi, serta merupakan kerangka utama beroperasinya sistem berbasis komputer. Sangat sulit dipisahkan operasi sistem berbasis komputer dan database. Dapat dikatakan keberadaan sistem berbasis komputer menandakan keberadaan database.

Suatu sistem penyediaan informasi bagi khalayak ramai atau yang lazim disebut dengan website, biasanya dibangun oleh database yang akan membuat website tersebut lebih dinamis dan interaktif, sehingga akan lebih menarik untuk dinikmati oleh user yang menggunakannya. Sebuah website dinamis adalah website yang secara berkala, informasi di dalamnya berubah, atau website ini bisa berhubungan dengan user dengan berbagai macam cara atau metode (HTTP cookies atau variabel database, sejarah kunjungan, variabel sesi dan lain-lain) bisa juga dengan cara interaksi langsung menggunakan form dan pergerakan mouse. Salah satu media komunikasi di dalam website adalah form, dimana form ini digunakan oleh user untuk berinteraksi dengan server. Pada zaman teknologi informasi sekarang ini, dapat dipublikasikan melalui internet dengan media

website. Akan tetapi, masih ada satu situs yang hanya memberikan hak akses tertentu kepada seseorang untuk dapat menikmati informasi yang terdapat di website tersebut

Informasi saat ini sudah menjadi komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa sudah berada di sebuah "information based society". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi.

Sangat pentingnya sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu saja. Jatuhnya informasi kepada pihak lain yang tidak diinginkan (misalnya pihak lawan bisnis) dapat merugikan bagi pihak yang memegang informasi. Untuk itu keamanan dari sistem informasi yang digunakan haruslah terjamin dalam batas yang dapat diterima.

Seperti yang dikatakan Munir, bahwa masalah keamanan (security) pada komputer menjadi isu penting pada era teknologi sekarang ini. Banyak kejahatan cyber yang pernah kita dengar dari media masa. Pelaku kejahatan memanfaatkann celah keamanan yang ada untuk dimasuki dan melakukan manipulasi (Munir, 2006:). Sayang sekali masalah keamanan ini seringkali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting.

Apabila mengganggu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan.

Berdasarkan berbagai pertimbangan tersebut maka dalam penyusunan skripsi ini, penulis memilih judul ***"Perancangan Sistem Keamanan Informasi Data Menggunakan Metode RSA (Ron Rivest , Adi Shamir)".***

1.2 Rumusan Masalah

Dalam pelaksanaan penelitian Skripsi ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah sebagai berikut:

1. Bagaimana aspek kerahasiaan pada algoritma RSA yang ditinjau berdasarkan: kompleksitas algoritma, karakteristik penyandian plaintext terhadap chipertext.
2. Membangun sistem yang dapat menjaga kerahasiaan data menggunakan algoritma RSA berbasis dekstop.

1.3 Batasan Masalah

Batasan masalah dalam penulisan skripsi ini adalah sebagai berikut:

1. Menggunakan metode RSA dengan teknik angka dan huruf.
2. Menggunakan kunci dalam penyandian
3. Data yang dienkripsi berupa hanya berupa data String.
4. Tidak menggunakan database

1.4 Tujuan Penelitian

Berdasarkan perumusan dan batasan masalah yang tertera diatas, ada pun tujuan dri penelitian ini, antara lain :

1. Untuk mengetahui mekanisme dari metode RSA..
2. Untuk meneliti metode RSA pada penyembunyian pesan teks.
3. Membangun aplikasi perangkat lunak komputer yang dapat digunakan untuk pengujian dan implementasi kriptografi pesan teks.

1.5 Manfaat Penelitian

Dari penjabaran di atas ada pula manfaat yang diberikan, adalah :

1. Memberi kemudahan bagi pengguna dalam menyandi tulisan.
2. Menjadi contoh program bagi pengajar dalam memberi materi pengajaran kriptografi.

BAB II

LANDASAN TEORI

2.1 Kemanan Data

Pada zaman teknologi informasi sekarang, data atau informasi merupakan suatu asset yang sangat berharga dan harus dilindungi. Hal ini juga diikuti oleh kemajuan teknologi komputer. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian muncul masalah baru, yaitu masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Dan tentunya akan merugikan pihak tertentu. Dalam keamanan data ada beberapa aspek yang berkaitan dengan persyaratan kemanan yaitu (Pabokory, 2015:2)[1]:

1. *Secrecy*. Berhubungan dengan akses membaca data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diakses dan dibaca oleh orang yang berhak.
2. *Integrity*. Berhubungan dengan akses merubah data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diubah oleh orang yang berhak.
3. *Availability*. Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. (Pabokory, 2015:2)[1].

4. Lebih lanjut menurut (Pabokory, 2015:2)[1], terdapat lima langkah kemanan komputer yang baik untuk diperhitungkan yaitu; aset, analisis resiko, perlindungan, alat dan prioritas.

2.2 *Kriptografi*

Kriptografi merupakan kata dari bahasa Yunani yaitu cryptography, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Sehingga, bila digabungkan akan menjadi kata yang berarti menyembunyikan/merahasiakan tulisan. *Kriptografi* adalah suatu ilmu ataupun seni mengamankan pesan dan dilakukan oleh *cryptographer* (Anonim, 2014).[2].

Menurut (Rhee, 2013).[3] *kriptografi* digunakan untuk memastikan privasi dan autentifikasi data dalam komunikasi antar sistem komputer. Terdapat dua proses dasar dalam *kriptografi* yaitu:

1. *Enkripsi*, adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). (Pabokory, 2015:11)[1],
2. *Deskripsi*, adalah kebalikan dari *Enkripsi* yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. (Pabokory, 2015).[4]

Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah plaintext. Kemudian setelah disamarkan dengan suatu cara penyandian, maka plaintextini disebut sebagai chipertext. Proses penyamaran dari

plaintextke *cipher*text disebut *Enkripsi* (encryption), dan proses pengembalian dari *cipher*textmenjadi plaintext kembali disebut dekripsi (decryption). (Pabokory, 2015).[4] *File* yang dapat di *Enkripsi* dapat berupa teks, gambar maupun audio dan video.

2.3 *Algoritma RSA*

Algoritma RSA merupakan penerapan dari kriptografi asimetri, yakni jenis kriptografi yang menggunakan dua kunci yang berbeda: kunci publik (public key) dan kunci pribadi (private key). Dengan demikian, maka terdapat satu kunci, yakni kunci publik, yang dapat dikirimkan melalui saluran yang bebas, tanpa adanya suatu keamanan tertentu. Hal ini bertolak belakang dengan kriptografi simetri yang hanya menggunakan satu jenis kunci dan kunci tersebut harus terjaga keamanan serta kerahasiaannya. Di dalam kriptografi asimetri, dua kunci tersebut diatur sedemikian hingga sehingga memiliki hubungan dalam satu persamaan aritmatika modulo.

RSA mendasarkan proses enkripsi dan deskripsinya pada konsep bilangan prima dan aritmatika modulo. Baik kunci enkripsi maupun kunci deskripsi keduanya berupa bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui umum (sehingga dinamakan juga kunci publik), namun kunci untuk deskripsi bersifat rahasia. Kunci deskripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Untuk menemukan kunci deskripsi, orang harus memfaktorkan suatu bilangan non prima menjadi faktor primanya. Kenyataanya, memfaktorkan bilangan non prima menjadi faktor primanya bukanlah pekerjaan yang

mudah. Belum ada algoritma yang mangkus (efisien) yang ditemukan untuk pemfaktoran itu. Semakin besar bilangan non primanya tentu semakin sulit pula pemfaktorannya. Semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA. Algoritma RSA sebenarnya sederhana sekali. Secara ringkas, algoritma RSA terdiri dari tiga bagian, yaitu bagian untuk membangkitkan pasangan kunci, bagian untuk enkripsi dan bagian untuk deskripsi.

Tabel 2.1 Besaran - besaran yang digunakan pada algoritma RSA

p dan q bilangan prima	rahasia
n = p . q	tidak rahasia
(n) = (p – 1)(q – 1)	rahasia
e (kunci enkripsi)	tidak rahasia
d (kunci dekripsi)	rahasia
m (plaintext)	rahasia
c (ciphertext)	tidak rahasia

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa,

$$a\,\Phi(n) = 1 \bmod n$$

dengan syarat :

1. a harus relative prima terhadap n

2. $\Phi(n) = n(1-1/p1)\ n(1-1/p2) \ldots n(1-1/pr)$ dalam hal ini p1,p2,….pr adalah faktor prima dari n. $\Phi(n)$ adalah fungsi yang menentukan berapa banyak dari bilangan – bilangan 1,2,3,..n yang relatif prima terhadap n.

Berdasarkan sifat $a^k = a^b \pmod n$ untuk k bilangan bulat ≥ 1, maka persamaan (I) dapat ditulis menjadi

$$a\Phi k(n) = 1k \pmod n$$

atau

$$a\Phi k(n) = 1 \pmod n$$

Bila a diganti m, maka persamaan (II) dapat ditulis menjadi

$$m\Phi k(n) = 1 \pmod n$$

Berdasarkan sifat $ac = bc \pmod n$ maka bila persamaan (III) dikali dengan m, maka menjadi,

$$m\Phi k(n)+1 = m \pmod n$$

dalam hal ini m relatif prima dengan n, misalkan e dan d dipilih sedemikian sehingga

$$e \cdot d = 1 \pmod{\Phi(n)}$$

atau

$$e \cdot d = k\Phi(n) + 1$$

Masukkan (V) ke dalam persamaan (VI) menjadi,

$$me \cdot d = m \pmod n$$

Persamaan (VI) dapat ditulis kembali menjadi,

$$(me)d = m \pmod n$$

Yang artinya perpangkatan m dengan e diikuti dengan perpangkatan dengan d yang menghasilkan kembali m semula. Berdasarkan persamaan (VII), maka enkripsi dan dekripsi dirumuskan sebagai berikut

$$Ee\ (m) = c = me \bmod n$$

$$Dd(c) = m = cd \bmod n$$

Karena e . d = d . e maka enkripsi dilakukan dengan dekripsi ekivalen dengan dekripsi diikuti enkripsi

$$Dd(Ee(m)) = Ee\ (Dd(m)) = md \bmod n$$

Oleh karena md mod n = (m + jn)d mod n untuk sembarang bilangan bulat j, maka setiap *plaintext* m, m + n, m| + 2n, …, menghasilkan *chipertext* yang sama. Dengan kata lain transformasinya dari banyak ke satu, maka m harus dibatasi dalam himpunan {0, 1. 2 … n-1} sehingga enkripsi dan dekripsi tetap benar seperti persamaan (VIII) dan (IX).

2.4 Pengertian Kriptografi

Kriptografi merupakan kata dari bahasa Yunani yaitu *cryptography*, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Sehingga, bila digabungkan akan menjadi kata yang berarti menyembunyikan/merahasiakan tulisan. *Kriptografi* adalah suatu ilmu ataupun seni mengamankan pesan dan dilakukan oleh *cryptographer* (**Anonim, 2014**).

Kriptografi digunakan untuk memastikan privasi dan autentifikasi data dalam komunikasi antar sistem komputer. Terdapat dua proses dasar dalam *kriptografi* yaitu: (**Rhee, 2013**).

3. *Enkripsi*, adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). (**Pabokory, 2015:11**).
4. *Deskripsi*, adalah kebalikan dari *Enkripsi* yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. (**Pabokory, 2015**.)

Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah *plaintext*. Kemudian setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini disebut sebagai chipertext. Proses penyamaran dari *plaintext* ke *Ciphertext* disebut *Enkripsi* (*encryption*), dan proses pengembalian dari *Ciphertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*). (Pabokory, 2015). *File* yang dapat di *Enkripsi* dapat berupa teks, gambar maupun audio dan video.

2.4.1 *Kriptografi Klasik*

Kriptografi klasik adalah *kriptografi* yang disebut juga sebagai *kriptografi* kunci tunggal atau *kriptografi* simetris yang menggunakan kunci yang sama untuk *Enkripsi* maupun *Deskripsi*. *Kriptografi* klasik merupakan *kriptografi* yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. *Kriptografi* ini melakukan pengacakan huruf pada kata terang / *plaintext*. (**Bishop, 2014**).

Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya. Teknik substitusi adalah menggantikan karakter dalam *plaintext* menjadi karakter lain yang hasilnya adalah *Cipher*text. Sedangkan transposisi adalah teknik mengubah *plaintext* menjadi *Cipher*text dengan cara permutasi karakter. Kombinasi keduanya secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher, Vigenere Cipher*, dan *Hill Cipher.*

2.4.2 *Kriptografi Modern*

Algoritma kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pengolahan simbol biner yang dibentuk dari kode *ASCII* (*American Standard Code for Information Interchange*) karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya . Algoritma ini memiliki tingkat kesulitan yang kompleks yang menyebabkan kriptanalis sangat sulit memecahkan *Cipher*text tanpa mengetahui kuncinya. Adapun jenis kunci dalam kriptografi modern terdiri dari 3 yaitu: *simetri*, *asimetri*, dan hibrida. Pada kriptogarfi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Contoh kriptografi modern yaitu *MD5, RC4, AES* dan lain-lain. (**Bishop, 2014**).

2.5 Proses *Enkripsi* dan *Deskripsi*

Enkripsi yaitu suatu proses pengaman suatu data yang disembunyikan atau proses konversi data (*plaintext*) menjadi bentuk yang tidak dapat dibaca/ dimengerti. Enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, namun, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970an enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet, e-commerce, jaringan telepon bergerak dan ATM pada bank. Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integrasi dan autentikasi dari sebuah pesan. Untuk menampilkan enkripsi dan kebalikannya dekripsi, digunakan algoritma yang biasa disebut *Cipher* dengan menggunakan metode serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah Enchiperment. Informasi yang asli disebuh sebagai *plaintext*, dan bentuk yang sudah dienkripsi disebut sebagai chiphertext. Pesan chipertext berisi seluruh informasi dari pesan *plaintext*, tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekasnisme yang tepat untuk melakukan dekripsi. (**Bishop, 2014**).

Sedangkan Dekripsi yaitu kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (ciphertext) kembali menjadi data aslinya (Original Plaintext) sehingga dapat dibaca/ dimengerti kembali.Pesan yang akan dienkripsi

disebut plaintext yang dimisalkan plaintext (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah dienkripsi disebut ciphertext yang dimisalkan ciphertext (C). (**Bishop, 2014**).

2.6 *One Time Pad (OTP)*

Algoritma *One Time Pad* (OTP) merupakan algoritma berjenis *Symetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream Cipher* yang berasal dari hasi XOR antara *bit plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode ASCII dan kemudian dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII. (Hamokwarong, 10 :2014)

One-time pad adalah salah satu stream *Cipher* klasik yang secara matematis terbukti sempurna aman. *Cipher* teksnya tidak mungkin dapat dipecahkan. Keamanan algoritma *one-time pad* terletak pada penggunaan barisan bilangan acak sejati (*trully random*) sebagai kunci enkripsi, panjang kunci sama dengan panjang pesan dan tidak ada perulangan kunci sebagaimana pada pada *Vernam Cipher* atau *RSA*. (Munir, 12 :2014)

Sayangnya *one-time pad* tidak dapat diimplementasikan secara praktis sebab pembangkitan bilangan acak sejati tidak dapat diulang kembali di sisi penerima pesan. Oleh karena itu kunci (*pad*) harus dikirim melalui saluran komunikasi yang kedua (misalnya melalui kurir), sayangnya saluran kedua itu umumnya lambat dan

ongkosnya mahal. One-time pad masih dapat diterapkan namun kunci yang berupa barisan bilangan acak diganti dengan barisan bilangan semi-acak (*pseudo-random*) dengan syarat barisan kunci itu tidak boleh berulang. (Munir, 12 :2014)

2.7 Algoritma

Penyelesaian permasalahan dengan menggunakan alat bantu system computer paling tidak akan melibatkan lima tahapan, yaitu:

1. Analisis masalah
2. Merancang algoritma
3. Membuat program computer
4. Menguji hasil program computer
5. Dokumentasi

Poin kedua menerangkan bahwa dalam perancangan sebuah system computer dibutuhkan adanya perancangan algoritma. Sehingga setelahnya dapat dilanjutkan ke tahap-tahap berikutnya hingga dokumentasi.

Algoritma adalah Sistim kerja komputer memiliki brainware, hardware, dan software. Tanpa salah satu dari ketiga sistim tersebut, komputer tidak akan berguna. Kita akan lebih fokus pada softwarekomputer. Software terbangun atas susunan program (silahkan baca mengenai pengertian program) dan syntax (cara penulisan/pembuatan program). Untuk menyusun program atau syntax, diperlukannya langkah-langkah yang sistematis dan logis untuk dapat menyelesaikan

masalah atau tujuan dalam proses pembuatan suatu software. Maka, Algoritma berperan penting dalam penyusunan program atau syntax tersebut.

Pengertian Algoritma adalah susunan yang logis dan sistematis untuk memecahkan suatu masalah atau untuk mencapai tujuan tertentu. Dalam dunia komputer,Algoritma sangat berperan penting dalam pembangunan suatu software. Dalam dunia sehari-hari, mungkin tanpa kita sadari Algoritma telah masuk dalam kehidupan kita.

Pengertian Algoritma adalah susunan yang logis dan sistematis untuk memecahkan suatu masalah atau untuk mencapai tujuan tertentu.

Algoritma adalah kunci dari bidang ilmu komputer, dan pada dasarnya setiap hari kita melakukan aktivitas algoritma. Kata algoritma berasal dari sebutan Algorizm (Abu Abdullah Muhammad Ibn Musa Al Khwarizmi, ahli matematika Uzbeki

a. Algoritma adalah urutan langkah-langkah berhingga untuk memecahkan masalah logika atau matematika
b. Algoritma adalah logika, metode dan tahapan (urutan) sistematis yang digunakan untuk memecahkan suatu permasalahan.
c. Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis.
d. Algoritma adalah urutan logis pengambilan keputusan untuk pemecahan masalah.

Pembuatan algoritma harus selalu dikaitkan dengan:

a. Kebenaran algoritma

b. Kompleksitas (lama dan jumlah waktu proses dan penggunaan memori)

Kriteria Algoritma yang baik:

a. Tepat, benar, sederhana, standar dan efektif
b. Logis, terstruktur dan sistematis
c. Semua operasi terdefinisi
d. Semua proses harus berakhir setelah sejumlah langkah dilakukan
e. Ditulis dengan bahasa yang standar dengan format pemrograman agar mudah untuk diimplementasikan dan tidak menimbulkan arti ganda.

2.8 *Unified Modeling Language* (UML)

1. Pengenalan UML

Unified Modelling Language (UML) adalah suatu alat untuk memvisualisasikan dan mendokumentasikan hasil analisis dan desain yang berisi sintak dalam memodelkan sistem secara visual (Haviluddin : 2015 : 1). Banyak orang yang telah membuat bahasa pemodelan pembangunan perangkat lunak sesuai dengan teknologi pemrograman yang berkembang pada saat itu, misalnya yang sempat berkembang dan digunakan oleh banyak pihak adalah *Data Flow Diagram* (DFD) untuk memodelkan perangkat lunak yang menggunakan pemrograman prosedural atau struktur, kemudian juga ada *State Transition Diagram* (STD) yang digunakan untuk memodelkan *real time* (waktu nyata).

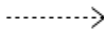
Pada perkembangan teknik pemrograman berorientasi objek, muncullah sebuah standarisasi bahasa pemodelan untuk pembangunan perangkat lunak yang

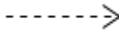
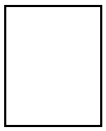
dibangun dengan menggunakan teknik pemrograman berorientasi objek, yaitu *Unified Modeling Language* (UML).

2. *Use Case Diagram*

Diagram yang menggambarkan *actor*, *use case* dan relasinya sebagai suatu urutan tindakan yang memberikan nilai terukur untuk aktor. Sebuah *use case* digambarkan sebagai elips horizontal dalam suatu diagram *use case diagram* (Haviluddin : 2015 : 4).

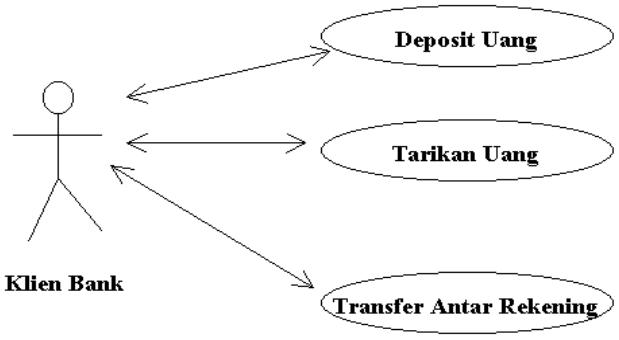
Tabel 2.2 Simbol *Use Case Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		*Actor*	Menspesifikasikan himpuan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.
2		*Dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri *(independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*independent*).
3		*Generalization*	Hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (*ancestor*).

4		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
5		*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.
6		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu actor
9		*Collaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

Sumber : (Gellysa Urva, 94 : 2015)

Contoh Use Case Diagram :



Gambar 2.1. Contoh *Use Case Diagram*
Sumber : (Haviluddin : 2015 : 4)

3. *Activity Diagram*

Diagram aktivitas atau *activity diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau *menu* yang ada pada perangkat lunak. Yang perlu diperhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem.

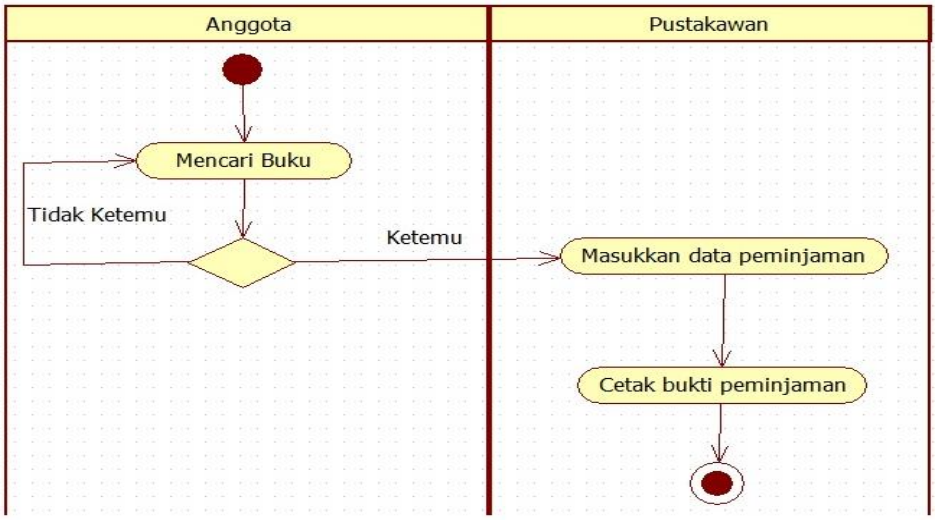
Tabel 2.3. Simbol *Activity Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		*Activity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain

2		*Action*	*State* dari sistem yang mencerminkan eksekusi dari suatu aksi
3		*Initial Node*	Bagaimana objek dibentuk atau diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Sumber : (Gellysa Urva, 94 : 2015)

Contoh Activity Diagram :



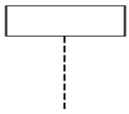
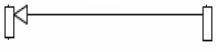
Gambar 2.2. Contoh *Activity Diagram*

Sumber : (Gellysa Urva, 94 : 2015)

4. *Sequence Diagram*

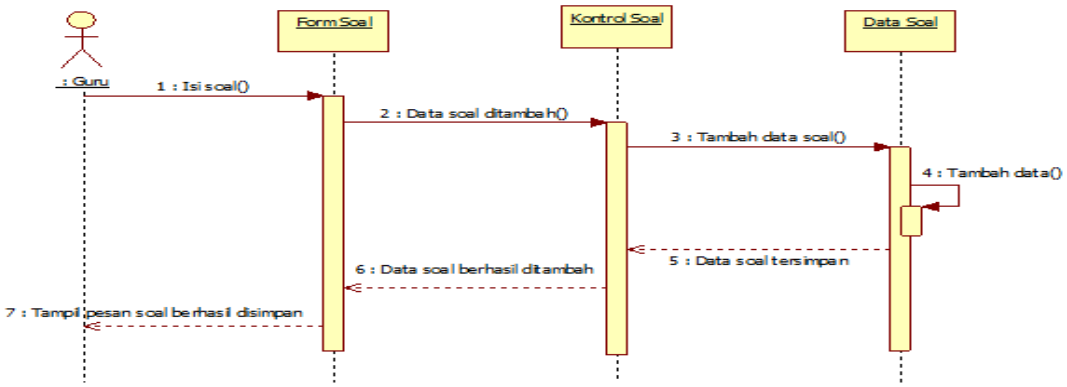
Diagram sekuen menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. Oleh karena itu untuk menggambar diagram sekuen maka harus diketahui objek-objek yang terlibat dalam sebuah *use case* beserta metode-metode yang dimiliki kelas yang diinstansiasi menjadi objek itu. Membuat diagram sekuen juga dibutuhkan untuk melihat skenario yang ada pada *use case.*

Tabel 2.4. Simbol *Sequence Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		*LifeLine*	Objek *entity*, antarmuka yang saling berinteraksi.
2		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi
3		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi

Sumber : (Gellysa Urva, 95 : 2015)

Contoh Squence Diagram :

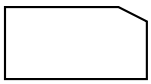
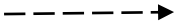


Gambar 2.3. Contoh *Squence Diagram*
Sumber : (Gellysa Urva, 95 : 2015)

5. *Class Diagram*

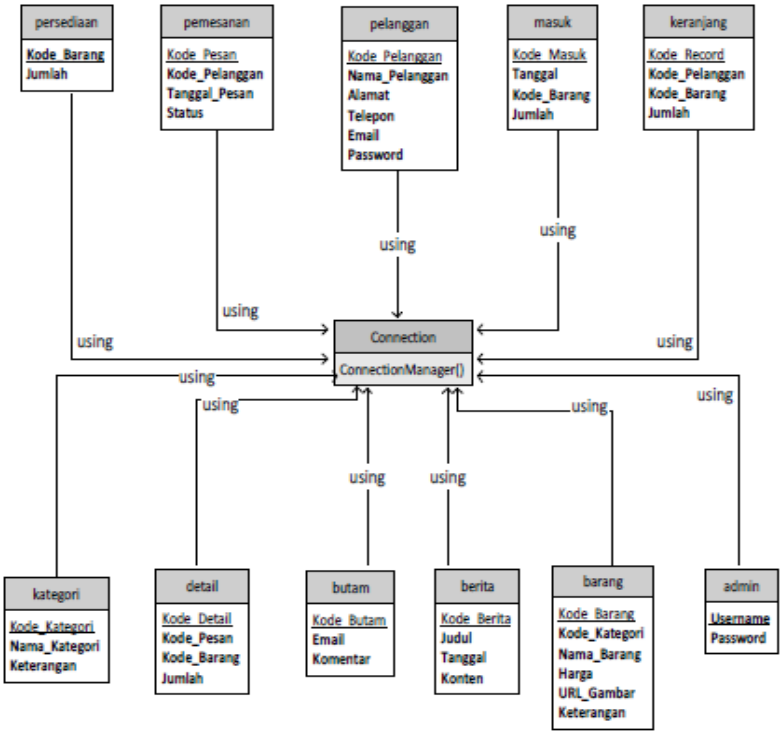
Class diagram menggambarkan struktur statis dari kelas dalam sistem anda dan menggambarkan atribut, operasi dan hubungan antara kelas. Class diagram membantu dalam memvisualisasikan struktur kelas-kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak dipakai. Selama tahap desain, class diagram berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat.

Tabel 2.5. Simbol *Class Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi
2		*dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri akan mempengaruhi elemen yang bergantung padanya
3		*extend*	Menspesifikasikan bahwa use case target memperluas prilaku dari use case sumber pada suatu titik yang diberikan.

Sumber : (Gellysa Urva, 95 : 2015)

Contoh *Class* Diagram :



Gambar 2.4. Contoh *Class Diagram*

Sumber : (Gellysa Urva, 95 : 2015)

2.9 Pengertian Informasi

Secara Etimologi, kata informasi ini berasal dari kata bahasa Perancis kuno *informacion* (tahun 1387) mengambil istilah dari bahasa Latin yaitu *informationem* yang berarti "konsep, ide atau garis besar". Informasi ini merupakan kata benda dari *informare* yang berarti aktivitas dalam "pengetahuan yang dikomunikasikan".

Informasi adalah hasil pemrosesan data yang diperoleh dari setiap elemen sistem menjadi bentuk yang mudah dipahami dan merupakan pengetahuan yang relevan dan berguna (Yulansari, 6 : 2013).

Informasi bisa menjadi fungsi penting dalam membantu mengurangi rasa cemas pada seseorang. Menurut pendapat Notoatmodjo (2018) bahwa semakin banyak memiliki informasi dapat memengaruhi atau menambah pengetahuan terhadap seseorang dan dengan pengetahuan tersebut bisa menimbulkan kesadaran yang akhirnya seseorang itu akan berperilaku sesuai dengan pengetahuan yang dimilikinya.

Informasi adalah data yang telah diolah melalui proses tertentu menjadi sesuatu yang menambah pengetahuan atau temuan yang mempunyai arti baru bagi pemakainya (Melina, 38 : 2014).

Adapun fungsi-fungsi informasi adalah sebagai berikut:

1. Untuk meningkatkan pengetahuan bagi si pemakai.
2. Untuk mengurangi ketidakpastian dalam proses pengambilan keputusan pemakai.
3. Menggambarkan keadaan yang sebenarnya dari sesuatu hal.Informasi yang berkualitas harus akurat, tepat dan relevan.

Sumber dari informasi adalah data. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Data merupakan bentuk yang masih mentah, belum dapat bercerita banyak sehingga perlu diolah lebih lanjut. Data diolah melalui suatu metode untuk menghasilkan informasi. Data dapat

berbentuk simbol-simbol semacam huruf, angka, bentuk suara, sinyal, gambar, dan sebagainya.

2.10 Pengertian Visual Studio

Visual Studio .Net merupakan salah satu *tool development Microsoft* yang dapat digunakan untuk membuat aplikasi di lingkungan kerja berbasis sistem operasi *Windows*. *Visual Studio .NET* menyediakan tools bagi para *developer* untuk membangun aplikasi yang berjalan di *.Net Framework* (Safik : 2015 : 2).

Visual Studio (*Beginners All-Purpose Symbolic Instruction Code*) merupakan Bahasa pemrograman *Integrated Development Environment* (IDE), yaitu bahasa pemrograman *visual* yang digunakan untuk membuat program aplikasi atau *software* berbasis sistem operasi *Microsoft Windows*, dengan menggunakan model pemrograman "*Common Object Model* (COM)".

Visual Studio merupakan turunan bahasa pemrograman *STUDIO* yang menawarkan pengembangan perangkat lunak komputer bebasis grafik dengan cepat. Dengan menggunakan bahasa pemrograman VB, para progammer dapat membangun aplikasi dengan menggunakan komponen-komponen yang di sediakan VB.

Microsoft Visual Studio (sering disingkat sebagai VB saja) merupakan sebuah bahasa pemrograman yang menawarkan *Integrated Development Environment* (IDE) visual untuk membuat program perangkat lunak berbasis sistem operasi Microsoft Windows dengan menggunakan model pemrograman (*COM*), *Visual Studio* merupakan turunan bahasa pemrograman *STUDIO* dan menawarkan pengembangan

perangkat lunak komputer berbasis grafik dengan cepat, Beberapa bahasa skrip seperti *Visual Studio for Applications* (*VBA*) dan *Visual Studio Scripting Edition* (*VBScript*), mirip seperti halnya *Visual Studio*, tetapi cara kerjanya yang berbeda.

Para *programmer* dapat membangun aplikasi dengan menggunakan komponen-komponen yang disediakan oleh *Microsoft Visual Studio* Program-program yang ditulis dengan *Visual Studio* juga dapat menggunakan *Windows* API, tapi membutuhkan deklarasi fungsi luar tambahan.

Dalam pemrograman untuk bisnis, *Visual Studio* memiliki pangsa pasar yang sangat luas. Dalam sebuah survey yang dilakukan pada tahun 2005, 62% pengembang perangkat lunak dilaporkan menggunakan berbagai bentuk *Visual Studio*, yang diikuti oleh *C++, JavaScript, C#,* dan *Java*.

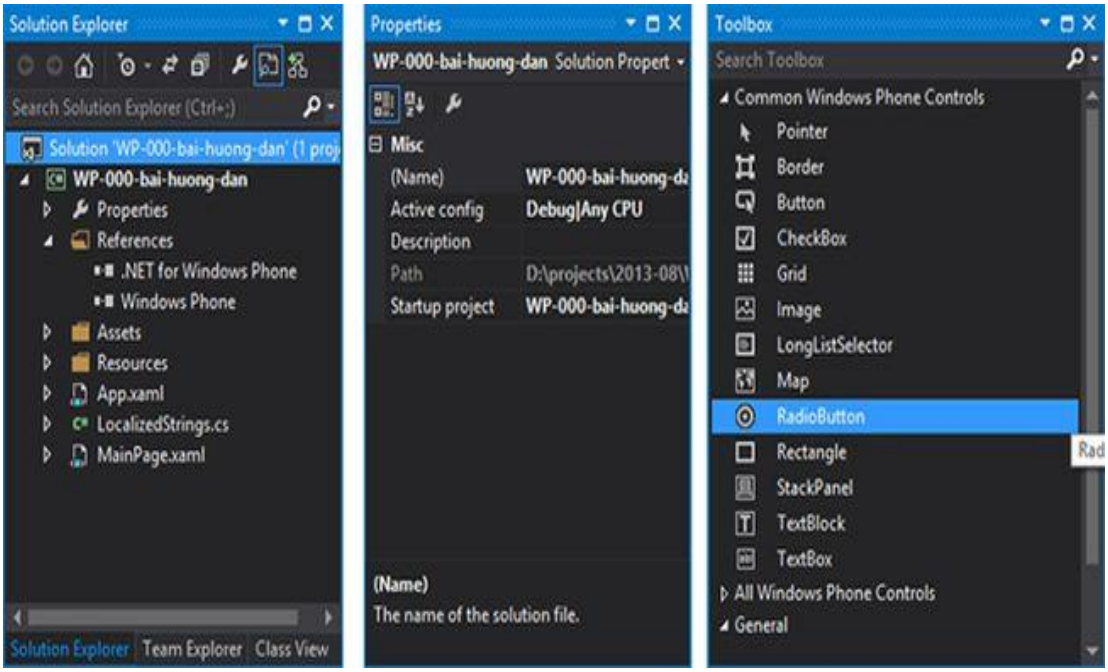
1. Komponen kerja

Beberapa komponen kerja program *visual Studio 2015* telah ditampilkan sebagai tampilan standard. Masih banyak lagi komponen yang masih tersembunyi sehingga memerlukan perintah tertentu untuk menampilkannya. Kita dapat mengatur komponen di dalam program visual Studio 2015 sesuai dengan yang kita butuhkan. Berikut ini adalah beberapa komponen kerja dari visual Studio 2015 adalah :

a. Toolbox

Toolbox adalah sebuah panel yang menampung tombol-tombol yang berguna untuk membuat suatu desain mulai dari tombol *label, pointer, button*, dan lain-lain. Berikut ini adalah gambaran *toolbox* pada *visual Studio 2015* :

Berikut ini adalah *table* yang berisi nama tombol yang terdapat didalam *toolbox* beserta fungsinya.



Gambar 2.5. Tampilan *Toolbox*
Sumber : (Safik : 2015 : 2).

Tabel 2.6. *Toolbox Visual Studio*

Nama tombol	Fungsi
Pointer	Memilih, mengatur ukuran dan memindahkan posisi yang terpasang di bagian form.
Bindingsources	Untuk mengkoneksikan program ke database
Label	Menampilkan teks, dimana pengguna program tidak bisa mengubah teks tersebut
Groupbox	Untuk mengelompokkan item yang ada di form
Checkbox	Membuat kotak periksa, dimana pengguna program dapat memilih sekaligus
Listbox	Membuat daftar pilihan
Timer	Membuat control waktu dan interval yang diperlukan
Image	Menampilkan gambar pada form dalam format *bit*map, icone,

	atau metafile
Picturebox	Menampilkan gambar dari sebuah file
Textbox	Membuat teks, dimana teks tersebut dapat diubah oleh pembuat program
Button	Membuat tombol perintah
Combobox	Menambahkan control kotak combo yang merupakan control gabungan antara textbox dan listbox

Sumber : (Safik : 2015 : 2).

2.11 Tabel ASCII

ASCII merupakan kepanjangan dari (American Standard Code for Information Interchange), dan pengertian dari ASCII sendiri adalah suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. sedangkan fungsi dari kode ASCII ialah digunakan untuk mewakili karakter-karakter angka maupun huruf didalam komputer, sebagai contoh dapat kita lihat pada karakter 1, 2, 3, A, B, C, dan sebagainya.

DEC	OCT	HEX	BIN	Symbol
0	000	00	00000000	NUL
1	001	01	00000001	SOH
2	002	02	00000010	STX
3	003	03	00000011	ETX
4	004	04	00000100	EOT
5	005	05	00000101	ENQ
6	006	06	00000110	ACK

7	007	07	00000111	BEL
8	010	08	00001000	BS
9	011	09	00001001	HT
10	012	0A	00001010	LF
11	013	0B	00001011	VT
12	014	0C	00001100	FF
13	015	0D	00001101	CR
14	016	0E	00001110	SO
15	017	0F	00001111	SI
16	020	10	00010000	DLE
17	021	11	00010001	DC1
18	022	12	00010010	DC2
19	023	13	00010011	DC3
20	024	14	00010100	DC4
21	025	15	00010101	NAK
22	026	16	00010110	SYN
23	027	17	00010111	ETB
24	030	18	00011000	CAN
25	031	19	00011001	EM
26	032	1A	00011010	SUB
27	033	1B	00011011	ESC
28	034	1C	00011100	FS
29	035	1D	00011101	GS
30	036	1E	00011110	RS
31	037	1F	00011111	US
DEC	OCT	HEX	BIN	Symbol
32	040	20	00100000	
33	041	21	00100001	!
34	042	22	00100010	"

35	043	23	00100011	#
36	044	24	00100100	$
37	045	25	00100101	%
38	046	26	00100110	&
39	047	27	00100111	'
40	050	28	00101000	(
41	051	29	00101001	)
42	052	2A	00101010	*
43	053	2B	00101011	+
44	054	2C	00101100	,
45	055	2D	00101101	-
46	056	2E	00101110	.
47	057	2F	00101111	/
48	060	30	00110000	0
49	061	31	00110001	1
50	062	32	00110010	2
51	063	33	00110011	3
52	064	34	00110100	4
53	065	35	00110101	5
54	066	36	00110110	6
55	067	37	00110111	7
56	070	38	00111000	8
57	071	39	00111001	9
58	072	3A	00111010	:
59	073	3B	00111011	;
60	074	3C	00111100	<
61	075	3D	00111101	=
62	076	3E	00111110	>
63	077	3F	00111111	?

64	100	40	01000000	@
65	101	41	01000001	A
66	102	42	01000010	B
67	103	43	01000011	C
68	104	44	01000100	D
69	105	45	01000101	E
70	106	46	01000110	F
71	107	47	01000111	G
72	110	48	01001000	H
73	111	49	01001001	I
74	112	4A	01001010	J
75	113	4B	01001011	K
76	114	4C	01001100	L
77	115	4D	01001101	M
78	116	4E	01001110	N
79	117	4F	01001111	O
80	120	50	01010000	P
81	121	51	01010001	Q
82	122	52	01010010	R
83	123	53	01010011	S
84	124	54	01010100	T
85	125	55	01010101	U
86	126	56	01010110	V
87	127	57	01010111	W
88	130	58	01011000	X
89	131	59	01011001	Y
90	132	5A	01011010	Z
91	133	5B	01011011	[
92	134	5C	01011100	\

93	135	5D	01011101	]
94	136	5E	01011110	^
95	137	5F	01011111	_
96	140	60	01100000	`
97	141	61	01100001	a
98	142	62	01100010	b
99	143	63	01100011	c
100	144	64	01100100	d
101	145	65	01100101	e
102	146	66	01100110	f
103	147	67	01100111	g
104	150	68	01101000	h
105	151	69	01101001	i
106	152	6A	01101010	j
107	153	6B	01101011	k
108	154	6C	01101100	l
109	155	6D	01101101	m
110	156	6E	01101110	n
111	157	6F	01101111	o
112	160	70	01110000	p
113	161	71	01110001	q
114	162	72	01110010	r
115	163	73	01110011	s
116	164	74	01110100	t
117	165	75	01110101	u
118	166	76	01110110	v
119	167	77	01110111	w
120	170	78	01111000	x
121	171	79	01111001	y

122	172	7A	01111010	z
123	173	7B	01111011	{
124	174	7C	01111100	|
125	175	7D	01111101	}
126	176	7E	01111110	~
127	177	7F	01111111	
128	200	80	10000000	€
129	201	81	10000001	
130	202	82	10000010	,
131	203	83	10000011	*f*
132	204	84	10000100	„
133	205	85	10000101	…
134	206	86	10000110	†
135	207	87	10000111	‡
136	210	88	10001000	ˆ
137	211	89	10001001	‰
138	212	8A	10001010	Š
139	213	8B	10001011	‹
140	214	8C	10001100	Œ
141	215	8D	10001101	
142	216	8E	10001110	Ž
143	217	8F	10001111	
144	220	90	10010000	
145	221	91	10010001	‘
146	222	92	10010010	’
147	223	93	10010011	“
148	224	94	10010100	”
149	225	95	10010101	•
150	226	96	10010110	–

151	227	97	10010111	—
152	230	98	10011000	˜
153	231	99	10011001	™
154	232	9A	10011010	š
155	233	9B	10011011	›
156	234	9C	10011100	œ
157	235	9D	10011101	
158	236	9E	10011110	ž
159	237	9F	10011111	Ÿ
160	240	A0	10100000	
161	241	A1	10100001	¡
162	242	A2	10100010	¢
163	243	A3	10100011	£
164	244	A4	10100100	¤
165	245	A5	10100101	¥
166	246	A6	10100110	¦
167	247	A7	10100111	§
168	250	A8	10101000	¨
169	251	A9	10101001	©
170	252	AA	10101010	ª
171	253	AB	10101011	«
172	254	AC	10101100	¬
173	255	AD	10101101	
174	256	AE	10101110	®
175	257	AF	10101111	¯
176	260	B0	10110000	°
177	261	B1	10110001	±
178	262	B2	10110010	²
179	263	B3	10110011	³

180	264	B4	10110100	´
181	265	B5	10110101	µ
182	266	B6	10110110	¶
183	267	B7	10110111	·
184	270	B8	10111000	¸
185	271	B9	10111001	¹
186	272	BA	10111010	º
187	273	BB	10111011	»
188	274	BC	10111100	¼
189	275	BD	10111101	½
190	276	BE	10111110	¾
191	277	BF	10111111	¿
192	300	C0	11000000	À
193	301	C1	11000001	Á
194	302	C2	11000010	Â
195	303	C3	11000011	Ã
196	304	C4	11000100	Ä
197	305	C5	11000101	Å
198	306	C6	11000110	Æ
199	307	C7	11000111	Ç
200	310	C8	11001000	È
201	311	C9	11001001	É
202	312	CA	11001010	Ê
203	313	CB	11001011	Ë
204	314	CC	11001100	Ì
205	315	CD	11001101	Í
206	316	CE	11001110	Î
207	317	CF	11001111	Ï
208	320	D0	11010000	Ð

209	321	D1	11010001	Ñ
210	322	D2	11010010	Ò
211	323	D3	11010011	Ó
212	324	D4	11010100	Ô
213	325	D5	11010101	Õ
214	326	D6	11010110	Ö
215	327	D7	11010111	×
216	330	D8	11011000	Ø
217	331	D9	11011001	Ù
218	332	DA	11011010	Ú
219	333	DB	11011011	Û
220	334	DC	11011100	Ü
221	335	DD	11011101	Ý
222	336	DE	11011110	Þ
223	337	DF	11011111	ß
224	340	E0	11100000	à
225	341	E1	11100001	á
226	342	E2	11100010	â
227	343	E3	11100011	ã
228	344	E4	11100100	ä
229	345	E5	11100101	å
230	346	E6	11100110	æ
231	347	E7	11100111	ç
232	350	E8	11101000	è
233	351	E9	11101001	é
234	352	EA	11101010	ê
235	353	EB	11101011	ë
236	354	EC	11101100	ì
237	355	ED	11101101	í

238	356	EE	11101110	î
239	357	EF	11101111	Ï
240	360	F0	11110000	Đ
241	361	F1	11110001	Ñ
242	362	F2	11110010	Ò
243	363	F3	11110011	Ó
244	364	F4	11110100	Ô
245	365	F5	11110101	Õ
246	366	F6	11110110	Ö
247	367	F7	11110111	÷
248	370	F8	11111000	Ø
249	371	F9	11111001	Ù
250	372	FA	11111010	Ú
251	373	FB	11111011	Û
252	374	FC	11111100	Ü
253	375	FD	11111101	Ý
254	376	FE	11111110	Þ
255	377	FF	11111111	Ÿ

2.12 Bahasa pemrograman

Bahasa pemrograman adalah perintah-perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas tertentu.Bahasa pemrograman merupakan sebuah instruksi untuk memerintah komputer agar bisa menjalankan fungsi tertentu, namun hanya instruksi standar saja. Bahasa pemrograman juga memiliki perhimpunan dari aturan sintaks dan semantik yang tugasnya untuk mendefinisikan program komputer. Bahasa pemrograman komputer yang kita kenal antara lain adalah *Java, Visual Basic, C++, C, PHP,* dan bahasa pemrograman lainnya. Namun tentu saja kebutuhan bahasa ini harus disesuaikan dengan fungsi dan perangkat yang menggunakannya.

Menurut generasi bahasa pemrograman digolongkan menjadi 4 generasi, yaitu:

a. Generasi ke-1: *machine language*
b. Generasi ke-2: *assembly language*: *Assembler*
c. Generasi ke-3: *high level programming language,* contoh: C dan *Pascal*
d. Generasi ke-4: *4 GL (fourth-generation language),* contoh: *SQL*
e. Generasi ke-5: *Programming Language Based Object Oriented & Web Development*

Secara umum bahasa pemrograman dibagi menjadi 4 kelompok, yaitu :

1. Object Oriented Language : Seperti bahasa *Visual C, Delphi, Visual dBase, Visual FoxPro.*
2. *Low Level Language* : Bahasa *Assembly.*
3. Middle Level Language : Bahasa *C.*
4. *High Level Language* : *Bahasa Basic* dan *Pascal.*

Menurut tingkat kedekatannya dengan mesin komputer, bahasa pemrograman terdiri dari:

a. Bahasa Mesin, yaitu memberikan perintah kepada komputer dengan memakai kode bahasa biner, contohnya 01100101100110.
b. Bahasa Tingkat Rendah, atau dikenal dengan istilah bahasa rakitan (bah.Inggris *Assembly*), yaitu memberikan perintah kepada komputer dengan memakai kode-kode singkat (kode *mnemonic*), contohnya *MOV, SUB, CMP, JMP, JGE, JL, LOOP,* dsb.

c. Bahasa Tingkat Menengah, yaitu bahasa komputer yang memakai campuran instruksi dalam kata-kata bahasa manusia (lihat contoh Bahasa Tingkat Tinggi di bawah) dan instruksi yang bersifat simbolik, contohnya {, }, ?, <<, >>, &&.

d. Bahasa Tingkat Tinggi, yaitu bahasa komputer yang memakai instruksi berasal dari unsur kata-kata bahasa manusia, contohnya *begin, end, if, for, while, and, or, dsb.* Komputer dapat mengerti bahasa manusia itu diperlukan program *compiler* atau *interpreter.*

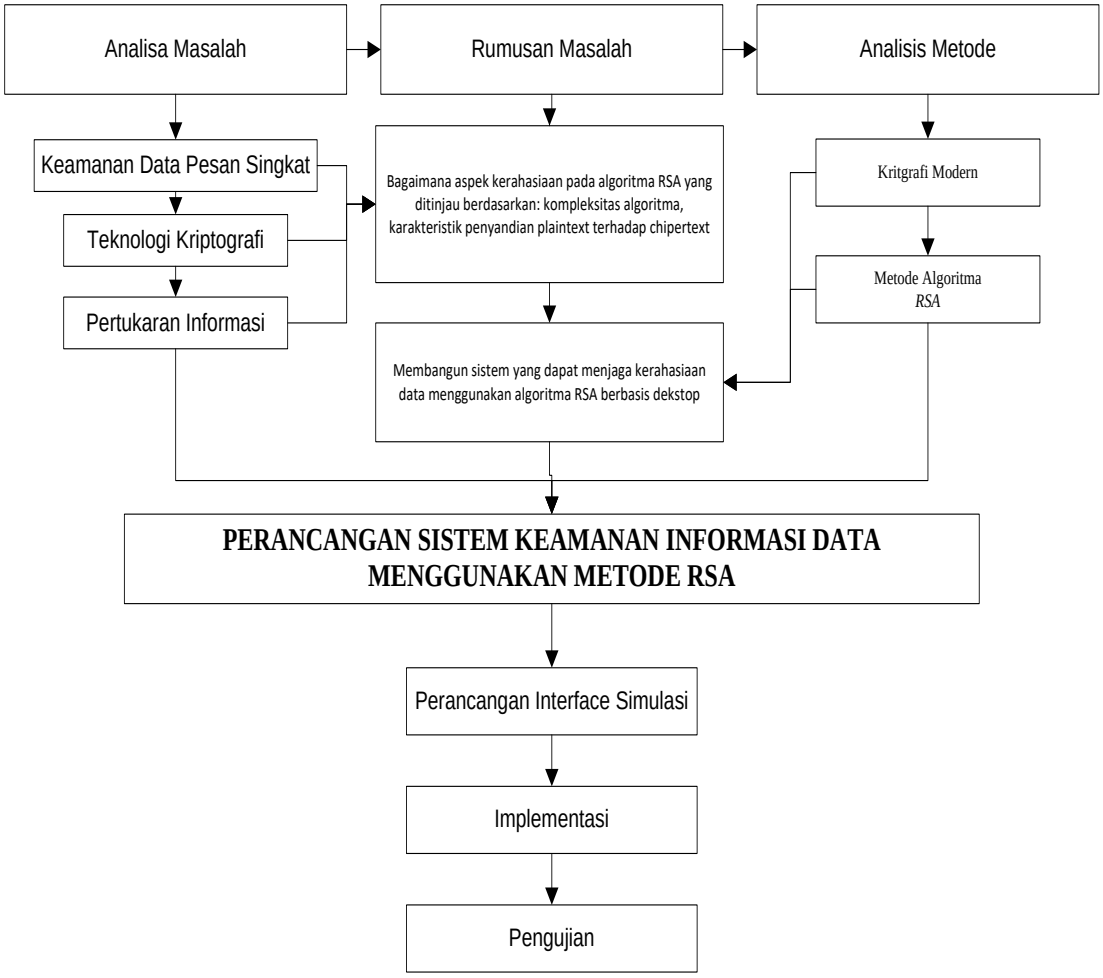
Fungsi dari bahasa pemrograman adalah untuk memerintahkan sebuah komputer agar dapat mengolah data yang sesuai dengan di inginkan. *Output* dari bahasa pemrograman ini dapat berupa aplikasi ataupun program khusus. Contoh sederhananya seperti lampu lalu lintas di jalan raya.

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul Perancangan Sistem Keamanan Informasi Data Menggunakan Metode RSA adalah sebagai berikut:



Gambar 3.1 Tahapan Penelitian

3.2 Metode Pengumpulan Data

Pengumpulan data adalah pencarian terhadap susuatu kerena ada perhatian dan keinginan terhadap hasil suatu aktivitas. Metode pengumpulan data dalam penulisan ini dibagi menjadi 3, yaitu :

1. Wawancara (*Interview*).

   Wawancara ini dilakukan dengan cara mengadakan komunikasi langsung dengan dosen pengampu mata kuliah kemanan data di Universitas Pembangunan Pancabudi Medan yang dapat memberikan informasi dan data-data yang diperoleh mengenai kemanaan data dan *RSA*.

2. Pengamatan (*Observation*)

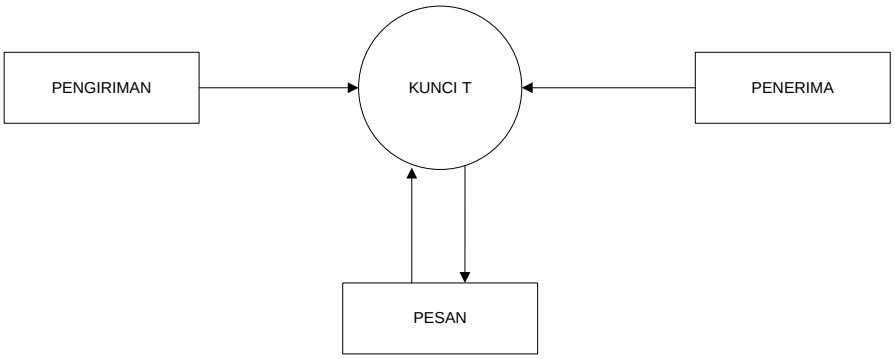
   Penulis melakukan pengamatan langsung pada setiap penggunan aplikasi chating yang sudah ada seperti WA, BBM dan Line untuk mengamati proses keamanan yang sudah dibuat sebelumnya.

3. Penelitian Kepustakaan (*Library Research*)

   Merupakan cara untuk mencari referensi dengan mengumpulkan bahan-bahan pustaka yang dilakukan di perpustakaan kampus, maupun perpustakaan umum, juga melakukan pencarian lewat internet, dengan mengunjungi situs-situs seperti *google Book online* yang dapat membantu pembahasan materi.

3.3 Analisa Permasalahan yang Berjalan

Pertukaran data dalam hal ini pesan rahasia berbentuk teks dengan menggunakan metode tradisional yaitu dengan cara bertukar kata kunci tunggal. Diagram dibawah adalah penggambaran bagaimana pertukaran pesan rahasia menggunakan kunci tunggal terjadi.



Gambar 3.2 Skema Pengiriman Pesan

Pemberitahuan kata kunci dari pengirim ke penerima menggunakan media yang umum digunakan oleh banyak orang.

3.4 Analisa Kelemahan yang Berjalan

1. Penggunaan kata kunci tunggal berpotensi terjadinya salah pemahaman. Dalam hal ini kemungkinan penerima salah mengartikan kunci yang diberikan oleh pengirim adalah hal yang dapat terjadi.
2. Pemberitahuan atau pertukaran kata kunci yang dikirimkan oleh pengirim ke penerima memiliki potensi dapat diketahui oleh orang lain sehingga pesan rahasia dapat terbongkar.

3.5 Solusi Pemecahan Masalah

Pemecahan masalah yang penulis lakukan adalah dengan melakukan penerapan metode ini yang didalamnya terdapat Algoritma *RSA*. Penggunaan metode ini dapat digunakan sebagai solusi agar pengirim dan penerima tidak lagi harus bertukar kunci tunggal untuk membuka pesan melainkan dapat memiliki kata kunci masing-masing.

Tabel 3.1 Tabel Perencanaan Rancangan

No	Sistem yang Berjalan	Sistem yang Diusulkan	Hasil yang Ingin Dicapai
1.	Penggunaan kunci tunggal yang harus diketahui oleh pengirim dan penerima untuk membuka pesan.	Pengirim dan penerima memiliki kunci masing-masing untuk membuka pesan	Tidak ada lagi kesalahan pemahaman atau salah tafsir kunci tunggal karena pengirim dan penerima memiliki kunci yang dapat ditetapkan masing-masing pihak.
2.	Pertukaran kunci tunggal menggunakan media komunikasi yang rentan untuk	Pengirim dan penerima dapat menentukan sendiri kunci yang ingin	Kemungkinan bocornya kunci saat proses pertukaran informasi kunci

	dapat diketahui orang lain.	digunakan untuk membuka pesan.	tunggal dapat dihindari.

3.6 Analisa Kebutuhan Sistem

Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen – komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukkan yan diperlukan sistem, keluaran yang akan dihasilkan sistem dan proses yang dibutuhkan untuk mengolah masukkan sehingga menghasilkan suatu keluaran yang diinginkan.

1. Analisis Perangkat Keras (Hardware)

Perangkat keras minimum yang digunakan untuk membangun Sistem Informasi Penjualan ini adalah

1. Processor berkecepatan 2.0 Ghz
2. RAM 2 Gb
3. Hardisk minimal 10 Gb untuk menyimpan data
4. LAN Card
5. Keyboard dan Mouse
6. Monitor 14.

2. Analisis Perangkat Lunak (Software)

Untuk mendukung dalam penyimpanan informasi, dibutuhkan suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (software) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sisten nantinya. Adapun perangkat lunak yang digunakan adalah sebagai berikut :

1. Microsoft Windows 7 , Windows XP sebagai sistem operasi
2. Mozila Firefox version 3.5 sebagai browser
4. Microsoft visual studio 2010 .

3.7 Analisa Proses Sistem Yang Berjalan

Visual basic 2010 akan menjadi sarana untuk menciptakan perangkat lunak ini. Pada analisa proses ini penggunaan digunakan sebagai metode yang didalamnya terdapat kombinasi dari algoritma *RSA*. Algoritma *RSA* digunakan oleh pengirim untuk mengenkripsi pesan yang akan dikirimkan..

Perhitungan secara matematis dilakukan sebagai penggambaran proses yang akan terjadi pada metode ini yang didalamnya terdapat algoritma *RSA*. Berikut tahapannya:

1. Proses Enkripsi Dan Deskripsi RSA

Misalkan

p = 3

q = 7

n = p.q

= 3 x 7

= 21

m = (p-1) (q-1)

= (3 -1)(7 – 1)

= 12

e * d mod 12 = 1

e = 5

d = 17

public key = (e,n) = (5,21)

private key = (d,n) = (17,21)

Plaintext:

TANTO

84 65 78 84 79 (tabel ascii code)

T=84	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
8 ^ 5 mod 21 = 8	8 ^ 17 mod 21 = 8
4 ^ 5 mod 21 = 16	16 ^ 17 mod 21 = 4
A=65	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
6 ^ 5 mod 21 = 6	6 ^ 17 mod 21 = 6
4 ^ 5 mod 21 = 16	16 ^ 17 mod 21 = 10
N=78	

Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
7 ^ 5 mod 21 = 7	7 ^ 17 mod 21 = 7
8^ 5 mod 21 = 8	8 ^ 17 mod 21 = 10
T=84	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
8 ^ 5 mod 21 = 8	8 ^ 17 mod 21 = 10
4 ^ 5 mod 21 = 16	16 ^ 17 mod 21 = 10
0=79	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
7 ^ 5 mod 21 = 7	7 ^ 17 mod 21 = 7
9 ^ 5 mod 21 = 18	18 ^ 17 mod 21 = 12

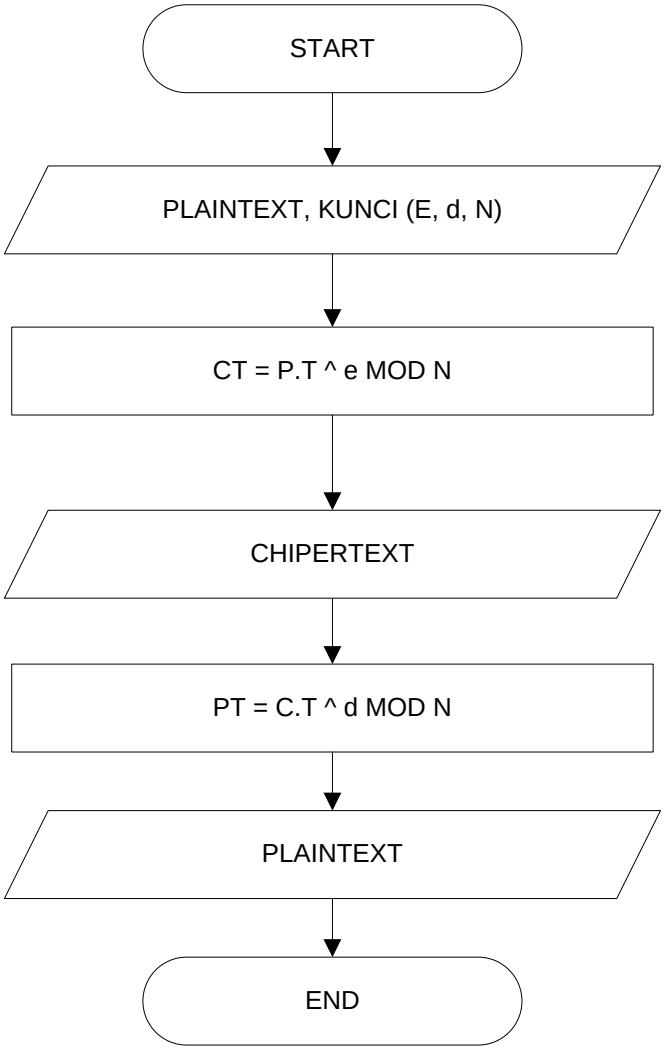
3.8 Flowchart Sistem

Flowchart merupakan langkah awal pembuatan program. Dengan adanya flowchart urutan proses kegiatan menjadi lebih jelas. Bila terdapat penambahan proses maka dapat dilakukan lebih mudah. Setelah flowchart selesai disusun,selanjutnya pemrogram (programmer) menerjemahkannya ke bentuk program dengan bahasa pemrograman.

Flowchart merupakan urutan-urutan langkah kerja suatu proses yang digambarkan dengan menggunakan simbo -simbol yang disusun secara sistematis.(Iswandy, 2015)

3.9 Flowchart *RSA*

Flowchart RSA yang digunakan oleh pengirim untuk mengenkripsi dan mendeskripsi plaintext hingga mendapatkan ciphertext digambarkan sebagai berikut:

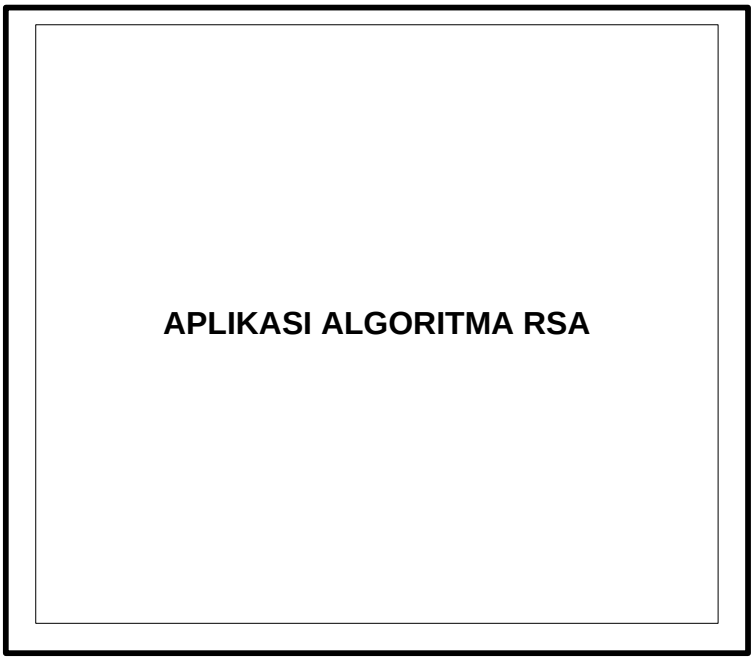


Gambar 3.3 Flowchart RSA

3.8 Perancangan Antarmuka

1. Rancangan Halaman Judul

   Halaman judul merupakan halaman yang pertama muncul pada saat program dijalankan

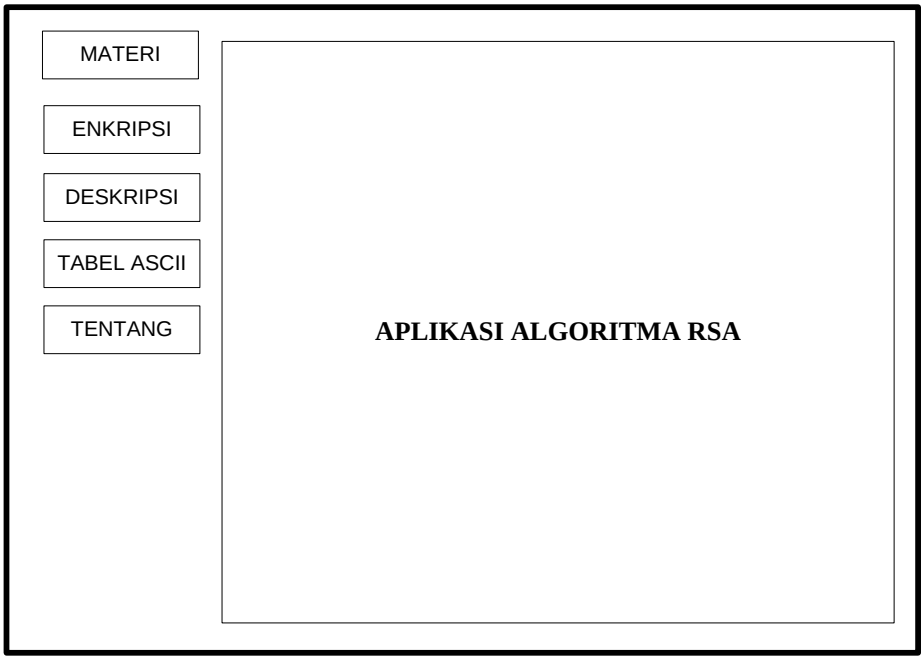


Gambar 3.4 Rancangan Halaman Judul

   Pada rancangan di atas akan menampilkan judul yang kemudian akan pindah ke form menu utama dengan menggunakan timer.

2. Rancangan Halaman Menu Utama

   Form ini berisi tombol-tombol seperti menu Materi, Enkripsi, Deskipsi, tentang, dan Keluar.



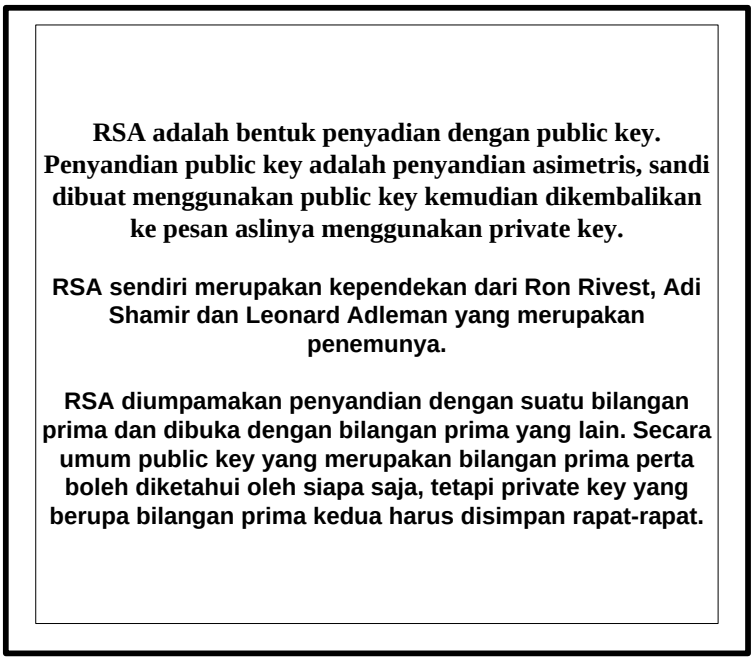
Gambar 3.5 Rancangan Halaman Menu Utama

Pada tampilan di atas terdapat 5 tombol yaitu Materi, Enkripsi, Deskripsi, Tabel Affine, Tentang dan keluar.

- Tombol Materi berfungsi untuk menghubungkan pengguna ke form materi.
- Tombol Enkripsi berfungsi untuk menghubungkan pengguna ke form Enkripsi.
- Tombol Deskripsi berfungsi untuk menampilkan form Deskripsi.
- Tombol Tentang berfungsi untuk menghubungkan pengguna ke form tentang.
- Tombol Keluar berfungsi untuk keluar dari program.

3. Rancangan Halaman Materi

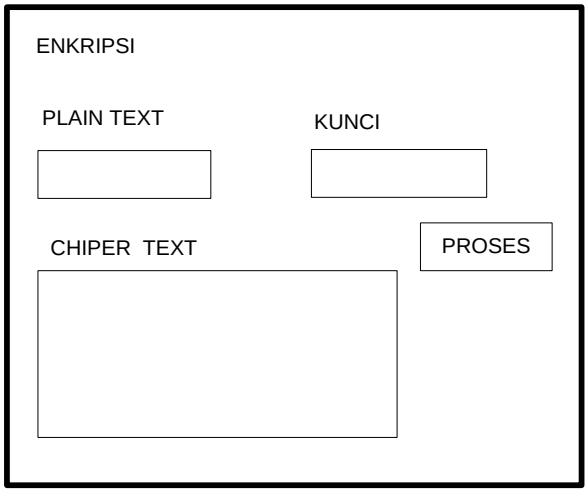
Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.



Gambar 3.6 Rancangan Halaman Materi

4. Rancangan Halaman Enkripsi

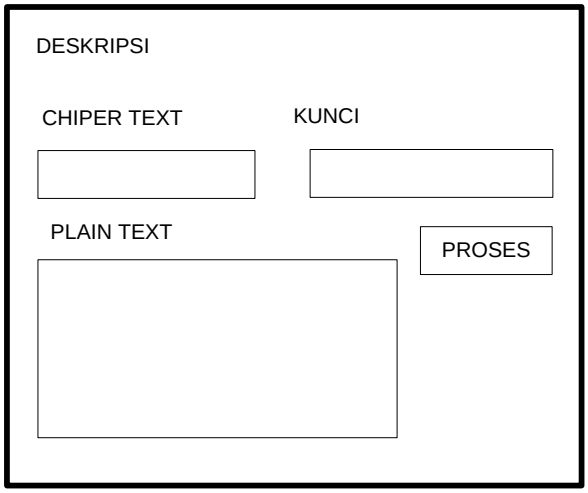
Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.



Gambar 3.7 Rancangan Halaman Enkripsi

5. Rancangan Halaman Deskripsi

   Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.



Gambar 3.8 Rancangan Halaman Deskripsi

Pada gambar di atas terdapat kotak input Deskripsi berfungsi untuk memasukkan tulisan yang telah disandikan. Kemudian terdapat tombol Proses Deskripsi untuk mengembalikan ke tulisan asli jika kunci yang dimasukkan sama dengan kunci pada saat penggunaan plaintext.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pengujian Sistem

Pengujian dilakukan dengan memasukkan karakter atau huruf dari file berformat .txt selanjutnya diproses oleh aplikasi apakah aplikasi tersebut dapat memberikan hasil yang sesuai. Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma *RSA* antara pengirim kepada penerima dengan kunci yang dimiliki masing-masing pihak tanpa perlu bertukar kunci tunggal hingga pada akhirnya pesan asli yang dikirimkan oleh pengirim dapat dibaca oleh penerima .

1. Tampilan Awal/ Home

Tampilan pada gambar 4.1 merupakan tampilan awal ketika aplikasi dijalankan. Pada form ini pengguna dapat memilih untuk membuka beberapa form lainnya seperti tombol tentang yang akan mengarahkan pengguna menuju form yang menjelaskan profil aplikasi ini, tombol *read me!* yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.

Gambar 4.1 Tampilan Awal/ Home

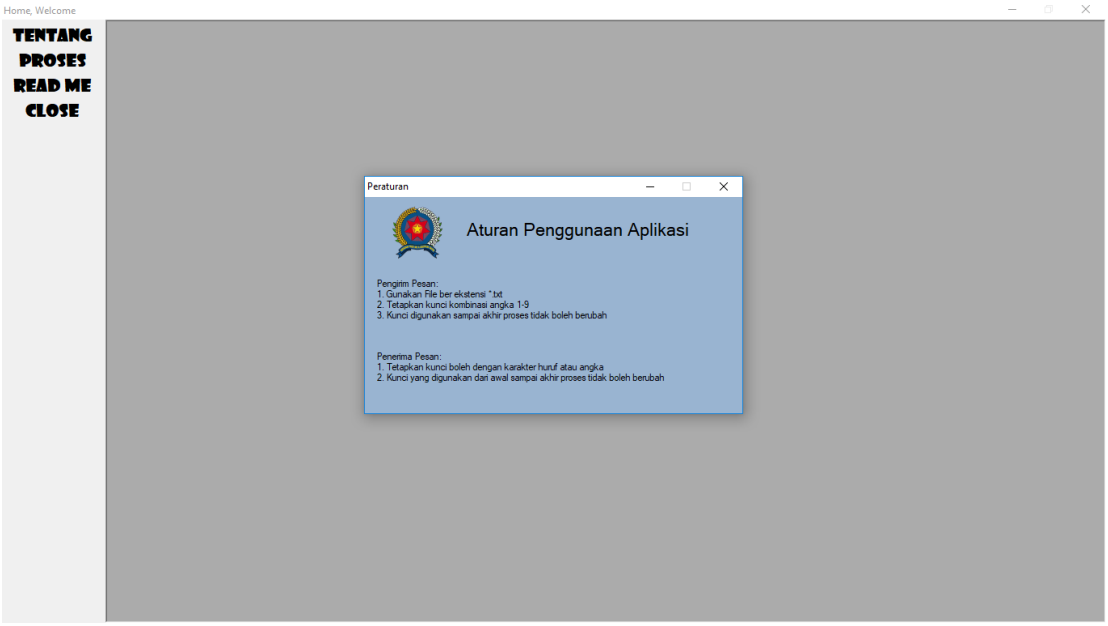
2. Tampilan Halaman Tentang

Tampilan berikut ini menampilakan halaman atau form yang berisi tentang profil dari aplikasi ini. Didalamnya terdapat judul dari aplikasi beserta maksud dari pembuatannya beserta nama dan nomor pokok mahasiswa penulis.

Gambar 4.2 Tampilan Halaman Tentang

3. Tampilan Aturan Penggunaan Aplikasi

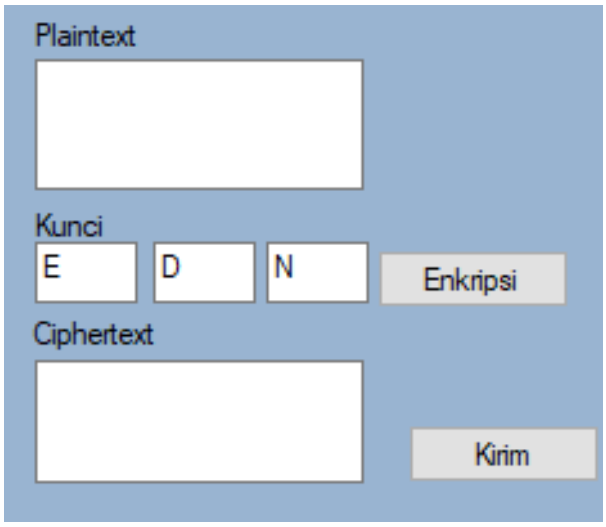
Tampilan aturan penggunaan aplikasi merupakan tampilan halaman atau form yang berisi tentang tata cara penggunaan aplikasi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma *RSA*.



Gambar 4.3 Tampilan Aturan Penggunaan Aplikasi

4. Tampilan Halaman Pengirim Pesan

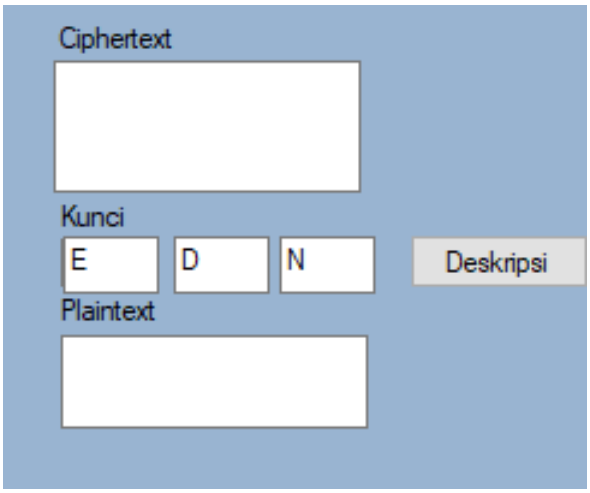
Tampilan berikut merupakan tampilan pengiriman pesan pada aplikasi ini. algoritma *RSA* merupakan protokol yang menjamin tidak adanya pertukaran kunci antara pihak-pihak yang melakukan enkripsi dan dekripsi. Kedua belah pihak menggunakan kunci mereka masing-masing untuk mengenkripsi pesan dan kemudian untuk mendekripsi pesan tanpa perlu mengetahui kunci yang lainnya



Gambar 4.4 Tampilan Halaman Pengirim Pesan

5. Tampilan Halaman Penerima Pesan

Tampilan berikut merupakan tampilan penerima pesan pada aplikasi ini.



Gambar 4.5 Tampilan Halaman Penerima Pesan

4.2 Hasil Enkripsi Pesan

Perhitungan Manual:

p = 3

q = 7

n = p.q

= 3 x 7

= 21

m = (p-1) (q-1)

= (3 -1)(7 – 1)

= 12

e * d mod 12 = 1

e = 5

d = 17

public key = (e,n) = (5,21)

private key = (d,n) = (17,21)

Plaintext:

T O M I

84 79 77 73

Proses Enkripsi dan Deskripsi	
T = 84	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
8 ^ 5 mod 21 = 8	8 ^ 17 mod 21 = 8
4 ^ 5 mod 21 = 16	16 ^ 17 mod 21 = 4

O = 79	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
7 ^ 5 mod 21 = 7	7 ^ 17 mod 21 = 7
9 ^ 5 mod 21 = 18	18 ^ 17 mod 21 = 9
M = 77	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
7 ^ 5 mod 21 = 7	7 ^ 17 mod 21 = 7
7 ^ 5 mod 21 = 7	7 ^ 5 mod 21 = 7
I = 73	
Enkripsi	Deskripsi
C = M ^ e mod n	M = C ^ d mod n
7 ^ 5 mod 21 = 7	7 ^ 17 mod 21 = 7
3 ^ 5 mod 21 = 12	12 ^ 17 mod 21 = 3

4.3 Pengujian Black Box

Perangkat lunak adalah elemen kritis dari jaminan kualitas perangkat lunak dan merepresentasikan kajian pokok dari spesifikasi, perancangan, dan pengkodean. Pengujian yang digunakan untuk menguji sistem ini adalah metode pengujian *black-box*. Pengujian *black-box* berfokus pada persyaratan fungsional perangkat lunak.

1. Rencana Pengujian

Pengujian fungsi Penerapan Matrix Persegi Pancajang Dalam Pengembangan Algoritma RSA dilakukan dengan menggunakan metode Black Box. Pengujian dilakukan pada fungsi-fungsi sistem untuk menentukan apakah fungsi tersebut telah berjalan sesuai dengan yang diharapkan.

1) Bangkitkan Kunci

Tabel 4.1 . Rencana Pengujian Tombol Cari

Menu yang diuji	**Detail pengujian**	**Kesimpulan**
Bangkitkan Kunci	Melakukan random kunci pada proses RSA.	*Diterima*

2) Proses Enkripsi

Tabel 4.2. Rencana Pengujian Pengguna (*User*)

Menu yang diuji	**Detai pengujian**	**Jenis uji**
Proses	Melakukan proses enkripsi	*Diterima*
Kirim	Proses pengiriman file enkripsi	*Diterima*
Clear All	Menghapus seluruh text yang ada pada text box	*Diterima*

3) Proses Deskripsi

Tabel 4.3. Rencana Pengujian Pengguna (*User*)

Menu yang diuji	**Detai pengujian**	**Jenis uji**
Dekripsi	Melakukan proses deskripsi atau pengembalian pesan asli	*Diterima*
Close	Menutup semua program	*Diterima*
Clear All	Menghapus seluruh text yang ada pada text box	*Diterima*

2. Pengujian Proses

Pengujian proses yang telah disusun, maka dapat dilakukan pengujian sebagai berikut :

Tabel 4.4. Proses Pengujian Enkripsi dan Deskripsi (*User*)

Data Pengujian Proses					Hasil
Nomor	**Isi Pesan**	**Kunci**	**Enkripsi**	**Deskripsi**	
1	TOMI	p = 3 q = 7	16 18 7 12	TOMI	Berhasil

3. Kesimpulan Dan Hasil Pengujian Sistem

Hasil pengujian dari pengujian alpha telah selesai, menunjukkan bahwa sistem sudah memenuhi syarat fungsional. Secara fungsional sistem yang sudah dibangun sudah dapat menghasilkan keluaran sesuai yang diharapkan.

Tabel 4.5. Kesimpulan Pengujian Alpha

Nama fungsi	**Hasil**
Tombol Cari	Fungsi berjalan dengan baik
Proses	Fungsi berjalan dengan baik
Enrkipsi	Fungsi berjalan dengan baik
Deskripsi	Fungsi berjalan dengan baik
Clear All	Fungsi berjalan dengan baik

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan dalam perancangan Penerapan Algoritma *RSA* dalam Meningkatkan Keamanan Data, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengiriman pesan berekstensi yang diinputkan kedalam *textbox* antara pengirim dan penerima.
2. Pengirim mengirimkan pesan menggunakan dua kunci yang ditentukan sendiri oleh pengirim.
3. Penerima pesan menggunakan kunci yang diberikan oleh pengirim pesan, agar bisa membuka pesan asli yang dikirimkan oleh pengirim.

5.2 Saran

Adapun saran-saran yang dapat dilakukan penelitian ataupun pengembangan selanjutnya adalah sebagai berikut:

1. Diharapkan adanya kombinasi algoritma keamanan data lainnya.
2. Proses pengamanan data yang dilakukan oleh penulis masih menggunakan visual studio, diharapkan ada yang menggunakan diandroid agar bisa digunakan pada mobile.

DAFTAR PUSTAKA

Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." Seminar Nasional Informatika (SNIf). Vol. 1. No. 1. 2017.

Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In IOP Conference Series: Materials Science and Engineering (Vol. 300, No. 1, p. 012067). IOP Publishing.

Dr. Kusnendi, M. S. (2014). Konsep Dasar Sistem Informasi. In *Konsep Dasar Sistem Informasi*.

Fachri, Barany. Aplikasi Perbaikan Citra Efek Noise Salt & Papper Menggunakan Metode Contraharmonic Mean Filter. In: Seminar Nasional Royal (Senar). 2018. P. 87-92.

Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.

Hafni, Layla, And Rismawati Rismawati. "Analisis Faktor-Faktor Internal Yang Mempengaruhi Nilai Perusahaan Pada Perusahaan Manufaktur Yang Terdaftar Di Bei 2011-2015." Bilancia: Jurnal Ilmiah Akuntansi 1.3 (2017): 371-382.

Hamdi, Muhammad Nurul, Evi Nurjanah, And Latifah Safitri Handayani. "Community Development Based Onibnu Khaldun Thought, Sebuah Interpretasi Program Pemberdayaan Umkm Di Bank Zakat El-Zawa." El Muhasaba: Jurnal Akuntansi (E-Journal) 5.2 (2014): 158-180.

Indra Permana, Aminuddin "Sistem Pakar Mendeteksi Hama Dan Penyakit Tanaman Kelapa Sawit Pada Pt. Moeis Kebun Sipare-Pare Kabupaten Batubara." (2013).

Jogiyanto. (2017). Konsep Dasar Sistem Informasi. *Konsep Dasar Sistem Informasi*.

Kadir, A. (2014). Pengertian Sistem Informasi Menurut Abdul Kadir. In *Pengenalan Sistem Informasi Edisi Revisi*.

Kosasih, S. (2015). Sistem Informasi Geografis Pemetaan Tempat Kost Berbasis Web. *CSRID (Computer Science Research and Its Development Journal)*. https://doi.org/10.22303/csrid.6.3.2014.171-181

Kristiyanti, M. (2016). Rancang Bangun Prototype Berbasis WEB Sebagai Implementasi Praktik Wirausaha Mahasiswa di Kota Semarang. *Jurnal Ekonomi Dan Bisnis*. https://doi.org/10.24914/jeb.v17i2.266

Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." Int. J. Recent Trends Eng. Res 2.12 (2016): 140-151.

Nugroho, B. (2014). Dasar Pemrograman Web PHP-MySQL dengan Dreamweaver. *Gava Media*. https://doi.org/10.1016/0378-1119(87)90155-7

Permana, A. I., and Z. Tulus. "Combination of One Time Pad Cryptography Algorithm with Generate Random Keys and Vigenere Cipher with EM2B KEY." (2020).

Permana, Aminuddin Indra. "Kombinasi Algoritma Kriptografi One Time Pad dengan Generate Random Keys dan Vigenere Cipher dengan Kunci EM2B." (2019).

Puspita, Khairani, and Purwa Hasan Putra. "Penerapan Metode Simple Additive Weighting (SAW) Dalam Menentukan Pendirian Lokasi Gramedia Di Sumatera Utara." Seminar Nasional Teknologi Informasi Dan Multimedia, ISSN. 2015.

Putera, A., Siahaan, U., & Rahim, R. (2016). Dynamic key matrix of hill cipher using genetic algorithm. Int. J. Secur. Its Appl, 10(8), 173-180.

Putra, D., & Akuntansi, J. (2014). Sistem Informasi Info Pelanggan Berbasis Android. *Skripsi, Fakultas Ilmu Komputer*.

Rizal, Chairul. "Pengaruh Varietas dan Pupuk Petroganik Terhadap Pertumbuhan, Produksi dan Viabilitas Benih Jagung (Zea mays L.)." ETD Unsyiah (2013).

Sisilia, S. J., Ardiansyah, R., & Inayatullah. (2017). SISTEM INFORMASI BODYBUILDING. *JATISI*.

Syahputra, Rizki, And Hafni Hafni. "Analisis Kinerja Jaringan Switching Clos Tanpa Buffer." Journal Of Science And Social Research 1.2 (2018): 109-115.

The World Wide Web Foundation.

The World Wide Web Foundation. (2015). Open Data Barometer - Global Report.

Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." Jurnal Abdi Ilmu 10.2 (2018): 1899-1902.