PENGAMANAN PESAN RAHASIA MENGGUNAKAN ALGORITMA KRIPTOGRAFI RSA

Skripsi

untuk memenuhi sebagian persyaratan mencapai derajat Sarjana S-1

Program Studi Matematika

Disusun Oleh:

Jajang Nurjaman

08610044

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2012

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Jajang Nurjaman
NIM : 08610044
Judul Skripsi : Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi RSA

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam bidang Matematika.

Dengan ini saya mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya saya ucapkan terima kasih.

Yogyakarta, Oktober 2012
Pembimbing I

M. Abrori, S.Si, M.Kom.
NIP. 19720423 199903 1 003

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Jajang Nurjaman
NIM : 08610044
Judul Skripsi : Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi RSA

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam bidang Matematika.

Dengan ini saya mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya saya ucapkan terima kasih.

Yogyakarta, Oktober 2012
Pembimbing II

M. Zaki Riyanto, S.Si, M.Sc.
NIDN. 0513018402

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/3464/2012

Skripsi/Tugas Akhir dengan judul : Pengamanan Pesan Rahasia menggunakan Algoritma Kriptografi RSA

Yang dipersiapkan dan disusun oleh :
Nama : Jajang Nurjaman
NIM : 08610044
Telah dimunaqasyahkan pada : 24 Oktober 2012
Nilai Munaqasyah : A

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Mochammad Abrori,S.Si,M.Kom
NIP. 19720423 199903 1 003

Penguji I

Muhammad Wakhid Musthofa, M.Si
NIP.19800402 200501 1 003

Penguji II

Mahmudi, S.Si., M.Si

Yogyakarta, 25 Oktober 2012
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : Jajang Nurjaman

NIM : 08610044

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Menyatakan dengan sesungguhnya bahwa skripsi ini merupakan hasil pekerjaan penulis sendiri dan sepanjang pengetahuan penulis tidak berisi materi yang dipublikasikan atau ditulis orang lain, dan atau telah digunakan sebagai persyaratan penyelesaian Tugas Akhir di Perguruan Tinggi lain, kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, Oktober 2012

Yang menyatakan

Jajang Nurjaman

NIM. 08610044

HALAMAN MOTTO

“Musuh yang paling berbahaya di atas dunia ini adalah penakut dan bimbang. Teman yang paling setia, hanyalah keberanian dan keyakinan yang teguh”.

(Andrew)

“Berani tidak dikenal”

(dr. Roebiono Kertopati)

"Jangan pernah sekali pun berpikir bagaimana caranya untuk bisa menang, tapi berpikirlah bagaimana caranya agar tidak kalah".

(Miyamoto Musashi)

HALAMAN PERSEMBAHAN

Tugas akhir ini penulis persembahkan untuk semua orang yang telah membantu dan memberikan inspirasi kepada penulis dalam menyelesaikan tugas akhir ini :

- Dengan cinta dan terima kasih penulis persembahkan karya ini kepada ayahanda dan ibunda tercinta yang telah bekerja keras untuk membiayai dan mencurahkan kasih sayangnya, serta menjadi modal semangat saat dalam kebimbangan belajar. Untuk kakak dan keponakan penulis yang selalu menjadi motivasi dan penepis sepi.
- Kepada semua bapak dan ibu guru, penulis haturkan terima kasih dari hati yang terdalam atas jasa dan pengabdiannya yang tulus ketika membimbing penulis dalam menuntut ilmu.
- Kepada semua bapak dan ibu dosen Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta, penulis haturkan terima kasih atas jasa dan pengabdiannya yang tulus dalam membimbing penulis.
- Tugas akhir ini penulis persembahkan kepada almamater tercinta Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

KATA PENGANTAR

Alhamdulillah segala puji syukur penulis haturkan kepada sang Ilahi Robbi Allah SWT. yang selalu melimpahkan rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir ini yang berjudul "Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi RSA".

Shalawat dan Salam semoga tercurah limpahkan kepada junjungan kita Nabi Muhammad SAW. sebagai manusia mulia pilihan yang telah memberikan sinar terang menuju jalan kehidupan yang di ridhai Allah.

Penulis menyadari bahwa dalam proses penyusunan skripsi ini banyak mendapatkan bimbingan, arahan dan bantuan baik moral maupun material dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Bapak Prof. Drs. Akh. Minhaji, M.A.,Ph.D. selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Ibu Dra. Khurul Wardati, M.Si. selaku Pembantu Dekan I Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Bapak M. Abrori, S.Si, M.Kom. selaku Ketua Program Studi Matematika dan selaku Dosen Pembimbing yang telah bersedia meluangkan pikiran dan waktu demi terselesaikannya penulisan tugas akhir.
4. Bapak M. Zaki Riyanto, S.Si, M.Sc. selaku Dosen Pembimbing yang telah bersedia meluangkan pikiran, waktu, serta memberikan pemahaman tentang dunia kriptografi hingga terselesaikannya penulisan tugas akhir ini.
5. Bapak Farhan Qudratullah, M.Si selaku Dosen Penasehat Akademik Program Studi Matematika yang telah memberikan motivasi dan pengarahan kepada penulis.
6. Semua Dosen Fakultas Sains dan Tekhnologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta yang telah memberikan wawasan dan ilmunya kepada penulis sebagai bekal di masa depan.

7. Ayahanda dan Ibunda tersayang, serta kakak-kakak tercinta yang selalu memberikan semangat, dan doa kepada penulis setiap hari.
8. Teman-teman Matematika 2008 yang selalu memberi semangat, semoga tali silaturahmi kita tetap terjaga, dan semoga kesuksesan menyertai kita semua.
9. Segenap pihak yang telah membantu penulis dari pembuatan proposal, sampai terselesaikannya penulisan skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari sepenuhnya bahwa karya ini masih sangat jauh dari kesempurnaan, oleh karena itu, penulis sangat mengharapkan kritik dan saran yang bersifat membangun demi menambah kesempurnaan tulisan ini. Harapan penulis semoga karya ini dapat memberikan manfaat dan sumbangan bagi kemajuan dan perkembangan ilmu pengetahuan terutama dalam bidang kriptografi.

Yogyakarta, 4 Oktober 2012

Penulis

Jajang Nurjaman

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ALGORITMA

ARTI LAMBANG

$x \in Z$	: x elemen bilangan bulat
$x \notin Z$	: x bukan elemen bilangan bulat
$A \subseteq X$	: A himpunan bagian (subset) atau sama dengan X
$\emptyset$	: Himpunan kosong
$\mathbb{Z}$	: Himpunan bilangan bulat
$\mathbb{R}$	: Himpunan bilangan real
$\mathbb{N}$	: Himpunan bilangan asli
$\Rightarrow$	: Jika maka
$\Leftrightarrow$	: Jika dan hanya jika
$\longrightarrow$	: Menuju
■	: Akhir sebuah bukti
$\sum_{i=1}^{n} a_i$	: Penjumlahan $a_1 + a_2 + \cdots + a_n$
$\prod_{i=1}^{n} a_i$	: Perkalian $a_1 . a_2 . \ldots . a_n$
C_r^n	: r kombinasi dari n unsur yang berbeda
$x \leftarrow a$	: Nilai a dimasukan ke dalam x

ABSTRAK

PENGAMANAN PESAN RAHASIA

MENGGUNAKAN ALGORITMA KRIPTOGRAFI RSA

Oleh :

Jajang Nurjaman

08610044

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika dalam mengamankan suatu informasi atau pesan asli (*Plainteks*) menjadi sebuah teks tersembunyi (*Cipherteks*) dan kemudian diubah menjadi pesan asli kembali. Kriptografi mempunyai tiga unsur penting yaitu pembangkitan kunci, enkripsi, dan dekripsi. Dalam kriptografi dikenal Algoritma kriptografi RSA yang ditemukan pada tahun 1978 oleh R. Rivest, A. Shamir, dan L. Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut.

Algoritma kriptografi RSA merupakan suatu sistem kriptografi yang bekerja pada himpunan bilangan bulat modulo *m* atau biasa ditulis Z*m*, dengan *m* adalah suatu bilangan hasil kali dari dua bilangan prima ganjil yang berbeda misalkan *p* dan *q*, sehingga diperoleh $m = p \times q$. Dalam sistem ini, himpunan *plainteks* dan *cipherteks* diambil dari himpunan Z*m*, sehingga keamanan sandi RSA terletak pada sulitnya memfaktorkan bilangan bulat *m* yang sangat besar.

Skripsi ini bertujuan untuk menerapkan algoritma RSA yang digunakan dalam proses enkripsi dan dekripsi dengan *Metode Fast Exponentation*, beserta konsep-konsep matematis yang melandasinya seperti teori bilangan dan teori aljabar. Kemudian dibuat sebuah program pengamanan pesan rahasia yang sederhana berdasarkan algoritma RSA dan tanda tangan digital RSA.

Kata kunci : Algoritma, Aljabar, Asimetris, RSA, Tanda Tangan Digital, Kriptografi, Kunci Publik.

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan ilmu pengetahuan sangat berpengaruh terhadap perkembangan teknologi. Salah satu teknologi yang sedang berkembang pesat adalah teknologi informasi yang ditandai dengan kemudahan untuk mencari suatu informasi dengan cepat dan murah tanpa harus memperhatikan batasan ruang dan waktu. Sehingga dalam hitungan menit ataupun detik, kita dapat mengetahui informasi dari suatu negara atau benua lain.

Di era teknologi internet sekarang ini, semua informasi dapat dikirim dengan bebas melalui suatu jaringan dengan tingkat keamanan yang rentan dan memungkinkan terjadinya penyadapan suatu informasi. Hal tersebut secara langsung maupun tidak langsung mempengaruhi sistem perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan yang umumnya mengandung informasi rahasia. Kasus bocornya data rahasia intelijen pemerintah Amerika Serikat bahkan dunia, tak terkecuali data rahasia intelijen pemerintah Indonesia oleh Wikileaks, merupakan salah satu contoh bahwa penyadapan informasi bisa terjadi di mana saja dan oleh siapa saja.

Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia. Faktor utama yang harus dipenuhi dalam mengamankan data rahasia adalah tingkat keamanan teknologi informasi yang tinggi. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-

kode yang tidak dimengerti sehingga penyadap akan kesulitan untuk mengetahui isi informasi yang sebenarnya.

Kriptografi merupakan sebuah studi matematis yang terkait dengan aspek-aspek yang berhubungan dengan keamanan informasi seperti bagaimana menyembunyikan isi data, mencegah data dirubah tanpa terdeteksi, ataupun mencegah data digunakan tanpa otorisasi yang cukup. Orang yang melakukan peroses kriptografi disebut sebagai *Kriptografer*. Kebalikan dari kriptografi adalah *Kriptoanalisis*, yaitu seni dan ilmu untuk memecahkan *Chiperteks* menjadi *Plainteks* tanpa melalui cara yang seharusnya dan orangnya disebut sebagai Kriptoanalis (Menezes dkk,1996: 4).

Salah satu algoritma kriptografi yang di bahas dalam tugas akhir ini adalah Algoritma Kriptografi RSA, ditemukan pertama kali pada tahun 1978 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA itu sendiri merupakan singkatan dari inisial nama mereka bertiga. RSA termasuk dalam algoritma kriptografi asimetris yang mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Sampai saat ini, Algoritma kriptografi RSA merupakan salah satu yang paling maju dalam bidang kriptografi kunci dan banyak digunakan karena kehandalannya yaitu algoritma pertama yang cocok untuk tanda tangan digital (*Digital Signature*).

Tanda tangan digital merupakan suatu tanda tangan (penanda) yang dibubuhkan pada data digital. Tanda tangan digital bukan merupakan hasil scan atau input tanda tangan melalui *interface* tertentu. Tanda tangan digital adalah suatu nilai kriptografis yang bergantung pada isi data itu sendiri serta kunci yang

digunakan untuk membangkitkan nilai kriptografisnya. Sehingga nilai setiap tanda tangan digital dapat selalu berbeda tergantung data yang ditandatangani.

Tanda tangan digital yang dibubuhkan ke dalam suatu data dapat memvalidasi dari mana data tersebut berasal. Tanda tangan ini memberi rasa aman kepada penerima data karena ia dapat mengetahui siapa yang mengirim data tersebut. Tanda tangan yang valid saat diotentikasi ulang juga menjamin bahwa data yang dikirim tidak mengalami perubahan atau modifikasi selama proses pengiriman.

1.2. Rumusan masalah

Berdasarkan latar belakang yang telah di uraikan, maka yang menjadi rumusan masalah pada penulisan tugas akhir ini adalah :

1. Konsep-konsep matematis yang melandasi pembentukan algoritma kriptografi RSA.
2. Cara kerja algoritma kriptografi RSA dan aplikasinya dalam tanda tangan digital.
3. Proses penyandian serta implementasi algoritma RSA dalam sebuah program komputer yang sederhana.

1.3. Batasan Masalah

Sesuai dengan judul tugas akhir ini, maka pembahasan akan lebih di fokuskan pada algoritma RSA yang merupakan bagian dari kunci publik. Adapun yang menjadi pembatasan masalah adalah sebagai berikut:

1. Pembahasan mengenai algoritma RSA ini meliputi, konsep matematis yang melandasinya, seperti konsep teori aljabar yang meliputi grup dan ring untuk memudahkan pemahaman mengenai algoritma RSA.
2. Membahas proses penyandian pesan yang meliputi proses pembentukan kunci, proses enkripsi dan proses dekripsi serta implementasinya dalam sebuah program sederhana.
3. Pada tugas akhir ini pembahasan implementasi RSA pada tanda tangan digital hanya meliputi konsep teoritis dan tidak membahas mengenai cara-cara untuk memecahkan mekanisme penyandian (Kriptanalisis Algoritma RSA).
4. Aplikasi pengamanan data dibuat dengan menggunakan bahasa pemrograman C++.

1.4. Tujuan Penulisan

Tujuan yang ingin di capai dalam pembuatan tugas akhir ini adalah

1. Mengenalkan konsep matematis yang melandasi pembentukan algoritma kriptografi RSA beserta penerapannya pada tanda tangan digital.
2. Dapat menentukan kunci publik dan kunci rahasia dari algoritma kriptografi RSA. Serta dapat melakukan proses Enkripsi dan Dekripsi pada algoritma kriptografi RSA.
3. Dapat membuat program aplikasi komputer yang dapat melakukan proses Enkripsi dan Dekripsi sesuai dengan algoritma RSA. program aplikasi

komputer tersebut hanya sebagai contoh aplikasi dalam mengamankan sebuah pesan rahasia.

1.5. Tinjauan Pustaka

Penelitian mengenai kriptografi telah banyak dilakukan oleh para ahli dalam bidang penyandian. Penelitian itu telah menghasilkan banyak algoritma penyandian baru dengan efektifitas dan keamanan yang lebih baik. Tetapi masih sangat sedikit sekali yang membahas secara mendetail tentang konsep matematisnya.

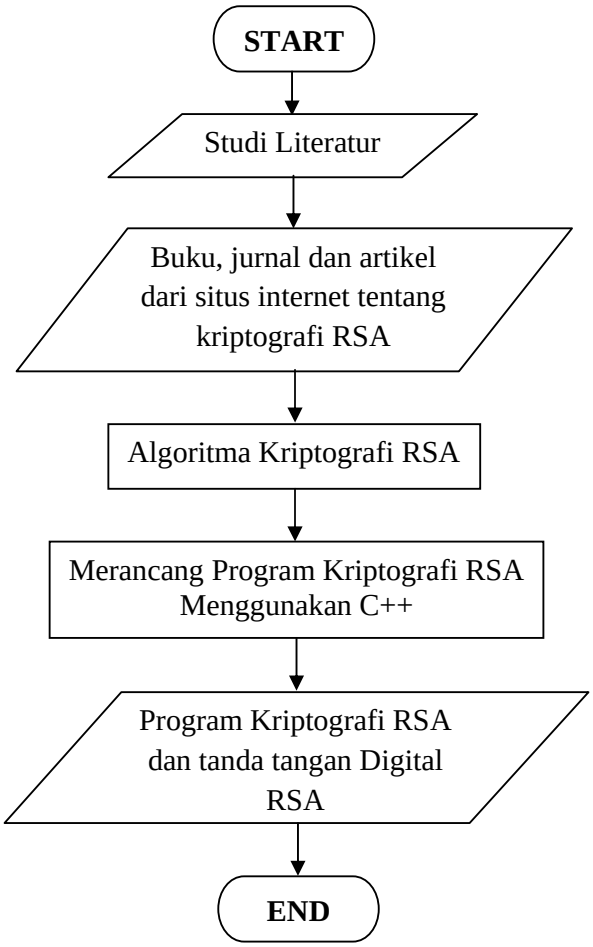
Referensi utama penulisan skripsi ini adalah artikel Kelompok Studi Sandi Yogyakarta yang di tulis oleh M. Zaki Riyanto dan Ardhi Ardhian pada tahun 2008 berjudul *Kriptografi Kunci Publik: Sandi RSA* sangat menarik untuk diteliti karena pada beberapa bagian telah dilengkapi dengan penjelasan mengenai proses enkripsi maupun dekripsi pada algoritma RSA. Selain itu, Jurnal teknik informatika yang di tulis oleh Rinaldi Munir yang berjudul *Penggunaan Tanda Tangan Digital Untuk Menjaga Integritas Berkas Digital* menjadi referensi kedua pada tugas akhir ini karena sebagai sarana pengembangan sistem kriptografi pada tanda tangan digital.

Selain itu beberapa buku kriptografi, tugas akhir mahasiswa S1, artikel situs internet yang berkaitan dengan kriptografi RSA sebagai bahan referensi tambahan pada pembuatan tugas akhir ini.

1.6. Metode Penelitian

Metode yang digunakan pada pembuatan tugas akhir ini adalah metode studi literatur mengenai algoritma RSA pada beberapa buku kriptografi, jurnal, maupun artikel dalam situs internet yang berhubungan dengan RSA. Kemudian penulis mengambil beberapa materi yang menjelaskan algoritma RSA dan membahasnya, langkah terakhir adalah melakukan perancangan dan menerapkan algoritma tersebut pada C/C++ untuk membuat program aplikasi penyandian tersebut.

1.6.1. Flowchart Metode Penelitian



1.7. Sistematika Penulisan

Dalam tugas akhir ini pembahasan materi akan disusun menjadi empat bab. Materi tersebut adalah sebagai berikut :

BAB I : Pendahuluan

Bab ini membahas mengenai latar belakang, perumusan masalah, batasan masalah, tujuan penulisan tugas akhir, tinjauan pustaka, metode penelitian, serta sistematika penulisan tugas akhir.

BAB II : Landasan Teori

Pada bab ini dibahas mengenai tiga landasan teori, yaitu mengenai kriptografi, bilangan bulat, dan konsep matematika pada pembentukan algoritma RSA. Pada bagian kriptografi akan diberikan definisi, dan algoritma kriptografi. Sedangkan pada bilangan bulat akan dibahas mengenai sifat-sifat menguntungkan yang dimiliki bilangan bulat seperti divisibilty, algoritma pembagian bilangan bulat, pembagi persekutuan terbesar, algoritma Euclid, algoritma Euclid yang diperluas, grup, homomorfisma grup, isomorfisma grup dan ring. Selain itu, terdapat konsep matematika pada algoritma RSA seperti persamaan kongruen, *residue clas ring*, pembagian pada residue clas ring, order elemen-elemen grup, *multiplicative grup residue*, teorema fermat, *metode fast exponention*, tes keprimaan dengan tes Miller-Rabin.

Bab III : Pembahasan

3.1. Algoritma RSA dan Tanda Tangan Digital RSA

Pada sub bab ini akan dibahas proses kerja algoritma RSA yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi, serta contoh kasus penggunaannya.

3.2. Tanda Tangan Digital RSA

Pada sub bab ini akan dibahas proses kerja tanda tangan digital RSA mulai dari pembentukan kunci, pembentukan nilai hash, proses tanda tangan digital, dan verifikasi tanda tangan digital, serta contoh kasus penggunaannya.

3.3. Implementasi dan Hasil Uji Coba

Sub bab ini mengulas mengenai langkah-langkah pembuatan program penyandian data menggunakan algoritma RSA, beserta hasil uji coba program tersebut.

Bab IV : Penutup

Bab ini berisi kesimpulan dan saran.

BAB IV

PENUTUP

4.1. Kesimpulan

Setelah menyelesaikan penyusunan Tugas Akhir ini, maka penulis dapat menarik beberapa kesimpulan yaitu:

1. Untuk algoritma kriptografi asimetris, seperti algoritma kriptografi RSA, sangat baik untuk mengatasi masalah distribusi kunci.
2. Secara komputasi, teknik enkripsi dan dekripsi pesan dengan algoritma kriptografi RSA memerlukan waktu eksekusi yang lebih lama, terutama jika menggunakan nilai pembangun kunci yang cukup besar. Sehingga, hal tersebut mengakibatkan algoritma RSA kurang efisien dan efektif untuk memperoses data yang cukup besar.
3. Untuk tetap menjaga keautentikan cipherteks ketika dalam proses perjalanan pengiriman, maka cipherteks tersebut harus dibubuhkan tanda tangan digital sebagai bukti pesan tersebut masih utuh. Dalam proses tanda tangan digital, terdapat fungsi hash yang melandasinya. Fungsi hash yang digunakan dalam tugas akhir ini adalah fungsi hash dengan metode penjumlahan nilai setiap karakter pada plainteks.
4. Bahasa yang digunakan untuk pembuatan program dalam tugas akhir ini adalah bahasa pemrograman C/C++. Program tersebut merupakan simulasi dasar seperti proses pembentukan kunci, proses enkripsi, proses dekripsi, proses tanda tangan digital, dan proses verifikasi tanda tangan digital RSA.

Kemampuan program dalam tugas akhir ini masih terbatas, seperti proses pembentukan kunci hanya sampai 5 digit bilangan prima, serta data (pesan) yang bisa di proses oleh program ini merupakan pesan singkat.

4.2. Saran

Setelah membahas dan mengimplementasikan algoritma RSA pada tugas akhir ini, penulis ingin menyampaikan beberapa saran sebagai berikut berikut :

1. Nilai kunci yang digunakan sebaiknya sangat besar, untuk mengantisipasi terjadinya serangan terhadap nilai faktor *n*.
2. Diperlukan suatu metode untuk mempercepat proses enkripsi dan dekripsi dengan menggunakan nilai kunci yang sangat besar.
3. Untuk menjaga keamanan cipherteks hasil enkripsi algoritma RSA, maka kunci publik harus selalu dilindungi dari upaya penghapusan dan penggantian nilai kunci publik oleh orang yang tidak bertanggung jawab.
4. Diperlukan suatu antisipasi pada fungsi hash penjumlahan karakter terhadap serangan perubahan tata letak setiap karakter, yang akan menyebabkan nilai hash akan selalu sama dengan nilai tanda tangan digital saat verifikasi.
5. Diperlukan suatu langkah penyempurnaan untuk program tugas akhir ini, agar bisa memperoses enkripsi dan dekripsi data yang besar dengan cepat ketika menggunakan kunci bilangan prima yang besar.

Daftar Pustaka

Ariswan. 2008. *Konsep Dasar Matematika pada Algoritma Kriptografi RSA*. Skripsi. Yogyakarta: Fakultas Matematika dan Ilmu Pegetahuan Alam UGM.

Buchmann, Johannes A. 2000. *Introduction to Cryptography*. USA : Springer-Verlag New York, Inc.

Fraleigh, John B.. 2000, *A First Course in Abstract Algebra*, Sixth Edition, Addison-Wesley Publishing Company, Inc., USA.

Isnarto. 2005. *Struktur Aljabar*. Semarang: Fakultas Matematika dan Ilmu Pegetahuan Alam Universitas Negeri Semarang.

Jeffrey, Pipher, and Silverman. 2000. *An Introduction Mathematical Cryptography*. USA : Springer-Verlag New York, Inc.

Latuconsina, Roswan. 2006. *Fungsi Hash: Tiger (Sebuah Kajian dan Spesifikasi)*. Bandung: Institut Teknologi Bandung.

Menezes, Oorcshot, and Vanstone. 1996. *Handbook of Applied Cryptography*, USA : CRC Press, Inc.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika.

Munir, Rinaldi. 2006. *Penggunaan Tanda Tangan Digital Untuk Menjaga Integritas Berkas Perangkat Lunak*. Bandung : Institut Teknologi Bandung.

M. Zaki Riyanto, Ardhi Ardian. 2008. *Kriptografi Kunci Publik : Sandi RSA*. Yogyakarta: Kelompok Studi Sandi Yogyakarta.

Ngoen, Thompson S. 2006. *Pengantar Algoritma Dengan Bahasa C*. Jakarta : Salemba Teknika.

Riyanto, Muhamad Z. 2007. *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi ElGamal Atas Grup Pergandaan Zp**. Skripsi. Yogyakarta : Fakultas Matematika dan Ilmu Pegetahuan Alam UGM.

Setiawan, Ahmad Budi. *Implementasi Algoritma RSA dalam Pembuatan Sistem Kriptografi Tanda Tangan Digital. Paper*. Jakarta : Badan Litbang SDM Depkominfo.

Stinson, RD. 2006. *Cryptography Theory and Practice*. Canada : Chapman and Hall/CRC.

Schneier, Bruce. 1996. *Applied Cryptography, Second Edition : Protocol, Algorithms and Source Code in C*. John Wiley and Sons, Inc.

_____, 2012, *RSA Algorithm Using C* , http://cppgm.blogspot.com, 24 Mei 2012, 13:21.

LAMPIRAN 1.

1.1. Kode Program RSA

```
#include<stdio.h>
#include<conio.h>
#include <iostream.h>
#include <time.h>
#include <stdlib.h>

long int phi,M,e,d,C,FLAG;
long int a, b, c, t, w,md,xx,zz;
long int p,q,s,kp,kr,y,x,ans,ans2,n;
unsigned long long j,i,num,pow;
signed chp;
char ss[1000],dd[1000];
long v[1000],qq[1000];
char jawab;

long int tampprima()
{
long int x1,y1,c=0;
printf("**) Masukkan Dua Buah Bilangan Bulat Positif Sebagai Batas
Awal dan Batas Akhir\n    Sebuah Deret Bilangan Prima\n\n");
    printf("\n\n=> Silahkan masukkan nilai batas awal deret  =
    ");   scanf("%d",&y1);
    printf("\n");
    printf("=> Silahkan masukkan nilai batas akhir deret = ");
    scanf("%d",&x1);
    printf("\n\n\n");
printf("========================================================="
);
printf("\n|| Deret Bilangan Prima dari %d sampai %d\t
||\n",y1,x1);
printf("=========================================================\n\n"
);
    for(int i=y1;i<=x1;i++){
        for(int j=1;j<=i;j++){
            if(i % j == 0){
                c++;
            }
        }
    if(c == 2) printf("%d\t",i);
    c=0;
    }
    getch();
    cout<<"               "<<endl;
printf("\n=================================================\n\n")
;
    printf("**) Pilihlah Dua Buah Bilangan Bulat dari deret
diatas,\n    kemudian masukan kedalam konstanta p dan q pada menu
pembangkitan kunci !\n\n");
}


using namespace std;
```

```
unsigned long random(unsigned long f,unsigned long g)
{
    srand((unsigned long)time(NULL));
    return (unsigned long)(f+rand()%g);
}
 long PowMod(long x,long y,long g)
{
    long k, l, u;
    k=1; l=x; u=y;
    while(u){
        if(u&1)k=(l*k)%g;
        u>>=1;
        l=(l*l)%g;
    }
    return k;
}
long int RabinMillerKnl(unsigned long g)
{
    unsigned long B, f=g-1, j=0, v, i;
    while(!(f & 1)){
        ++j;
        f>>=1;
    }
    B=random(2,f);
    v=PowMod(B, f, g);
    if(v == 1)
        return 1;
    i=1;
    while(v != g - 1){
        if(i == j)
            return 0;
        v=PowMod(v, 2, g);
       i++;
    }
    return 1;
}
long int PrimeTestp()
{
unsigned long p;
    int TestNum=5;
    int count=0;
  op:
    cout<<"\n\n=> Masukan sembarang bilangan prima p =  ";
    cin>>p;

    for(int temp=0; temp < TestNum; temp++)
    {
        if (p%2==0)
        {
            if (p==2)
                count=TestNum;
            break;
        }
        if(RabinMillerKnl(p))
            count++;
        else
```

```
            break;
     }
          if(count==TestNum)
         {
printf("\n   >>> Hasil Tes :  %d adalah bilangan prima \n\n",p);
         }
    else
{
printf("\n ** >>> Hasil Tes : %d bukan bilangan prima \n\n
Silahkan masukan kembali nilai p !\n\n", p);
         goto op;}
 }
long int PrimeTestq()
 {
     unsigned long q;
     int TestNum=5;
     int count=0;
 oq :
     cout<<"\n\n=> Masukan sembarang bilangan prima q =  ";
     cin>>q;
     for(int temp=0; temp < TestNum; temp++)
     {
         if (q%2==0)
         {
             if (q==2)
                 count=TestNum;
             break;
         }
         if(RabinMillerKnl(q))
             count++;
         else
             break;
     }
     if(count==TestNum)
  printf("\n   >>> Hasil Tes :  %d adalah bilangan prima\n\n",q);
    else
    {
printf("\n  ** >>> Hasil Tes :  %d bukan bilangan prima, \n\n
Silahkan masukan kembali nilai q !\n\n",q);
     goto oq;}
 }
long int pembangkit(){
      pq:
      int  jum, i;
    cout<<"=> Masukan Bilangan Prima p = ";  //sebagai nilai p
    cin>>p;
    jum = 0;
    for (i=1; i<=p; i++)
    if (p%i==0) jum++;
    if (jum==2) {
    goto q;}
    else{
printf("\n ** maaf! nilai %d adalah bilangan composit,\n
silahkan masukan kembali bilangan prima lain ! \n\n",p);
     goto pq;
     }
```

```
q:
printf("\n\n");
cout<<"=> Masukan Bilangan Prima q = ";  //sebagai nilai q
cin>>q;
jum = 0;
for (i=1; i<=q; i++)
if (q%i==0) jum++;
 if (jum==2) {
  goto q2;}
 else{
 cout << "** maaf nilai p bukan bilangan prima, silahkan masukan
kembali bilangan prima lain ! \n";
 goto q;
 }
q2 :
      if (p==q){
printf("\n ** maaf nilai p tidak boleh sama dengan nilai q !\n");
      goto pq;}
      else
n = p*q;
printf("\n\n Nilai modulus :\n");
printf("\n\t\t\2\tn = %d * %d = %d \t\n",p,q,n);
if (n<250){
      printf("\n\a ** Maaf nilai n harus lebih besar dari 250,\n
Masukan kembali bilangan prima p dan q yang besar!\n\n");
      goto pq;}
phi=(p-1)*(q-1);
printf("\n Nilai  Totien :\n");
printf("\n\t\t\5\tF(n)= (%d - 1)*(%d - 1)= %d \t",p,q,phi);
cout<<"               "<<endl;
 }
long int gcd(int a, int b) {
  long int temp;
  while (b != 0) {
    temp = a % b;
    a = b;
    b = temp;
  }
  return(a);
}
long int eu () {

}
long int extended(int x,int y)
{
   long int a1=1,a2=0,a3=x,b1=0,b2=1,b3=y,q,t1,t2,t3;
abc:    if(b3==0)
    {
        return a3;
    }
    if(b3==1)
    {
        return b2;
    }
    q=(a3/b3);
    t1=a1-(q*b1);
```

```
    t2=a2-(q*b2);
    t3=a3-(q*b3);
    a1=b1;
    a2=b2;
    a3=b3;
    b1=t1;
    b2=t2;
    b3=t3;
    goto abc;
}
unsigned mod_powEnk(unsigned num,unsigned kp,unsigned n)
{
    unsigned long long test;
    unsigned long long nn = num;
    for(test = 1; kp; kp >>= 1)
    {
        if (kp & 1)
            test = ((test % n) * (nn % n)) % n;
              nn = ((nn % n) * (nn % n)) % n;
    }
        return test;
        }
unsigned mod_powEnk2(unsigned num,unsigned kp,unsigned n)
{
    unsigned long long test;
    unsigned long long nn = num;
    for(test = 1; kp; kp >>= 1)
    {
        if (kp & 1)
            test = ((test % n) * (nn % n)) % n;
        nn = ((nn % n) * (nn % n)) % n;
    }
    return test;
    }
unsigned mod_powEnk3(unsigned num,unsigned kp,unsigned n)
{
    unsigned long long test;

    unsigned long long nn = num;
    for(test = 1; kp; kp >>= 1)
    {
        if (kp & 1)
            test = ((test % n) * (nn % n)) % n;
        nn = ((nn % n) * (nn % n)) % n;
    }
        return test;
        }
unsigned    Enkripsi3 (){
      signed long long pow=ans;

cout<<"======================================================"<<endl
;
      cout<<"=\tSilahkan Ketikan Pesan (Tanpa Spasi)\t   ="<<endl;
cout<<"======================================================"<<endl
;
   printf("\nPesan : ");scanf("%s",&ss);
```

```
   for (i = 0 ; ss[i] !=0; i++)
   v[i] = (ss[i]);
  printf("\n Nilai ASCII nya : \n\n");
     for (j = 0; j < i; j++){
     printf("\t%c = %d\t", v[j],v[j]);
     int num=v[j];
        }
    printf("\n\n=> jumlah karakter yang diketik = %d\n\n",j);
    cout<<"               "<<endl;
    cout<<"==================================="<<endl;
    cout<<"=\tPeroses Enkripsi\t   ="<<endl;
    cout<<"==================================="<<endl;
    printf("\n");
    printf("\n\1 masukan Kunci Publik : "); scanf("%d",&kp);
    printf("\n\2 masukan nilai modulo: "); scanf("%d",&n);
    printf("\n **) Nilai Chiperteksnya adalah :\n\n");
    cout<<" +--------------------------------------+"<<endl;
    cout<<" +--------------------------------------+\n"<<endl;
       for (j = 0; j < i; j++){
       unsigned long long num=v[j];
       qq[j]=mod_powEnk3(v[j],kp,n);
    printf("  ");
    printf("%d\t", qq[j]);
      }
      {
       cout<<"\n\n +-----------------------------------+"<<endl;
       cout<<" +-----------------------------------+\n"<<endl;
       printf("\n\n");
      }
}
unsigned mod_powDek2(unsigned num, unsigned pow, unsigned mod)
{
    unsigned long long test;
    unsigned long long n = num;
    for(test = 1; pow; pow >>= 1)
    {
        if (pow & 1)
            test = ((test % mod) * (n % mod)) % mod;
        n = ((n % mod) * (n % mod)) % mod;
    }
    return test;
}
int metfastDek2()
{
      unsigned long long num;
      unsigned long long pow;
      unsigned long long mod=n;
      cout<<"               "<<endl;
    cout<<"Peroses Dekripsi"<<endl;
    cout<<"================"<<endl;
    printf("Masukan Nilai Chiperteks = ");
    scanf("%d",&num);
    printf("\n\n Kunci Rahasia = ");
    scanf("%d",&pow);
    printf(" modulo        = %d",&n);
```

```
    printf("\n **) hasil Dekripsinya adalah %d\n\n",
mod_powDek2(num, pow, mod));
    {
      printf("\n\n pesan aslinya adalah  ");
    int i=mod_powDek2(num, pow, mod);
    cout<<i<<" --> "<<char(i)<<endl;
    getch();
    cout<<"               "<<endl;
      }
}
unsigned mod_pow3(unsigned num3, unsigned pow3, unsigned mod3)
{
    unsigned long long test3;
    unsigned long long n = num3;
    for(test3 = 1; pow3; pow3 >>= 1)
    {
        if (pow3 & 1)
            test3 = ((test3 % mod3) * (n % mod3)) % mod3;
        n = ((n % mod3) * (n % mod3)) % mod3;
    }
    return test3;
}
int metDek3()
{
      int j,i;
      unsigned long long num3;
      unsigned long long pow3;
      unsigned long long mod3;
      printf("\n Masukan jumlah partisi enkripsi = ");
    scanf("%d",&j);
    printf("\n\nMasukan Kunci Rahasia = ");
    scanf("%d",&pow3);
    printf("\nMasukan modulusnya = ");
    scanf("%d",&mod3);
    for(i=0; i<j;i++){
    printf("\n\n Masukan nilai enkripsinya = ");
    scanf("%d",&num3);
    printf("\n\n pesan aslinya adalah  ");
    int a=mod_pow3(num3, pow3, mod3);
    cout<<a<<" --> "<<char(a)<<endl;
    cout<<"               "<<endl;
      }
}
void main()
{
   int pilih;

printf("############################################################\n")
;
    printf("##
##\n");
    printf("#\t\t\tPROGRAM KRIPTOGRAFI RSA\t\t\t
#\n");
    printf("#
#\n");
```

```
      printf("#\tPROGRAM PENGAMANAN PESAN RAHASIA RSA\
#\n");
      printf("#==================*****=====================#\n"
);
      printf("#\t\t\t Cr: Jajang Nurjaman (08610044)\t\t\t
#\n");
      printf("#\tUIN Sunan Kalijaga Yogyakarta\t
\n");
      printf("################################################\n"
);
    Menu:
printf("==================\n");
printf("|| MENU PROGRAM  ||\n");
printf("\1\1=========================================\1\1\n");
printf("||1.Tampilkan Deret Bilangan Prima         ||\n");
printf("||2.Tes Keprimaan Miller-Rabbin             ||\n");
printf("||3.Pembentukan Kunci (Enkripsi & Dekripsi Otomatis||\n");
printf("||4.Enkripsi Manual                           ||\n");
printf("||5.Dekripsi Manual                           ||\n");
printf("||6.Keluar                                    ||\n");
printf("\1\1=========================================\1\1\n");
printf("=> Silahkan Pilih No MENU (1-6) =  ");
scanf("%d",&pilih);
printf("\n\n\n\n");
switch (pilih){
case 1:
     cout<<"               "<<endl;
     printf("======================================\n");
       cout<<"=    Menampilkan Deret Bilangan Prima   ="<<endl;
     cout<<"======================================"<<endl;
     printf("                                    \n");
tampprima();
cout<<"               "<<endl;
goto cs2;
case 2:
     printf("======================================\n");
       cout<<"=      Tes keprimaan Miller-Rabbin       ="<<endl;
     cout<<"======================================"<<endl;
printf("\n**) Catatan :  Pilihlah Bilangan Prima yang besar
!\n\n");
     PrimeTestp();

     PrimeTestq();
     cout<<"               "<<endl;
     cout<<"(***)"<<endl;
cout<<"\nJika nilai p dan q prima, masukanlah kedua nilai pada
proses pembangkitan kunci"<<endl;
     cout<<"               "<<endl;
     goto cs2;
     case 5:
      {
      cout<<"               "<<endl;
     printf("======================================\n");
       cout<<"=    Menampilkan Dekripsi manual        ="<<endl;
     cout<<"======================================"<<endl;
     printf("                                    \n");
```

```
     metDek3();
       goto ax;}
       case 4:
      {
            cout<<"              "<<endl;
     printf("=======================================\n");
       cout<<"=    Menampilkan Enkripsi manual        ="<<endl;
     cout<<"======================================="<<endl;
     Enkripsi3();
       goto ax;}
       case 6:
      {goto ak;}
cs2:
case 3:
     cout<<"\n\n========================="<<endl;
     cout<<"=   Pembangkitan kunci   ="<<endl;
     cout<<"========================="<<endl;
     cout<<"                          "<<endl;
pembangkit();
int x=phi, y,kk;
 printf("\n\n\n** Masukan Bilangan Bulat Positif yang Relatif
Prima b > 1 dan b < %d \n\n   atau Nilai Gcd (%d , b) = 1.\n\n",
phi,phi);
  printf("\n\n\n\n");
  printf("|>>>> Menampilkan Deret Bilangan Relatif Prima (Y/T) ?
");
  fflush(stdin);
  scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){
printf("\n\n \1 Tentukan Nilai Batas Bawah Untuk Menampilkan
Bilangan Relatif Prima \1");
  printf("\n\n\n=> Masukan Batas Bawah = ");scanf("%d",&kk);

printf("\n=====================Relatifprima=================\n");
  for( y=kk;y<phi;y++){
      if(gcd(phi,y)==1)
      printf("%d\t",y);}
      printf("\n\n=============================================\n
");
      goto abc;}
 abc:
cout << "\n\n==> Masukan Bilangan Positif b yang Relatif prima =
";
  cin >> y;
  cout<<"              "<<endl;
  cout << "\n|>>>>  Nilai Gcd(" << x << ", " << y << ") = " <<
gcd(x,y) <<"   <<<<|\t\n";
  printf("\n\n\n");
  if (gcd(x,y)!=1){
printf("\n\a ** maaf nilai Gcd(%d , %d) !=  1,\n\n silahkan ulangi
kembali !\n\n\n\n\n",phi,y);
      goto abc;}
printf ("Caution : Kunci Publik dikirim ke pembuat pesan !\n\n");
printf(">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>")
;
```

```
printf("\n|>>>> \tkunci publiknya adalah %d dan modulo %d\t",y, n
);
printf("\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<\n"
);
    printf("\n\n\n");
    int extended(int x,int y);
    int ans;
        ans=extended(x,y);
    if (0<ans){
      printf ("Caution : Harap Dirahasiakan !\n\n");
printf(">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>");
printf("\n> \tkunci rahasia adalah %d dan mod %d\t ",ans%phi, n );
printf("\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<\n");}
    else{
    printf ("Caution : Harap Dirahasiakan !\n\n");
printf(">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>");
printf("\n>\tkunci rahasia  %d dan mod %d\t ",(ans+phi)%phi, n);
printf("\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<\n"
);
    }
  printf("|>>>> Apakah Anda Akan Menulis Pesan (Y/T) ?  ");
  fflush(stdin);
  scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){goto pesan;}
  while(jawab=='T'||jawab=='t'){goto ax;}
    pesan:
    printf("\n\n\n");
      signed long long pow=ans;
cout<<"\n\n=====================================================<<
endl;
      cout<<"=\tSilahkan Ketikan Pesan (Tanpa Spasi)\t   ="<<endl;
cout<<"=====================================================<<endl
;
   printf("\nPesan : ");scanf("%s",&ss);
   for (i = 0 ; ss[i] !=0; i++)
   v[i] = (ss[i]);
    printf("\n Nilai ASCII nya : \n\n");
   for (j = 0; j < i; j++){
    printf("\t%c = %d\t", v[j],v[j]);
   int num=v[j];
       }
printf("\n\n=> jumlah karakter yang diketik = %d\n\n",j);
cout<<"               "<<endl;
cout<<"=================================="<<endl;
cout<<"=\tPeroses Enkripsi\t   ="<<endl;
cout<<"=================================="<<endl;
printf("\n");
printf("\n **) Nilai Chiperteksnya adalah :\n\n");
cout<<" +-----------------------------------------+"<<endl;
cout<<" +-----------------------------------------+\n"<<endl;
     for (j = 0; j < i; j++){
      unsigned long long num=v[j];
      unsigned long long kp=y;
      qq[j]=mod_powEnk(v[j],kp,n);
    printf("  ");
```

```
    printf("%d\t", qq[j]);
      }
      {
cout<<"\n\n +----------------------------------------+"<<endl;
cout<<" +----------------------------------------+\n"<<endl;
printf("\n\n");
  printf("|>>>> Apakah Pesan akan di Dekripsi (Y/T) ?  ");
  fflush(stdin);
  scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){goto ext;}
  while(jawab=='T'||jawab=='t'){goto ax;}
      }
      ext:
        printf("\n\n\n\n");
    int extended(int x,int y);
    cout<<"\n==================================="<<endl;
    cout<<"=\tPeroses Dekripsi\t   ="<<endl;
    cout<<"==================================="<<endl;
    printf("\n");
    ans=extended(x,y);
    if (0<ans){
    printf("\n\1\3| kunci rahasianya adalah %d \t ",ans%phi);
      }
    else{
  printf("\n\1\3| kunci rahasianya adalah  %d \t ",(ans+phi)%phi);
      }
}
  {
     printf("\n");
    unsigned long long kr;
printf("\n=> Masukan Kunci Rahasia diatas= ");
    scanf("%d",&kr);
    unsigned long long num=qq[j];
    unsigned long long pow=kr;
    unsigned long long mod=n;
    printf("\n pesan aslinya adalah:\n\n ");
cout<<"+----------------------------------------+"<<endl;
cout<<" +----------------------------------------+\n"<<endl;
    for (j = 0; j < i; j++){
    unsigned long long num=qq[j];
    unsigned long long i=mod_powDek2(num, pow, mod);
    cout<<"\t"<<char(i);
      }
      {
cout<<"\n\n +----------------------------------------
+"<<endl;
cout<<" +----------------------------------------+\n"<<endl;
      }
    goto ax;
    }
    while(jawab=='T'||jawab=='t'){goto ak;}
 ak :
printf(" \n\n\t\tTerima Kasih Telah Menggunakan Program ini\n");
goto end;
{
```

```
ax:
printf("\n\n|>> Apakah anda ingin kembali ke MENU awal (Y/T) ?
");
  fflush(stdin);
  scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){
  printf("\n\n\n\n\n");
  goto Menu;}
  while(jawab=='T'||jawab=='t'){goto ak;}}
 end: return 0;
}
```

1.2. Kode Program TTD RSA

```
#include<stdio.h>
#include<conio.h>
#include <iostream.h>
#include <time.h>
#include <stdlib.h>

long int phi,M,e,d,C,FLAG;
long int a, b, c, t, w,md,xx,zz;
long int p,q,s,kp,kr,y,x,ans,ans2,n;
unsigned long long j,i,num,pow,total,total1,count,sig;
signed chp;
char jawab;
long int tampprima()
{
    long int x1,y1,c=0;
printf("**) Masukkan Dua Buah Bilangan Bulat Positif Sebagai Batas
Awal dan Batas Akhir\n    Sebuah Deret Bilangan Prima\n\n");
printf("\n\n=> Silahkan masukkan nilai batas awal deret  =  ");
scanf("%d",&y1);
printf("\n");
printf("=> Silahkan masukkan nilai batas akhir deret =  ");
scanf("%d",&x1);
printf("+-----------------------------------------------------+");
printf("\n|| Deret Bilangan Prima dari %d sampai %d\t
||\n",y1,x1);
printf("+-----------------------------------------------+\n\n");
    for(int i=y1;i<=x1;i++){
       for(int j=1;j<=i;j++){
       if(i % j == 0){
       c++;
            }
        }
    if(c == 2) printf("%d\t",i);
    c=0;
    }
    getch();
    cout<<"               "<<endl;
printf("\n===============================================\n\n");
printf("**) Pilihlah Dua Buah Bilangan Bulat dari deret diatas,\n
kemudian masukan kedalam konstanta p dan q pada menu pembangkitan
kunci !\n\n");
 clrscr;
}
using namespace std;
unsigned long random(unsigned long f,unsigned long g)
 {
     srand((unsigned long)time(NULL));
     return (unsigned long)(f+rand()%g);
 }
  long PowMod(long x,long y,long g)
 {
     long k, l, u;
     k=1; l=x; u=y;
     while(u){
```

```
        if(u&1)k=(l*k)%g;
        u>>=1;
        l=(l*l)%g;
    }
    return k;
 }
long int RabinMillerKnl(unsigned long g)
 {
    unsigned long B, f=g-1, j=0, v, i;
    while(!(f & 1)){
        ++j;
        f>>=1;
    }
    B=random(2,f);
    v=PowMod(B, f, g);
    if(v == 1)
    return 1;
    i=1;
    while(v != g - 1){
        if(i == j)
            return 0;
        v=PowMod(v, 2, g);
       i++;
    }
    return 1;
 }
long int PrimeTestp()
 {
 unsigned long p;
    int TestNum=5;
    int count=0;
  op:
    cout<<"\n\n=> Masukan sembarang bilangan prima p =  ";
    cin>>p;

    for(int temp=0; temp < TestNum; temp++)
    {
        if (p%2==0)
        {
            if (p==2)
            count=TestNum;
            break;
        }
        if(RabinMillerKnl(p))
            count++;
        else
            break;
    }
    if(count==TestNum)
        {
   printf("\n   >>> Hasil Tes :  %d adalah bilangan prima
\n\n",p);
         }
    else{
printf("\n ** >>> Hasil Tes : %d bukan bilangan prima \n\n
Silahkan masukan kembali nilai p !\n\n", p);
```

```
        goto op;}
 }
long int PrimeTestq()
{
     unsigned long q;
    int TestNum=5;
    int count=0;
oq :
    cout<<"\n\n=> Masukan sembarang bilangan prima q =  ";
    cin>>q;
    for(int temp=0; temp < TestNum; temp++)
    {
        if (q%2==0)
        {
            if (q==2)
                count=TestNum;
            break;
        }
        if(RabinMillerKnl(q))
            count++;
        else
            break;
    }
    if(count==TestNum)
  printf("\n   >>> Hasil Tes :  %d adalah bilangan prima\n\n",q);
    else
    {
printf("\n  ** >>> Hasil Tes :  %d bukan bilangan prima, \n\n
Silahkan masukan kembali nilai q !\n\n",q);
     goto oq;}
 }
long int pembangkit(){
      pq:
      int  jum, i;
    cout<<"=> Masukan Bilangan Prima p = ";  //sebagai nilai p
    cin>>p;
    jum = 0;
    for (i=1; i<=p; i++)
    if (p%i==0) jum++;
    if (jum==2) {
    goto q;}
    else{
    printf("\n ** maaf! nilai %d adalah bilangan composit,\n
silahkan masukan kembali bilangan prima lain ! \n\n",p);
     goto pq;
     }
q:
printf("\n\n");
cout<<"=> Masukan Bilangan Prima q = ";  //sebagai nilai q
cin>>q;
jum = 0;
for (i=1; i<=q; i++)
if (q%i==0) jum++;
 if (jum==2) {
  goto q2;}
 else{
```

```
 cout << "** maaf nilai p bukan bilangan prima, silahkan masukan
kembali bilangan prima lain ! \n";
 goto q;
 }
q2 :
      if (p==q){
printf("\n ** maaf nilai p tidak boleh sama dengan nilai q !\n");
      goto pq;}
      else
n = p*q;
printf("\n Nilai modulus :\n");
printf("\n\t\t|>>>>\tn = %d * %d = %d \t\n",p,q,n);
if (n<250){
printf("\n\a ** Maaf nilai n harus lebih besar dari 250,\n Masukan
kembali bilangan prima p dan q yang besar!\n\n");
      goto pq;}
phi=(p-1)*(q-1);
printf("\n Nilai  Totien :\n");
printf("\n\t\t|>>>>\tF(n)= (%d - 1)*(%d - 1)= %d \t",p,q,phi);
cout<<"               "<<endl;
 }
 long int gcd(int a, int b) {
  long int temp;
  while (b != 0) {
    temp = a % b;
    a = b;
    b = temp;
  }
  return(a);
}
long int eu () {
}
long int extended(int x,int y)
{
   long int a1=1,a2=0,a3=x,b1=0,b2=1,b3=y,q,t1,t2,t3;
abc:    if(b3==0)
    {
        return a3;
    }
    if(b3==1)
    {
        return b2;
    }
    q=(a3/b3);
    t1=a1-(q*b1);
    t2=a2-(q*b2);
    t3=a3-(q*b3);
    a1=b1;
    a2=b2;
    a3=b3;
    b1=t1;
    b2=t2;
    b3=t3;
    goto abc;
}
unsigned mod_powEnk(unsigned num,unsigned kp,unsigned n)
```

```
{
    unsigned long long test;
    unsigned long long nn = num;
    for(test = 1; kp; kp >>= 1)
    {
        if (kp & 1)
       test = ((test % n) * (nn % n)) % n;
        nn = ((nn % n) * (nn % n)) % n;
    }
    return test;
    }    }
unsigned mod_powEnk2(unsigned num,unsigned kp,unsigned n)
{
    unsigned long long test;
    unsigned long long nn = num;
    for(test = 1; kp; kp >>= 1)
    {
        if (kp & 1)
        test = ((test % n) * (nn % n)) % n;
        nn = ((nn % n) * (nn % n)) % n;
    }
    return test;
       }
unsigned signature (){
cout<<"\n\n================================================="<<endl
;
cout<<"= Buat fungsi hash dari Pesan asli(Tanpa Spasi) ="<<endl;
Cout<<"=================================================="<<end
l;
    int count = 0;
    FILE *in_file;
    int ch;
    int total = 0;
printf("\n Pesan Asli =   ");
    in_file = fdopen(0, "r");
    if (in_file == NULL) {
        printf("Error input%s\n");
        exit(8);
    }
    while (1) {
        ch = fgetc(in_file);
        if ((ch == EOF) || (ch == 10))
            break;
        ++count;
        printf("\n %c nilainya %d",ch, ch);
        total += ch;
            }
    printf("\n\n jumlah karakternya adalah %d\n", count);
printf("\n\n\t\t\4\4\4\4\4\4\4\4\4\4\44\4\4\4\4\4\4\4\4\4\4\4\4\4\4"
);
printf("\n\t\t\4\4 Nilai hashya adalah : %d          \4\4",
total);
printf("\n\t\t\4\4\4\4\4\4\4\4\4\\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4");
printf("\n\n");
cout<<"               "<<endl;
cout<<"==================================="<<endl;
```

```
cout<<"=\Peroses Signature="<<endl;
cout<<"==================================="<<endl;
    printf("\n");
    printf("\n \1 Masukan Nilai Kunci Publiknya : ");
    scanf("%d",&kp);
    printf("\n \1 Masukan Nilai Modulo          : ");
    scanf("%d",&n);
printf("\n **) Nilai Signaturenya adalah :");
{
      unsigned long long num=total;
      sig=mod_powEnk2(total,kp,n);
 printf("\n   ==============================") ;
 printf("\n \t\t Nilai Signature =   |>>>   %d            ", sig);
 printf("\n   ==========================") ;
 printf("\n\n\t Nilai Signature dikirimkan bersama Cipherteks") ;
}
}
unsigned mod_powDek2(unsigned num, unsigned pow, unsigned mod)
{
    unsigned long long test;
    unsigned long long n = num;
    for(test = 1; pow; pow >>= 1)
    {
        if (pow & 1)
     test = ((test % mod) * (n % mod)) % mod;
        n = ((n % mod) * (n % mod)) % mod;
    }
    return test;
}
unsigned mod_pow3(unsigned num3, unsigned pow3, unsigned mod3)
{
    unsigned long long test3;
    unsigned long long n = num3;
    for(test3 = 1; pow3; pow3 >>= 1)
    {
        if (pow3 & 1)
        test3 = ((test3 % mod3) * (n % mod3)) % mod3;
        n = ((n % mod3) * (n % mod3)) % mod3;
    }
    return test3;
}
int metDek3()
{
      unsigned long long num3;
      unsigned long long pow3;
      unsigned long long mod3;
      printf("\n\n Masukan nilai signature = ");
    scanf("%d",&num3);
    printf("\n\n Kunci Publik = ");
    scanf("%d",&pow3);
    printf(" Modulus      = ");
    scanf("%d",&mod3);
    int a=mod_pow3(num3, pow3, mod3);
    printf("\n\n nilai verifikasinya adalah  %d",a);
    cout<<"               "<<endl;
cout<<"\n\n========================================="<<endl;
```

```
cout<<"=\t\tFungsi hash kedua\t\t=";
cout<<"\n==============================================";
cout<<"\n=========================================="<<endl;
cout<<"=Silahkan Ketikan Pesan yang sudah didekripsi ="<<endl;
cout<<"===================================================="<<end
l;
    int count = 0;
    FILE *in_file;
    int ch;
    int total = 0;
    printf("\n Pesan Dekripsi =   ");
    in_file = fdopen(0, "r");
    if (in_file == NULL) {
        printf("Error input%s\n");
        exit(8);
    }
    while (1) {
        ch = fgetc(in_file);
        if ((ch == EOF) || (ch == 10))
            break;
        ++count;
        printf("\n %c nilainya %d",ch, ch);
        total += ch;
         printf("\n\n jumlah karakternya adalah %d\n", count);
printf("\n\n\t\t\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4");
printf("\n\t\t\4\4 Nilai hashya adalah : %d          \4\4",
total);
printf("\n\t\t\4\44\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4");
    cout<<"\n\n\n================================="<<endl;
    cout<<"=\tverifikasi\t         ="<<endl;
    cout<<"================================="<<endl;
    if (total==a){
cout<<"\n\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<"<<endl;
cout<<"<< Nilai Verifikasi sama dengan nilai hash (pesan dekripsi)
<<endl;
cout<<"<<      \t\tPesan masih otentik\t\t   >>"<<endl;
cout<<">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>"<<endl;}
      else{
cout<<"\n\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<"<<endl
;
cout<<"<< Nilai Verifikasi tidak sama dengan nilai hash (pesan
dekripsi)    >>"<<endl;
cout<<"<<\t\tPesan tidak otentik\t\t              >>"<<endl;
cout<<">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>"<<endl;}
          }
   }
void main()
{
    int pilih;
   printf("##############################################\n");
    printf("##                             ##\n");
    printf("#\t\t    PROGRAM DIGITAL SIGNATURE RSA\t\t\t#  \n");
    printf("#\tPROGRAM PENGAMANAN PESAN RAHASIA TTD RSA\t  #
\n");
```

```
    printf("#====================*****=======================#
\n");
    printf("#\t\t\t\t Cr: Jajang Nurjaman (08610044)\t\t\t#  \n");
    printf("#\UIN Sunan Kalijaga Yogyakarta\t        #  \n");
    printf("#############################################\n");
    Menu:clrscr();
printf("==================\n");
printf("|| MENU PROGRAM  ||\n");
printf("||=================================\n");
printf("|| 1. Tampilkan Deret Bilangan Prima  ||\n");
printf("|| 2. Tes Keprimaan Miller-Rabbin     ||\n");
printf("|| 3. Pembentukan Kunci               ||\n");
printf("|| 4. Signature  (Manual)             ||\n");
printf("|| 5. Verifikasi (Manual)             ||\n");
printf("|| 6. Keluar                          ||\n");
printf("=====================================\n");
printf("=> Silahkan Pilih No MENU (1-6) =  ");
scanf("%d",&pilih);
switch (pilih){
case 1:
     cout<<"               "<<endl;
     printf("=======================================\n");
       cout<<"=    Menampilkan Deret Bilangan Prima   ="<<endl;
     cout<<"======================================="<<endl;
     printf("                                       \n");
tampprima();
cout<<"              "<<endl;
goto cs2;
case 2:
     printf("=======================================\n");
       cout<<"=      Tes keprimaan Miller-Rabbin       ="<<endl;
     cout<<"======================================="<<endl;
printf("\n**) Catatan :  Pilihlah Bilangan Prima yang besar
!\n\n");
  PrimeTestp();
    PrimeTestq();
     cout<<"              "<<endl;
     cout<<"(***)"<<endl;
cout<<"\nJika nilai p dan q prima, masukanlah kedua nilai pada
proses pembangkitan kunci"<<endl;
     cout<<"              "<<endl;
     clrscr;
     goto cs2;
      case 4:
      {
      printf("\n\n=======================================\n");
       cout<<"=    Menampilkan Signature manual       ="<<endl;
     cout<<"=======================================";
       signature();
       goto ver2;
while(jawab=='T'||jawab=='t'){
  goto pil;}
      }
      ver1:
    case 5:
      {
```

```
            cout<<"               "<<endl;
     printf("\n\n=========================================\n");
       cout<<"=    Menampilkan Verifikasi manual       ="<<endl;
     cout<<"=========================================="<<endl;
     metDek3();
     goto pil;
      }
      case 6:
      {goto end;}
cs2:
case 3:
     cout<<"\n\n========================="<<endl;
     cout<<"=   Pembangkitan kunci   ="<<endl;
     cout<<"========================="<<endl;
pembangkit();
int x=phi, y,kk;
printf("\n\n\n** Masukan Bilangan Bulat Positif yang Relatif Prima
b > 1 dan b < %d \n\n   atau Nilai Gcd (%d , b) = 1.\n\n",
phi,phi);
  printf("\n\n");
 printf(">>>>> Menampilkan Deret Bilangan Relatif Prima (Y/T) ?
");
  fflush(stdin);
  scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){
printf("\n\n ++ Tentukan Nilai Batas Bawah Untuk Menampilkan
Bilangan Relatif Prima");
  printf("\n\n\n=> Masukan Batas Bawah = ");scanf("%d",&kk);
  printf("\n=========Relatif prima=======================\n");
  for( y=kk;y<phi;y++){
      if(gcd(phi,y)==1)
      printf("%d\t",y);}
printf("\n\n================================================\n");
      goto abc;}
 abc:
  cout<<"               "<<endl;
cout << " Masukan Bilangan Bulat Positif b yang Relatif prima = ";
  cin >> y;
  cout<<"               "<<endl;
cout << "\n|>>>>  Nilai Gcd(" << x << ", " << y << ") = " <<
gcd(x,y) <<"   <<<<|\t\n";
    if (gcd(x,y)!=1){
printf("\n\a ** maaf nilai Gcd(%d , %d) !=  1,\n\n silahkan ulangi
kembali !\n\n",phi,y);
      goto abc;}
printf ("\n\nCaution : Kunci Publik dikirim kepada pembuat pesan
!\n\n");
printf(">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>");
printf("\n|>>\tkunci publiknya adalah %d dan modulo %d\t   ",y, n
);
printf("\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<\n");
printf("\n\n");
int extended(int x,int y);
        int ans;
            ans=extended(x,y);
```

```
      if (0<ans){
      printf ("\n\nCaution : Harap Dirahasiakan !\n\n");
      printf(">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>");
printf("\n\tkunci rahasianya %d dan modulo %d\t ",ans%phi, n );
printf("\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<\n");}
    else{
    printf ("\n\nCaution : Harap Dirahasiakan !\n\n");
    printf(">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>");
printf("\n>>>> \tkunci rahasianya adalah  %d dan modulo %d\t
",(ans+phi)%phi, n);
  printf("\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<\n");
    }
    printf("\n");
printf("\n\n|> Apakah anda ingin membentuk fungsi hash (Y/T) ?
");
       fflush(stdin);
       scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){
  clrscr;goto hash1;}
  goto pil;
  hash1:
   cout<<"\n\n=========================================="<<endl;
   cout<<"=\tSilahkan Ketikan Pesan (Tanpa Spasi)\t   ="<<endl;
  cout<<"=========================================="<<endl;
    int count = 0;
    FILE *in_file;
    int ch;
    int total = 0;
    printf("\n Pesan Asli :   ");
    in_file = fdopen(0, "r");
    if (in_file == NULL) {
        printf("Error input%s\n");
        exit(8);
    }
    while (1) {
        ch = fgetc(in_file);
        if ((ch == EOF) || (ch == 10))
            break;
        ++count;
        printf("\n %c nilainya %d",ch, ch);
        total += ch;
           }
    printf("\n jumlah karakternya adalah %d\n", count);

printf("\n\n\t\t\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4");
 printf("\n\t\ Nilai hashya adalah : %d          \4\4", total);
   printf("\n\t\t\44\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4");
printf("\n\n Silahkan tekan enter untuk mengetahui nilai
Signature!");
   getche();
    cout<<"               "<<endl;
    printf("\n\n\n");
    cout<<"==================================="<<endl;
    cout<<"=\tPeroses Signature\t   ="<<endl;
    cout<<"==================================="<<endl;
```

```
    printf("\n");
printf("\n **) Nilai Signaturenya adalah :");
{
      if(0<ans){
      unsigned long long num=total;
      unsigned long long kp=ans;
      sig=mod_powEnk(total,kp,n);
    printf("\n \t\t Signature =   |>>>   %d            ", sig);
printf("\n\n\t\1\1\1 Nilai Signature dikirimkan bersama
Cipherteks") ;
     if(0>ans){
      unsigned long long num=total;
      unsigned long long kp=ans+phi;
      sig=mod_powEnk(total,kp,n);
   cout<<"";
    printf("\n======================") ;
    printf("\n \t\t Signature =    |>>>   %d            ", sig);
    printf("\n==================") ;
    printf("\n\n\t\1\1\1 Nilai Signature dikirimkan bersama
Cipherteks") ;}
      }
      printf("\n\n");
  printf("\n\n|>>> Apakah Pesan akan di verifikasi (Y/T) ?  ");
  fflush(stdin);
  scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){
      printf("\n\n\n\n");
cout<<"              "<<endl;
    cout<<"===================================="<<endl;
    cout<<"=\tPeroses Verifikasi\t  ="<<endl;
    cout<<"===================================="<<endl;
    printf("\n");
      printf("\n\2\2 kunci publiknya adalah %d \t   \n",y);
      goto verifikasi;}
      goto pil;
}
  {
      verifikasi:
      unsigned long long kp;
printf("\n=> Masukan kembali Kunci Publik diatas = ");
    scanf("%d",&kp);
    unsigned long long num=sig;
      unsigned long long pow=kp;
      unsigned long long mod=n;
       printf("\n pesan aslinya adalah:\n  ");
      printf("\n\t  ");
    unsigned long long i=mod_powDek2(num, pow, mod);
    printf("\n ==================") ;
    printf("\n \t nilai verifikasinya = |>>>   %d            ",
i);
     printf("\n =====================") ;
            cout<<"              ";
      {
cout<<"\n\n\n\n=========================================="<<endl;
```

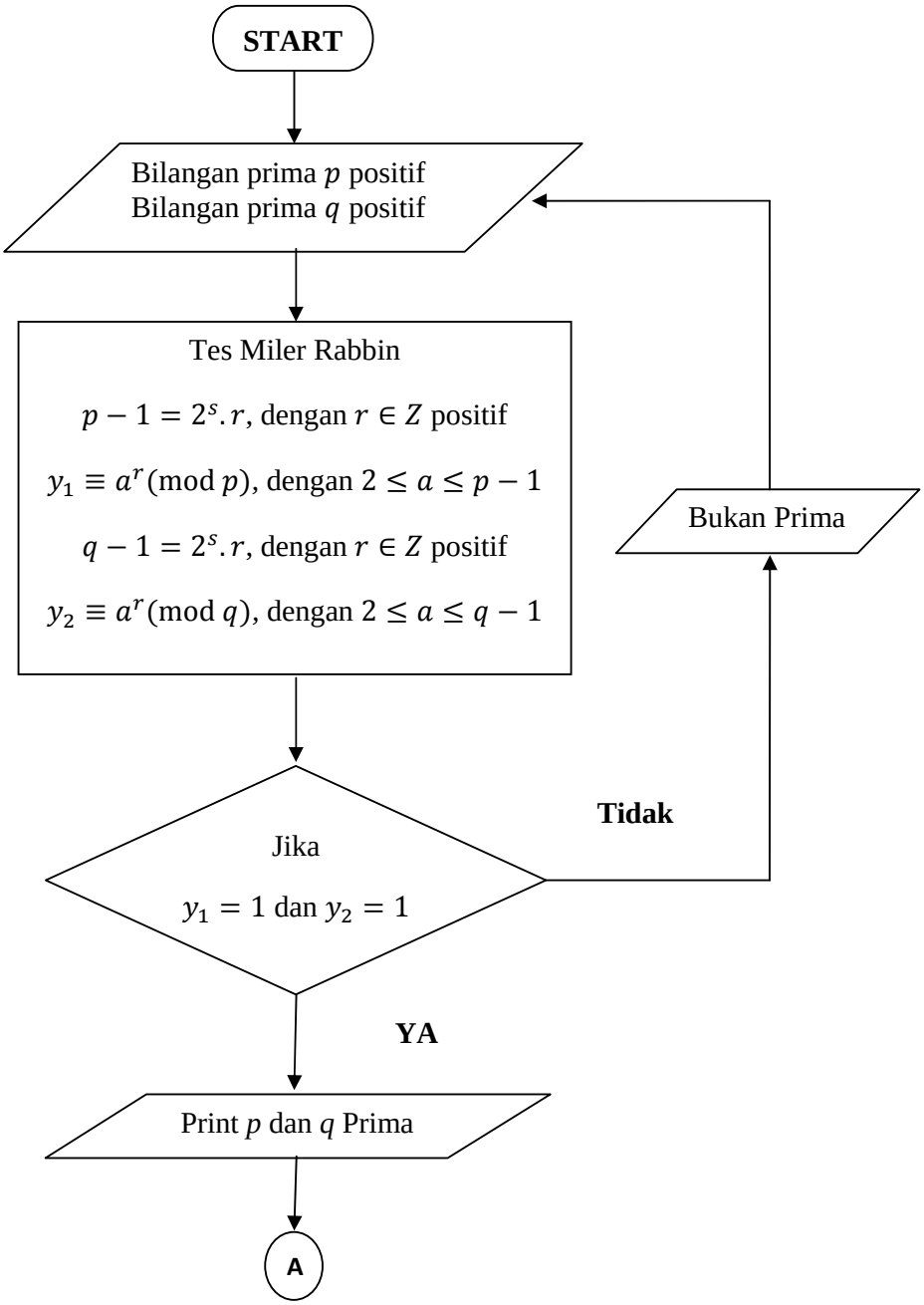
```
cout<<"=  Silahkan Buat Fungsi hash dari pesan dekripsi
="<<endl;
cout<<"================================================="<<endl
;
    int count = 0;
    FILE *in_file;
    int ch;
    int total1 = 0;
printf("\n Pesan Dekripsi =   ");
    in_file = fdopen(0, "r");
    if (in_file == NULL) {
        printf("Error input%s\n");
        exit(8);
    }
    while (1) {
        ch = fgetc(in_file);
        if ((ch == EOF) || (ch == 10))
            break;

        ++count;
        printf("\n %c nilainya %d",ch, ch);
        total1 += ch;

    }
    printf("\n\n jumlah karakternya adalah %d\n", count);

printf("\n\n\t\t\4\44\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4");
    printf("\n\tNilai hashya adalah : %d          \4\4", total1);
    printf("\n\t\t\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4\4");

    if(i==total1){
      printf("\n\n");
cout<<"\n\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<"<<end
l;
cout<<"<< Nilai Verifikasi sama dengan nilai hash (pesan dekripsi)
>>"<<endl;
cout<<"<<      \t\tPesan masih otentik\t\t             >>"<<endl;
cout<<">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>"<<endl
;}
      else{
      printf("\n\n");
cout<<"\n\n<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<"<<endl;
cout<<"<< Nilai Verifikasi  tidak sama dengan nilai hash (pesan
dekripsi)    >>"<<endl;
cout<<"<< \t\tPesan tidak otentik\t\t              >>"<<endl;

cout<<">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>"<<endl;
}
    printf("\n\n\n");
    goto pil;
      }

cout<<"\n\n\n\n\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1";
      }
      ver2:
```

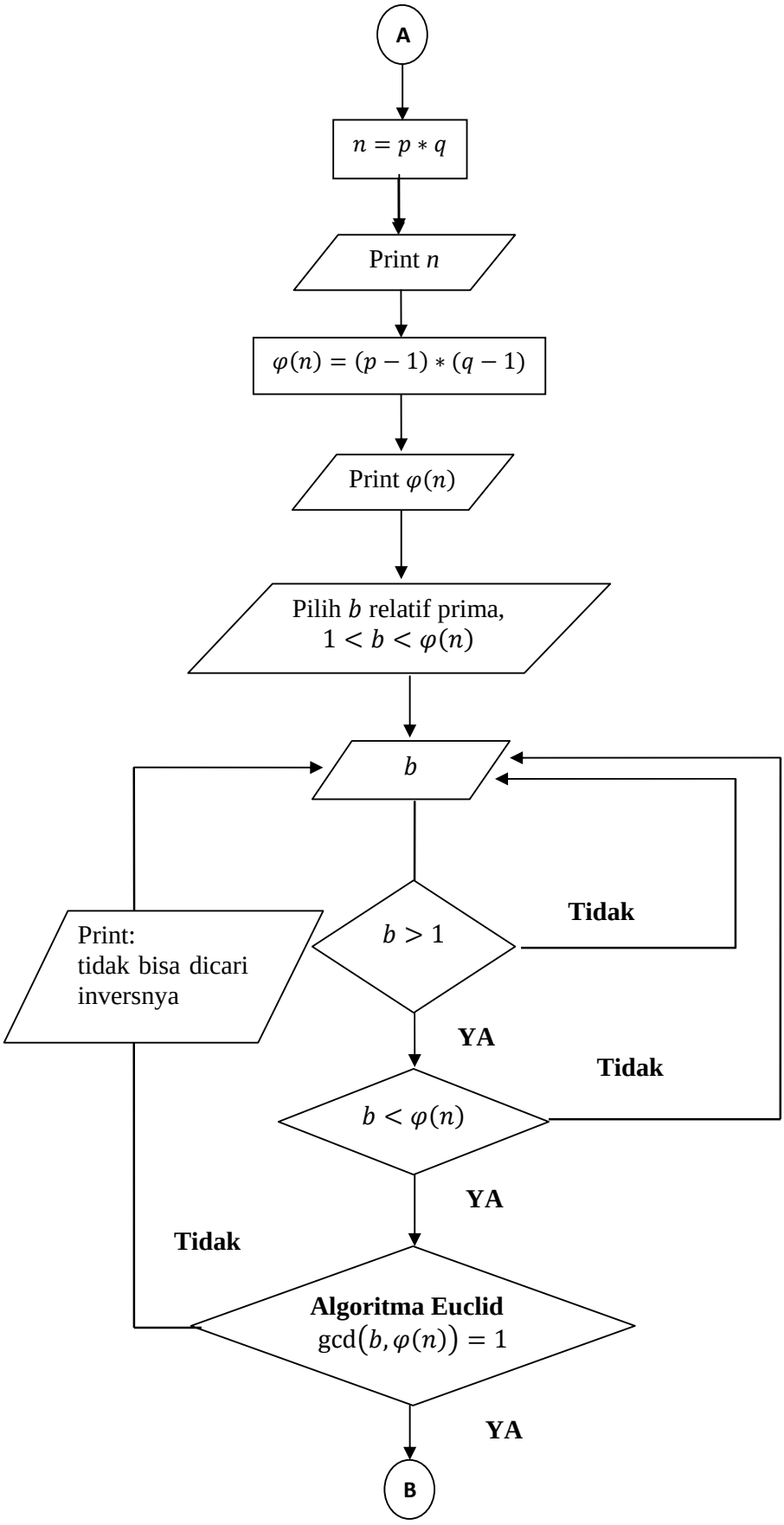
```
printf("\n\n\n\n|>>>> Apakah anda ingin Melakukan verifikasi (Y/T)
?  ");
       fflush(stdin);
       scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){
  clrscr;goto ver1;}
  goto pil;
  pil:
printf("\n\n|>>>> Apakah anda ingin kembali ke MENU awal (Y/T) ?
");
  fflush(stdin);
  scanf("%c",&jawab);
  printf("\n");
  while(jawab=='Y'||jawab=='y'){printf("\n\n\n\n");  goto Menu;}
  while(jawab=='T'||jawab=='t'){goto end;}

 end: printf(" \n\n\t\tTerima Kasih Telah Menggunakan Program
ini\t\t\n\n\n");
 return 0;
}
```

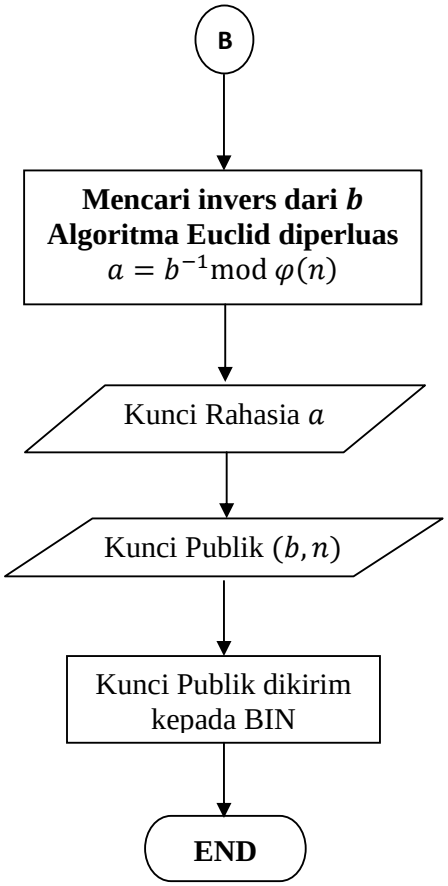
Lampiran 2.

2.1. Flowchart Kriptografi RSA

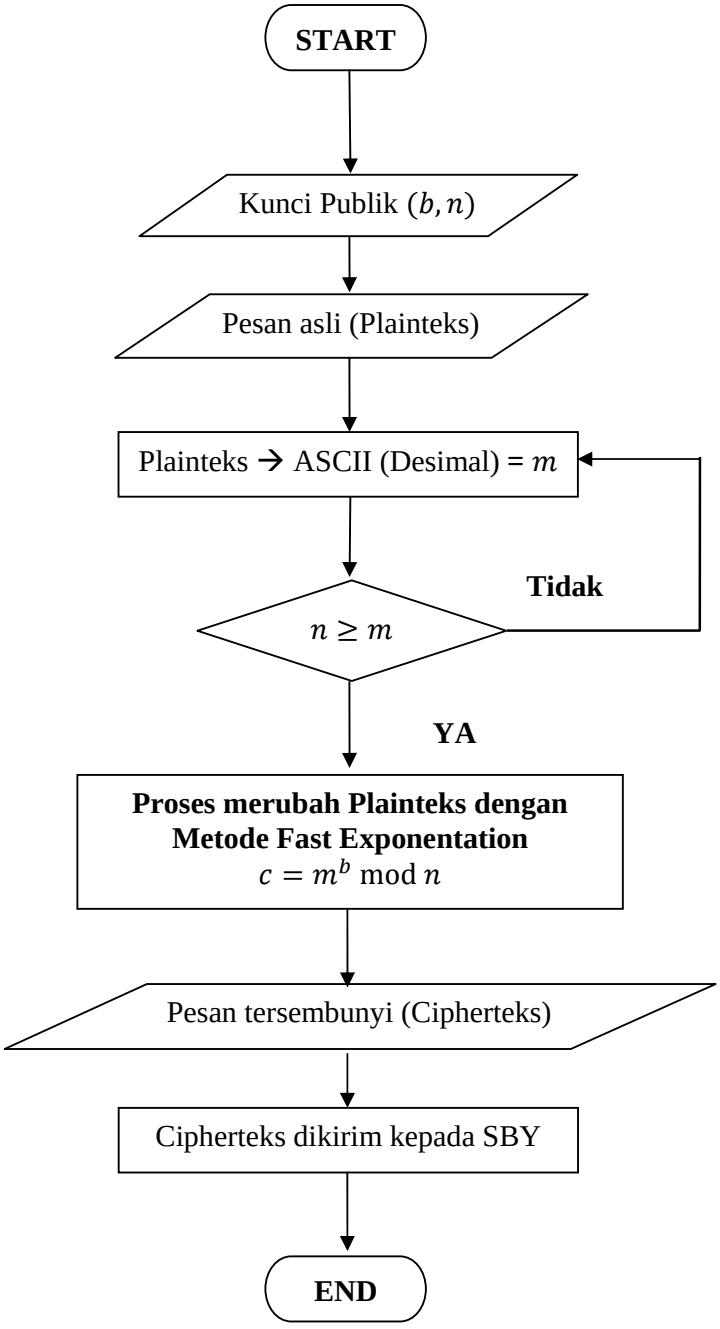
2.1.1. Flowchart Pembentukan Kunci Algoritma RSA



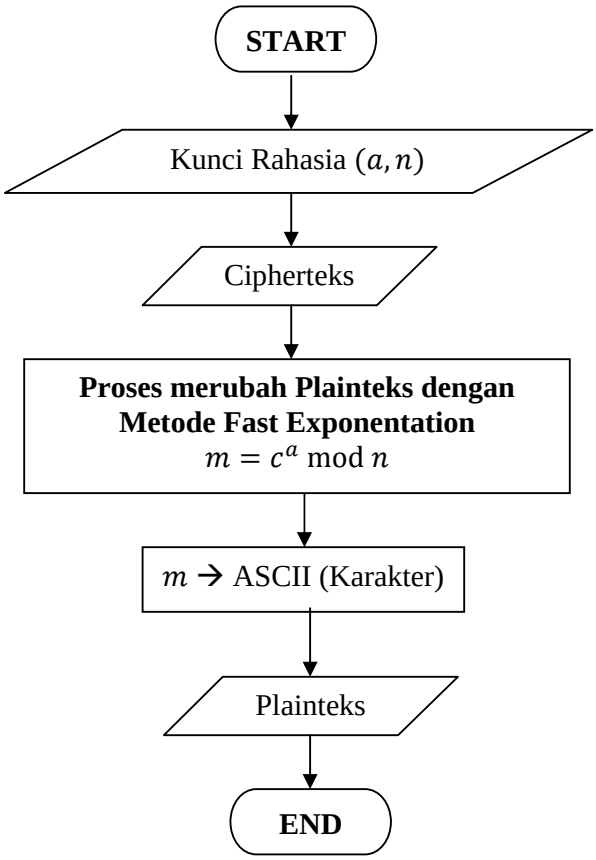

A
$n = p * q$
Print n
$\varphi(n) = (p-1) * (q-1)$
Print $\varphi(n)$
Pilih b relatif prima,
$1 < b < \varphi(n)$
b
$b > 1$
Tidak
Print:
tidak bisa dicari
inversnya
YA
Tidak
$b < \varphi(n)$
YA
Tidak
Algoritma Euclid
$\gcd(b, \varphi(n)) = 1$
YA
B


B
Mencari invers dari b
Algoritma Euclid diperluas
$a = b^{-1} \bmod \varphi(n)$
Kunci Rahasia a
Kunci Publik (b, n)
Kunci Publik dikirim kepada BIN
END

2.1.2. Flowchart Enkripsi RSA



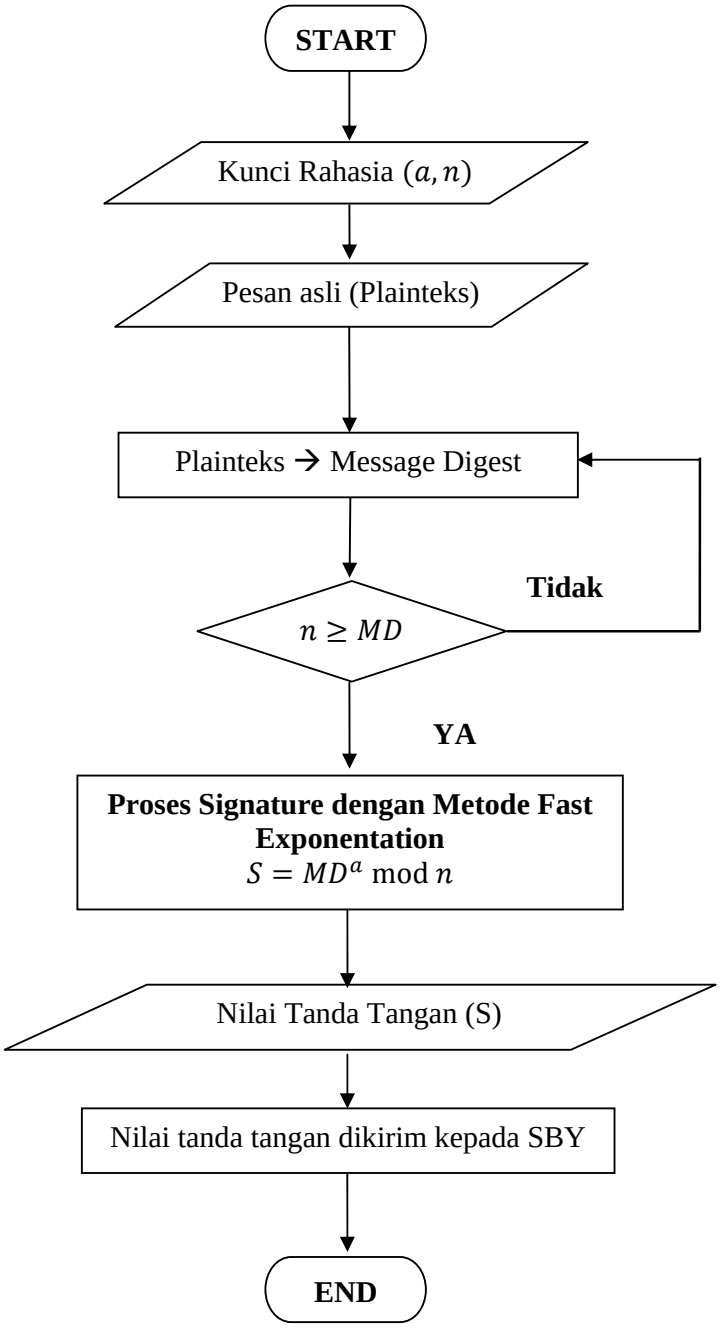
2.1.3. Flowchart Dekripsi RSA



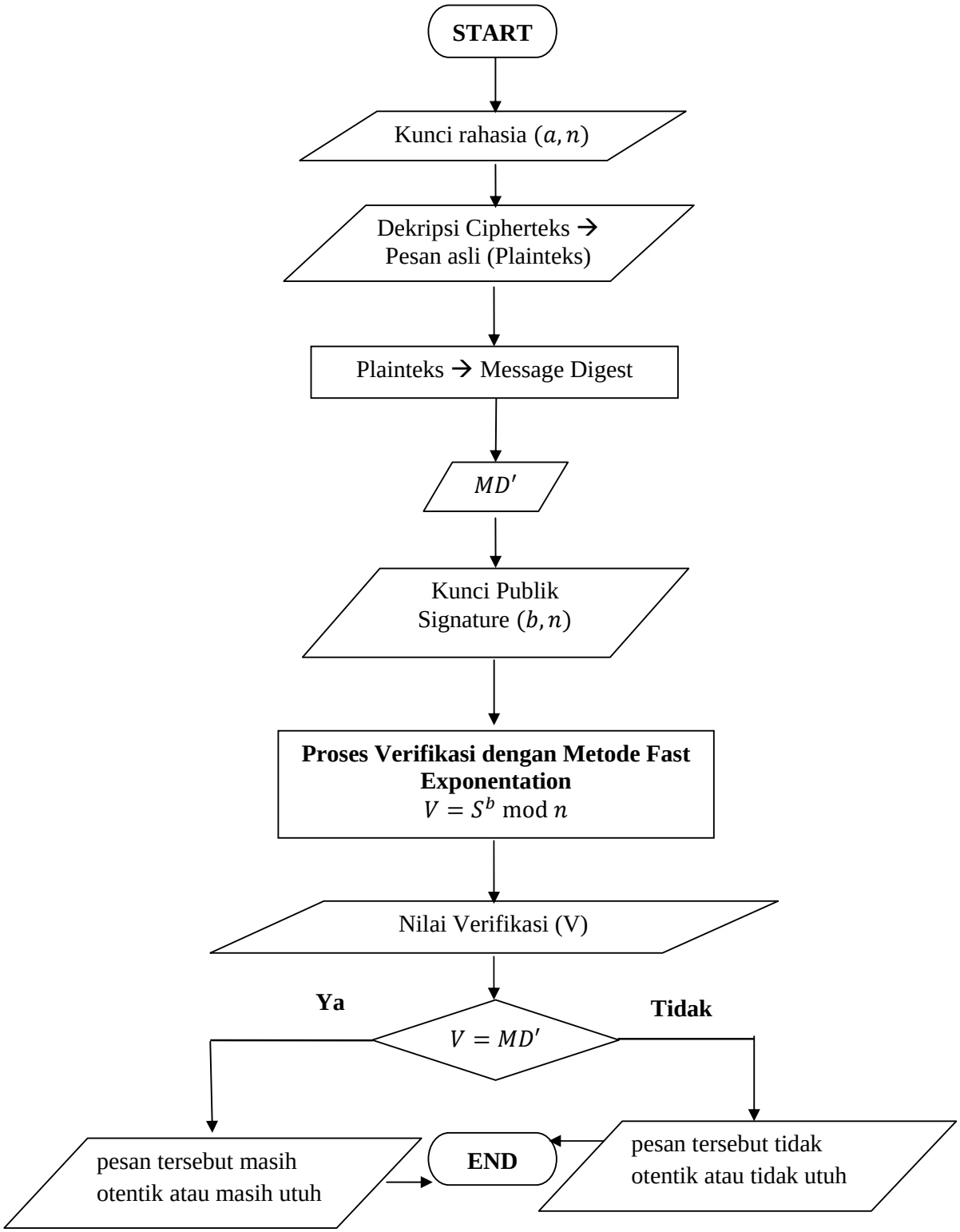
2.2. Tanda Tangan Digital RSA

2.2.1. Flowcahrat Pembangkitan Kunci sama dengan RSA

2.2.2. Flowchart Tanda Tangan Digital



2.2.3. Flowchart Verifikasi Tanda Tangan Digital



Lampiran 3.

DATA PRIBADI PENULIS

Nama Lengkap	: Jajang Nurjaman
NIM	: 08610044
Tempat, Tgl. Lahir	: Kuningan, 22 Desember 1988
Alamat	: Desa Dukuh Dalem RT 06 RW 02, Kec. Ciawigebang, Kab. Kuningan, Jawa Barat 45591
No. Hp	: 081332074047
E-Mail	: dak_ciawi@yahoo.co.id

Riwayat Pendidikan :

2008 – 2012	: S1 Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2007 – 2008	: S1 Jurusan Sejarah Kebudayaan Islam Fakultas Adab UIN Sunan Kalijaga Yogyakarta.
2004 – 2007	: MAN Ciawigebang.
2001 – 2004	: MTS PUI Ciawigebang.
1995 – 2001	: SDN Dukuh Dalem.