KRIPTOANALISIS RSA
DENGAN KURVA ELLIPTIK
(*CRYPTANALYSIS OF RSA WITH ELLIPTIC CURVES*)

Skripsi

untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

Zeni Fera Bhakti

08610026

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2013

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Surat Persetujuan Skripsi / Tugas Akhir
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 kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Zeni Fera Bhakti
NIM : 08610026
Judul Skripsi : Kriptoanalisis RSA dengan Kurva Elliptik
(Cryptanalysis RSA with Elliptic Curves)

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

Wassalamu'alaikum wr. wb.

Yogyakarta, 18 Desember 2012
Pembimbing

Muhamad 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.01.1/175/2013

Skripsi/Tugas Akhir dengan judul : Kriptoanalisis RSA dengan Kurva Elliptik (Cryptanalysis of RSA with Elliptic Curves)

Yang dipersiapkan dan disusun oleh :
Nama : Zeni Fera Bhakti
NIM : 08610026
Telah dimunaqasyahkan pada : 07 Januari 2013
Nilai Munaqasyah : A
Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Zaki Riyanto, M.Si
NIDN. 0513018402

Penguji I

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

Penguji II

Mahmudi,S.Si.,M.Si

Yogyakarta, 17 Januari 2013
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA FAKULTAS SAINS DAN TEKNOLOGI YOGYAKARTA UIN SUNAN KALIJAGA

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

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : Zeni Fera Bhakti

NIM : 08610026

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, 18 Desember 2012

Yang menyatakan

Zeni Fera Bhakti

NIM. 08610026

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penulisan skripsi ini. Salawat dan salam semoga selalu tercurahkan kepada Nabi Muhammad Saw.

Penyusunan skripsi ini dimaksudkan untuk memenuhi sebagian persyaratan guna memperoleh gelar Sarjana Program Studi Matematika. Skripsi ini berisi pembahasan mengenai kriptoanalisis RSA dengan kurva elliptik. Penulis menyadari bahwa tanpa bimbingan dan doa dari berbagai pihak, skripsi ini tidak dapat selesai dengan baik. Oleh karena itu ucapan terima kasih disampaikan sebesar-besarnya kepada :

1. Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Muhamad Zaki Riyanto, S.Si., M.Sc. selaku pembimbing yang telah meluangkan waktu untuk membantu, memotivasi dan mengarahkan sehingga skripsi ini dapat terselesaikan.
4. Mochammad Farhan Qudratullah, M.Si selaku Penasihat Akademik yang telah meluangkan waku untuk membantu dan mengarahkan selama menempuh studi juga segenap dosen dan karyawan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

5. Ari Dwi Hartanto, S.Si. yang telah bersedia membagi ilmunya. Terimakasih untuk waktu dan bimbingannya.

Tiada gading yang tak retak. Tiada karya yang sempurna. Tentunya penulis menyadari bahwa dalam penulisan skripsi ini tidak lepas dari kekurangan. Oleh karena itu, saran dan kritik yang membangun sangat penulis harapkan untuk menyempurnakan skripsi ini. Semoga skripsi ini dapat memberikan manfaat bagi semua pihak.

Yogyakarta, 18 Desember 2012

Penulis

PERSEMBAHAN

Untuk Bapak dan Ibuku tercinta, yang telah memberikan kasih sayang dan doanya. Ku persembahkan karya sederhana ini untuk mereka, semoga dapat memberikan kebanggaan atas jerih payahnya selama ini.

Untuk Adikku, yang selalu menjadi alasanku untuk terus semangat. Semoga dapat termotivasi untuk memberikan yang lebih baik dariku.

Special Thank's to Nanang Bayu Herjunantiyo, yang tak lelah menyemangati dan mendoakanku. Terimakasih. ^_^

Juga untuk Lia Setyawati, S.Si,
Rossi Fauzi S.Si, Fanny Brilliyanti. S.Si, Hanifah Nurlatifah, S.Si,
Purwanti Cahyaningtyastuty, S.Si
dan si cantik Dewi Sri Suharsono. Thank's for all...

Almamaterku, Prodi Matematika Fakultas Sains dan Teknologi
Universitas Islam Negeri Sunan Kalijaga Yogykarta.

MOTTO

Kalau kita yakin sama sesuatu, kita harus percaya, terus berusaha bangkit dari kegagalan, jangan pernah menyerah dan taruh keyakinan itu di kening kamu. Lima centimeter di depan kening kamu. Jadi dia nggak akan pernah lepas dari mata kamu. Bawa mimpi dan keyakinan kamu setiap hari, kamu lihat setiap hari dan percaya bahwa kamu bisa. Sehabis itu yang kamu perlu cuma..

Cuma kaki yang akan berjalan lebih jauh dari biasanya, tangan yang akan berbuat lebih banyak dari biasanya, mata yang akan menatap lebih lama dari biasanya, leher yang akan lebih sering melihat ke atas. Lapisan tekad yang seribu kali lebih keras dari baja dan hati yang akan bekerja lebih keras dari biasanya. Serta, mulut yang akan selalu berdoa...

(Novel 5 cm)

"Lakukan yang terbaik dan tetap semangat "
(Nanang Bayu H.)

DAFTAR ISI

ARTI LAMBANG DAN SINGKATAN

$\mathbb{Z}$: himpunan semua bilangan bulat

$\mathbb{N}$: himpunan semua bilangan asli

$\mathbb{Z}_m$: himpunan semua bilangan bulat modulo m

$x \in A$: *x* anggota himpunan *A*

$a|n$: *a* membagi habis *n*

$\neq$: tidak sama dengan

$>$: lebih besar dari

$\leq$: lebih kecil dari atau sama dengan

$\geq$: lebih besar dari atau sama dengan

$|a|$: harga mutlak *a*

$\lfloor \alpha \rfloor$: bilangan bulat terbesar yang lebih kecil atau sama dengan α

$gcd(a, b)$: *great common division* (faktor persekutuan terbesar) dari *a* dan *b*

$x \leftarrow a$: nilai *a* dimasukkan ke *x*

$\prod_{i=1}^{n} a_i$: perkalian $a_1 . a_2 . \ldots . a_n$

$a \ mod \ b$: *a modulo b*

$a \equiv b (mod \ m)$: *a* kongruen *b* modulo *m*

$a \not\equiv b (mod \ m)$: *a* tidak kongruen *b* modulo *m*

a^{-1} : invers dari *a*

$A \subseteq X$: *A* himpunan *(subset)* atau sama dengan *X*

$H < G$: *H* subgrup dari *G*

$|G|$: banyaknya elemen *G*

$\emptyset : G \rightarrow G'$: $\emptyset$ suatu pemetaan dari grup *G* ke grup *G'*

$G \cong G'$: *G* isomorfis dengan *G'*

$\Rightarrow$: "Berakibat" atau bukti implikasi ke arah kanan

$\Leftarrow$	: bukti implikasi ke arah kiri
$\Leftrightarrow$	: biimplikasi atau jika dan hanya jika
$\sum_{i=1}^{n} a_i$	: penjumlahan $a_1 + a_2 + \ldots + a_n$
$\mathbb{R}$	: himpunan semua bilangan real
C_r^n	: *r* – kombinasi dari *n* unsur yang berbeda
■	: akhir dari suatu pembuktian
$n!$	: *n* faktorial

DAFTAR TABEL

DAFTAR GAMBAR

KRIPTOANALISIS RSA

DENGAN KURVA ELIPTIK

ABSTRAKSI

Zeni Fera Bhakti

NIM. 08610026

Sistem kripto RSA merupakan suatu sistem kripto asimetris yang bekerja pada himpunan bilangan bulat modulo *n* atau biasa ditulis Z_n, dengan *n* adalah suatu bilangan hasil kali dua bilangan prima ganjil yang berbeda. Disebut asimetris karena kunci pada RSA mencakup dua buah kunci, yaitu kunci publik dan kunci rahasia. Kunci publik digunakan untuk melakukan enkripsi, dan dapat diketahui oleh orang lain. Sedangkan kunci rahasia tetap dirahasiakan dan digunakan untuk melakukan dekripsi. Keamanan sistem kripto RSA ini terletak pada bilangan *n* yang cukup besar dan sulit difaktorkan. Selain kriptografi dalam kriptologi (ilmu persandian) dikenal juga istilah kriptoanalisis, yakni sebuah teknik memecahkan kunci dari suatu sistem persandian.

Pembahasan skripsi ini difokuskan pada kriptoanalisis RSA dengan memanfaatkan kegunaan kurva elliptik dalam pemfaktoran *n*. Pemfaktoran ini dilakukan untuk memperoleh kunci rahasia. Kurva elliptik adalah himpunan dari semua titik-titik yang merupakan solusi dari persamaan kurva elliptik dua variabel yang mana di dalam kurva elliptik ini berlaku beberapa aturan penjumlahan titik yang dapat digunakan untuk mendapatkan faktor dari *n*.

Kata kunci: bilangan prima, faktorisasi, kriptologi, RSA, kurva eliptik.

CRYPTANALYSIS OF RSA

WITH ELLIPTIC CURVES

ABSTRACT

Zeni Fera Bhakti

NIM. 08610026

System crypto RSA is an asymmetric crypto system that works on the set of integers modulo *n* or regular written Z_n, where *n* is a number the product of two distinct odd primes. It is called asymmetric because the RSA key includes two keys, the public key and the secret key. The public key is used to do encryption, and be known by others. While the secret key is kept secret and used to decryption. Security RSA crypto system which is located on a number *n* is quite large and difficult to be factored. Besides cryptography, in crytology also known as the term cryptanalysis. Cryptanalysis is a technique of key solving a system of coding.

Discussion of this paper focused on cryptanalysis RSA with the application of elliptic curves in factoring *n*. Factoring is done to obtain the secret key. Elliptik curves is the set of all points which is a solution of the equation of the elliptic curves two variable. In elliptic curves applies some point sum rules which can be used to get a factor of *n*.

Key word : primes, factorization, cryptology, RSA, eliptik curves.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring berkembangnya teknologi informasi maka kebutuhan akan jaringan keamanan yang aman pun semakin meningkat. Apalagi jika sudah menyangkut hal-hal yang penting dan sangat rahasia. Oleh karena itu, salah satu upaya yang dapat dilakukan yaitu dengan menyandikan pesan menjadi pesan bersandi yang tidak mudah dimengerti.

Sistem kripto RSA merupakan salah satu sistem penyandian yang dapat digunakan untuk menyandikan pesan menjadi pesan bersandi. Sistem ini pertama kali dipublikasikan pada tahun 1978 oleh Ron Rivest, Adi Shamir dan Leonard Adleman dari Massachussetts Institute of Technology (MIT). Nama RSA adalah singkatan dari nama belakang mereka bertiga. Sekarang kriptografi RSA sudah digunakan hampir di segala bidang yang terkait dengan penggunaan jaringan komputer. Bahkan kehidupan kita saat ini tidak lepas dari kriptografi; mulai dari transaksi di mesin ATM, transaksi di bank, transaksi dengan kartu kredit, percakapan melalui telepon genggam serta mengakses internet. RSA termasuk dalam kelompok algoritma kunci publik maka sistem ini memiliki dua macam kunci, yakni kunci publik dan kunci rahasia. Di dalam sistem ini terdapat algoritma dan kunci untuk menyandikan pesan, selain itu juga terdapat kunci lain, yaitu kunci yang berfungsi untuk mengembalikan pesan bersandi menjadi pesan

asli. Algoritma penyandian tersebut dapat diketahui, digunakan dan dipelajari oleh siapapun. Akan tetapi, kunci rahasia yang digunakan untuk mengembalikan pesan bersandi menjadi pesan asli harus dijaga kerahasiaannya. Sejalan dengan berkembangnya ilmu pengetahuan, ada kemungkinan pesan bersandi dapat dipecahkan oleh pihak yang tidak berwenang. Hal semacam ini di dalam kriptografi disebut dengan kriptoanalisis. Sistem kripto RSA ini dikenal sebagai sistem kripto yang keamanannya terletak pada bilangan *n* yang cukup besar dan sulit difaktorkan (Rinaldi Munir, 2006). Walaupun demikian, karena bilangan ini terdapat dalam kunci publik yang dipublikasikan maka tentu saja sembarang orang dapat mengetahuinya. Tidak menutup kemungkinan akan ditemukan suatu cara untuk dapat memecahkannya. Seiring berkembangnya ilmu matematika pada tahun 1980-an ditemukanlah salah satu kegunanaan kurva elliptik dalam kriptoanalisis RSA, yakni menemukan faktor dari *n* sehingga keamanan pesan menjadi terancam (L.C. Washington, 2008). Jika pihak yang tidak berwenang terhadap pesan tersebut dapat menemukan faktor dari *n* dan jika pihak tersebut memahami algoritma kriptografi RSA maka pesan dapat didekrip sehingga dapat diperoleh pesan asli.

1.2 Batasan Masalah

Pembatasan masalah sangat penting dilakukan dalam suatu penelitian untuk memfokuskan objek yang diteliti. Pembahasan penelitian ini dibatasi pada pembahasan sistem kripto RSA meliputi konsep matematis yang melandasinya, proses penyandian dan proses kriptoanalisis menggunakan kurva elliptik.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan maka dirumuskan permasalahan sebagai berikut :

1. Bagaimana konsep-konsep matematis yang melandasi pembentukan sistem kripto RSA?
2. Bagaimana proses pembentukan kunci, enkripsi dan dekripsi sistem kripto RSA?
3. Bagaimana proses kriptoanalisis RSA dengan kurva elliptik?
4. Bagaimana implementasi kriptoanalisis RSA dengan kurva elliptik dalam bentuk program sederhana menggunakan MATLAB?

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk :

1. Mengkaji tentang konsep-konsep matematis yang melandasi sistem kripto RSA.
2. Mengkaji tentang proses penyandian.
3. Mengkaji tentang proses kriptoanalisis.
4. Mengkaji implementasi kriptoanalisis RSA dengan kurva elliptik dalam bentuk program sederhana menggunakan MATLAB.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut :

1. Memberikan kontribusi dalam dunia kriptografi khususnya kriptoanalisis bahwa dalam sebuah sistem kripto RSA yang dikenal aman karena

sulitnya pemfaktoran bilangan *n* yang bahkan masih digunakan hingga saat ini, tetap terdapat celah untuk mengancam keamanannya.

2. Selain itu, dapat menjadi referensi bagi peneliti selanjutnya.

1.6 Tinjauan Pustaka

Penulisan skripsi ini terinspirasi dari paper yang ditulis oleh M. Zaki Riyanto dan Ardhi Ardhian (2008) dan skripsi yang ditulis oleh Ari Dwi Hartanto (2010). Keduanya membahas tentang kriptografi kunci publik khususnya sandi RSA mulai dari konsep dasar perhitungan matematis, pembentukan kunci, enkripsi hingga dekripsi dengan terperinci sehingga sangat membantu penulis dalam memahami sandi RSA. Selain itu, terdapat tesis yang ditulis oleh Michael Pemberton (2009). Dalam tesis ini, salah satunya memuat penjelasan bahwa pada tahun 1980-an ditemukan aplikasi kurva elliptik dalam kriptografi, yakni dapat menemukan faktor *n*, dimana *n* merupakan bagian dari kunci publik sandi RSA yang mana jika ada pihak yang dapat menemukan faktor dari *n* tersebut maka dapat dipastikan keamanan pesan menjadi terancam. Stinson (2006) memberikan penjelasan mengenai sistem kripto RSA. Pembahasan mengenai konsep dasar matematis, seperti teori bilangan bulat, persamaan kongruen dan struktur aljabar abstrak yang meliputi grup, homomorfisma dan gelanggang diberikan oleh Buchmann (2000). Pembahasan mengenai bilangan bulat juga diberikan oleh Rosen (1992). Fraleigh (2000) juga ambil bagian dalam skripsi ini dengan memberikan penjelasan mengenai struktur aljabar abstrak. Walaupun demikian, tidak ada pembahasan yang mengaitkan secara langsung dengan sistem kripto RSA. Sedangkan untuk beberapa algoritma diberikan oleh Menezes, Oorschot dan

Vanstone (1996). Selanjutnya, juga ada buku dari L.C. Washington (2008) dan J.H. Silverman (1986) yang menjelaskan tentang kurva elliptik.

BAB VII

KESIMPULAN

7.1. Kesimpulan

Berdasarkan hasil studi literatur tentang kriptoanalisis RSA dengan kurva elliptik yang dilakukan penulis dapat ditarik kesimpulan sebagai berikut :

1. Konsep-konsep matematis yang melandasi sistem kripto RSA dibagi menjadi dua bagian yaitu bilangan bulat dan dasar struktur albajar. Bilangan bulat meliputi: pembagi persekutuan terbesar *(greatest common divisor),* algoritma Euclide dan algoritma Euclide diperluas. Sedangkan dasar struktur aljabar meliputi: grup, ring dan lapangan.
2. Dalam proses penyandian sistem kripto RSA terdapat proses pembentukan kunci, enkripsi dan dekripsi.

   2.1 Algoritma pembentukan kunci RSA adalah sebagai beikut:

   Input : Bilangan prima ganjil yang berbeda, *p* dan *q*.

   Output : Kunci publik *(n,b)* dan kunci rahasia *(p,q,a).*

   Langkah :

   1. Hitung $n = p.q$ dan $\varphi(n) = (p-1)(q-1)$.
   2. Pilih sebarang bilangan b, $(1 < b < \varphi(n))$, dengan $\gcd(b, \varphi(n)) = 1$.
   3. Hitung invers dari b, yaitu $a = b^{-1} mod\ \varphi(n)$.
   4. Diperoleh kunci publik *(n,b)* dan kunci rahasia *(p,q,a).*

2.2 Algoritma enkripsi RSA adalah sebagai berikut:

Input : Suatu pesan (misal panjangnya *t* karakter) dan kunci publik RSA (n, b).

Output : Cipherteks: $c = c_1 - c_2 - \cdots - c_t$.

Langkah :

1. Konversikan karakter – karakter pesan menjadi bilangan plainteks $m_i \in \mathbb{Z}_n, i = 1,2, \ldots, t$.
2. Untuk *i* dari 1 sampai *t* dikerjakan:

   Hitung $c_i = m_i^b mod\ n$.
3. Diperoleh cipherteks $c = c_1 - c_2 - \cdots - c_t$.

2.3 Algoritma dekripsi RSA adalah sebagai berikut:

Input : Cipherteks $c = c_1 - c_2 - \cdots - c_t$ dan kunci rahasia RSA (p, q, a).

Output : Pesan asli.

Langkah :

1. Untuk i dari 1 sampai *t* dikerjakan :

   Hitung $m_i = c_i^a mod\ n$.
2. Konversikan bilangan m_i menjadi karakter pesan m_i^* menggunakan Tabel ASCII.
3. Gabungkan karakter-karakter pesan m_i^* sehingga diperoleh pesan asli.

3. Kriptoanalisis RSA dengan kurva elliptik merupakan suatu teknik memecahkan pesan dengan menemukan faktor suatu bilangan *n* dengan memanfaatkan aturan penjumlahan titik-titik pada kurva elliptik. Pemfaktoran ini bertujuan untuk menemukan kunci rahasia.

   3.1. Algoritma Pemfaktoran dengan Kurva Elliptik adalah sebagai berikut:

   Input : Bilangan bulat *n*.

   Output : Bilangan prima ganjil yang berbeda, *p* dan *q*.

   Langkah :

   1. Pilih kurva elliptik E modulo *n* dan titik *P*.
   2. Pilih bilangan bulat *B* dan hitung *(B!)P* di *E*.
   3. Jika (2) gagal karena gradien garis modulo *n* tidak ada maka faktor dari *n* ditemukan.
   4. Jika (2) sukses, pilih *B* yang lebih besar atau pilih kurva elliptik dan titik *P* baru, dan mulai dari awal.

   3.2. Algoritma kriptoanalisis RSA dengan kurva elliptik adalah sebagai berikut:

   Input : Bilangan bulat *n* dan cipherteks.

   Output : Pesan asli hasil kriptoanalisis.

Langkah :

1. Faktorkan nilai *n* menggunakan aturan penjumlahan titik dalam kurva elliptik sehingga nilai *p* dan *q* ditemukan. (Algoritma 5.1.)
2. Temukan kunci rahasia dengan memanfaatkan nilai *p* dan *q* hasil pemfaktoran. (Algoritma 3.1.)
3. Dekripsi cipherteks menggunakan kunci rahasia hasil kriptoanalisis. (Algoritma 3.3.)

7.2. Saran

Berdasarkan pada proses penelitian yang dilakukan tentang kriptoanalisis RSA dengan kurva elliptik maka saran-saran yang ingin disampaikan penulis adalah :

1. Perlu dilakukan penelitian kembali tentang kriptoanalisis RSA menggunakan cara lain selain dengan kurva elliptik.
2. Implementasi kriptoanalisis RSA dengan kurva elliptik menggunakan program komputer selain software MATLAB, misalkan dengan Maple, Delphi, Java dsb.

Demikian saran-saran yang dapat disampaikan penulis. Semoga skripsi ini dapat menjadi inspirasi bagi pembaca untuk mengembangkan lebih lanjut tentang kriptoanalisis RSA dengan kurva elliptik.

DAFTAR PUSTAKA

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

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

Hartanto, Ari Dwi. 2010. *Manfaat General Linear Grup pada Sistem Kripto RSA*. Skripsi S1. Yogyakarta : Jurusan Matematika FMIPA UGM.

http://id.m.wikipedia.org/wiki/kriptoanalisis, diakses pada 17 Desember 2012 pukul 10.04 WIB.

http://id.m.wikipedia.org/wiki/MATLAB, diakses pada 8 Januari 2013 pukul 09.04 WIB.

J.H. Silverman. 1986. *The Arithmetic of Elliptic Curves*. New York : Springer-Verlag.

L.C. Washington. 2008. *Elliptik curves : Number Theory and Cryptography*. Second Edition. New York : Chapman & Hall/CRC.

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

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

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

Rosen, K.H. 1992. *Elementary Number Theory and Its Applications*. USA : AT and T Bell Laboratories.

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

Stinson, D.r. 2006. *Cryptography Theory and Practice*. Third Edition. Florida : CRC Press, Inc.

Widiarsono, Teguh. 2005. *Tutorial Praktis Belajar MATLAB*. Jakarta.

LAMPIRAN-LAMPIRAN

LAMPIRAN A

SKRIP PROGRAM

Listing A.1. : Skrip program untuk menentukan titik-titik kurva elliptik.

```
function titik(m,a,b,x)
disp('=====================================================')
if mod(4*a^3+27*b^2,m)==0
    error('Masukkan nilai a atau b yang lain.');
else
  ykuadrat=mod((a*(x^3))+x+b,m);
  for n=0:m-1
      t=mod(n^2,m);
      if ykuadrat==t
      disp(['x=',num2str(x) '   y=',num2str(n)])
      end;
  end;
  disp('=====================================================')
end;
```

Listing A.2. : Skrip program untuk mencari faktor dari *m*.

```
function pemfaktoran(m,Px,Py,a,B)
Pfakx=Px;
Pfaky=Py;
N=factorial(B);
disp('=====================================================')
for i=2:N
     [G,w]=cekinvers(Px,Py,Pfakx,Pfaky,m);
    if w==0;
        if i==N;
            disp(['Berdasarkan penjumlahan titik-titik di atas.']);
            disp(['Didapatkan faktor dari ' ,num2str(m), ' yaitu :']);
            p=abs(G);
            q=m/p;
            fprintf('p=%d\n',p);
            fprintf('q=%d\n',q);
            disp('=====================================================')
            break;
        end;
    elseif w~=0;
        if i==N;
            disp('Tidak bisa bisa dihitung faktornya.');
            disp('Gunakan variabel yang lain.');
            disp('=====================================================');
        elseif i~=N;
            [Tempx,Tempy]=penjumlahan(Px,Py,Pfakx,Pfaky,m,a);
            Pfakx=Tempx;
            Pfaky=Tempy;
            disp(['Koordinat titik untuk ',num2str(i),'P adalah :']);
            disp(['x=',num2str(Pfakx), '    y=',num2str(Pfaky)]);
            disp('-----------------------------------------------------')
        end;
        end;
    end;
```

```
function [G,w]=cekinvers(x1,y1,x2,y2,m)
    if x1==x2 & y1==y2;
        [G,w]=inversG(2*y1,m);
    elseif x1~=x2 & y1~=y2;
        x=x2-x1;
        X=mod(x,m);
        [G,w]=inversG(X,m);
    else
        error('x1=x2 tapi y1 tidak sama dengan y2');
    end;


function [x3,y3]=penjumlahan(x1,y1,x2,y2,m,a)
    if x1==x2 & y1==y2;
        [G,w]=inversG(2*y1,m);
        L=mod(((3*(x1)^2)+a)*w,m);
        x3=mod(L^2-x1-x2,m);
        y3=mod(L*(x1-x3)-y1,m);
    elseif x1==x2 & y1==-y2;
        x3=0;
        y3=0;
    elseif x1~=x2 & y1~=y2;
        x=x2-x1;
        X=mod(x,m);
        [G,w]=inversG(X,m);
        L=mod((y2-y1)*w,m);
        x3=mod(L^2-x1-x2,m);
        y3=mod(L*(x1-x3)-y1,m);
    else
        error('x1=x2 tapi y1 tidak sama dengan y2');
    end;


function [G,i]=inversG(b,m)
G=m;
c=b;
i=0;
if b==0;
    error('nilai tidak boleh 0');
elseif b~=0;
    while c~=0
       r=mod(G,c);
       G=c;
       c=r;
    end;
    if G==1;
        for i=0:m-1
            in=mod(b*i,m);
            if in==1
                break;
            end
        end;
    end;
end
```

LAMPIRAN B

TABEL KODE ASCII

Kode ASCII (0 – 127)

No.	Kode	No.	Kode	No.	Kode	No.	Kode
0	NULL	32	SP (*Space*)	64	@	96	`
1	SOH (*Start of Heading*)	33	!	65	A	97	a
2	STX (*Start of Text*)	34	"	66	B	98	b
3	ETX (*End of Text*)	35	#	67	C	99	c
4	EOT (*End of Transmission*)	36	$	68	D	100	d
5	ENQ (*Enquiry*)	37	%	69	E	101	e
6	ACK (*Acknowledge*)	38	&	70	F	102	f
7	BEL (*Bell*)	39	'	71	G	103	g
8	BS (*Backspace*)	40	(	72	H	104	h
9	HT (*Horizontal Tab*)	41	)	73	I	105	i
10	NL (*New Line*)	42	*	74	J	106	j
11	VT (*Vertical Tab*)	43	+	75	K	107	k
12	NP (*New Page*)	44	,	76	L	108	l
13	CR (*Carriage Return*)	45	-	77	M	109	m
14	SO (*Shift Out*)	46	.	78	N	110	n
15	SI (*Shift In*)	47	/	79	O	111	o
16	DLE (*Data Link Escape*)	48	0	80	P	112	p
17	DC1 (*Device Control 1*)	49	1	81	Q	113	q
18	DC2 (*Device Control 2*)	50	2	82	R	114	r
19	DC3 (*Device Control 3*)	51	3	83	S	115	s
20	DC4 (*Device Control 4*)	52	4	84	T	116	t
21	NAK (*Negative Acknowledge*)	53	5	85	U	117	u
22	SYN (*Synchronus Idle*)	54	6	86	V	118	v
23	ETB (*End of Trans. Blok*)	55	7	87	W	119	w
24	CAN (*Cancel*)	56	8	88	X	120	x
25	EM (*End of Medium*)	57	9	89	Y	121	y
26	SUB (*Substitute*)	58	:	90	Z	122	z
27	ESC (*Escape*)	59	;	91	[	123	{
28	FS (*File Separator*)	60	<	92	\	124	|
29	GS (*Group Separator*)	61	=	93	]	125	}
30	RS (*Record Separator*)	62	>	94	^	126	~
31	US (*Unit Separator*)	63	?	95	_	127	DEL

Kode ASCII *Extended* (128 – 255)

128	Ç	144	É	161	í	177	▒	193	┴	209	╤	225	ß	241	±
129	ü	145	æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
130	é	146	Æ	163	ú	179	│	195	├	211	╙	227	π	243	≤
131	â	147	ô	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
132	ä	148	ö	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
133	à	149	ò	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
134	å	150	û	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
135	ç	151	ù	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
136	ê	152	ÿ	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
137	ë	153	Ö	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
138	è	154	Ü	171	½	187	╗	203	╦	219	█	235	δ	251	√
139	ï	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	ⁿ
140	î	157	¥	173	¡	189	╜	205	═	221	▌	237	ϕ	253	²
141	ì	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
142	Ä	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	
143	Å	160	á	176	░	192	└	208	╨	224	α	240	≡		