PENGGUNAAN KRIPTOGRAFI KURVA ELIPTIK PADA PROSES PENYANDIAN ELGAMAL

SKRIPSI

Oleh:
FEBRINA MEDIAWATI SETYOBUDI
NIM. 09610007

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2013

PENGGUNAAN KRIPTOGRAFI KURVA ELIPTIK PADA PROSES PENYANDIAN ELGAMAL

SKRIPSI

Diajukan Kepada:
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Sains (S.Si)

Oleh:
FEBRINA MEDIAWATI SETYOBUDI
NIM. 09610007

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2013

PENGGUNAAN KRIPTOGRAFI KURVA ELIPTIK PADA PROSES PENYANDIAN ELGAMAL

SKRIPSI

Oleh:
FEBRINA MEDIAWATI SETYOBUDI
NIM. 09610007

Telah Diperiksa dan Disetujui untuk Diuji :
Tanggal: 13 Februari 2013

Dosen Pembimbing I,	Dosen Pembimbing II,
Abdussakir, M.Pd	Dr. H. Ahmad Barizi, MA
NIP. 19751006 200312 1 001	NIP.19731212 199803 1 001

Mengetahui,
Ketua Jurusan Matematika

Abdussakir, M.Pd
NIP. 19751006 200312 1 001

PENGGUNAAN KRIPTOGRAFI KURVA ELIPTIK PADA PROSES PENYANDIAN ELGAMAL

SKRIPSI

Oleh:
FEBRINA MEDIAWATI SETYOBUDI
NIM. 09610007

Telah Dipertahankan di Depan Dewan Penguji Skripsi dan
Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Sains (S.Si)
Tanggal: 2 Maret 2013

Penguji Utama	: Dr. Usman Pagalay, M.Si NIP. 19650414 200312 1 001	_____
Ketua Penguji	: Abdul Aziz, M.Si NIP. 19760318 200604 1 002	_____
Sekretaris Penguji	: Abdussakir, M.Pd NIP. 19751006 200312 1 001	_____
Anggota Penguji	: Dr. H. Ahmad Barizi, M.A NIP.19731212 199803 1 001	_____

Mengesahkan,
Ketua Jurusan Matematika

Abdussakir, M.Pd
NIP. 19751006 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Febrina Mediawati Setyobudi

NIM : 09610007

Jurusan : Matematika

Fakultas : Sains dan Teknologi

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambil alihan data, tulisan atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 13 Februari 2013
Yang membuat pernyataan,

Febrina Mediawati Setyobudi
NIM. 09610007

MOTTO

Waktu adalah rahasia. Kebahagian dan kesedihan bisa datang dan pergi bersamanya. Lakukan sekarang, sebelum waktu itu hilang…

HALAMAN PERSEMBAHAN

Penulis persembahkan karya ini kepada:

Ayahanda "Bambang Dwi S" dan ibunda "Ella Nora A.H" atas kerja keras, kasih sayang, dukungan, serta doa yang tak pernah putus…

Dan juga para guru yang telah memberikan bekal ilmu yang bermanfaat...

KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

Assalamualaikum.wr.wb

Segala puji bagi Allah SWT yang telah memberikan segala kemudahan dan ridho-Nya sehingga penulis mampu menyelesaikan studi di Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang sekaligus menyelesaikan penulisan skripsi dengan judul *"Penggunaan Kriptografi Kurva Eliptik pada Proses Penyandian Elgamal"* dengan baik. Sholawat dan salam penulis persembahkan kepada Nabi Muhammad, keluarga, dan para sahabat beliau. Semoga penulis dapat meneladani beliau dalam berakhlaq.

Ucapan terima kasih penulis haturkan pada berbagai pihak yang telah membantu selesainya skripsi ini. Dengan iringan syukur penulis mengucapkan terima kasih kepada:

1. Prof. Dr. H. Imam Suprayogo, selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Prof. Drs. Sutiman Bambang Sumitro, SU., D.Sc, selaku Dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Abdussakir, M.Pd, selaku Ketua Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang dan

sebagai pembimbing I, yang telah memberikan bimbingan dengan baik sehingga penulis dapat menyelesaikan skripsi ini.

4. Dr. H. Ahmad Barizi, M.A selaku pembimbing II, atas arahan selama penyusunan skripsi ini.
5. Seluruh dosen dan staf administrasi Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan ilmu pengetahuan pada penulis.
6. Bapak dan Ibu tercinta serta segenap keluarga yang telah banyak berkorban secara materiil dan moril serta doa mereka yang mengiringi langkah-langkah penulis dalam menjalankan studi.
7. Semua teman-teman matematika angkatan 2009, khususnya Iswahyuni Purwanti, Arni Hartanti, Tutik Rosidatul A, Novita Imroatus S, dan Siti Mutmainah, yang selalu memberikan dukungan serta selalu bersama penulis dalam suka dan duka selama mencari ilmu di kampus tercinta.
8. Penghuni kost "Islamiyah", khususnya Heni, Khotim, Linda, Miftah, Devita, Tia, atas doa dan dukunganya.
9. Semua pihak yang tidak mungkin penulis sebut satu persatu, atas keikhlasan bantuan moral dan spiritual, penulis ucapkan terima kasih.

Semoga skripsi ini memberikan manfaat kepada para pembaca khususnya bagi penulis secara pribadi *Amin.*

Wassalamualaikum Wr. Wb.

Malang, Februari 2013

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ABSTRAK

Setyobudi, Febrina Mediawati. 2013. **Penggunaan Kriptografi Kurva Eliptik Pada Proses Penyandian Elgamal**. Skripsi. Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Abdussakir, M.Pd. (II) Dr. H. Ahmad Barizi, M.A.

Kata kunci: kriptografi, kurva eliptik, medan berhingga prima, Elgamal ECC

Kriptografi kurva eliptik termasuk sistem kriptografi kunci asimetris yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Ada beberapa cara yang digunakan untuk mendefinisikan persamaan kurva eliptik yang tergantung berdasarkan pada medan berhingga yang digunakan, yaitu medan berhingga prima (F_p, dimana $p > 3$) atau karakteristik dua medan berhingga (F_{2^m}). Kriptografi kurva eliptik dapat digunakan untuk beberapa keperluan seperti protokol, tanda tangan digital, dan skema enkripsi.

Inti dari skripsi ini adalah melakukan proses penyandian menggunakan algoritma dari Elgamal ECC. Elgamal ECC atau Elgamal *Elliptic Curve Cryptography* adalah contoh dari penggunaan kriptografi kurva eliptik untuk keperluan skema enkripsi.

Hasil dari skripsi ini adalah didapatkannya kode yang merupakan hasil dari proses enkripsi dan dekripsi menggunakan algoritma dari Elgamal ECC. Untuk mendapatkan hasil tersebut maka yang perlu dilakukan adalah (1) menentukan elemen kurva eliptik, (2) merepresentasikan titik dengan simbol, (3) menentukan kunci publik dan kunci privat, (4) melakukan proses enkripsi, (5) melakukan proses dekripsi.

Pembahasan dalam skripsi ini hanya meliputi tentang kurva eliptik pada medan berhingga prima saja, maka untuk skripsi selanjutnya dapat melakukan pembahasan mengenai kurva eliptik pada karakteristik dua medan berhingga (F_{2^m}) atau aplikasi kriptografi kurva eliptik pada bidang lainnya.

ABSTRACT

Setyobudi, Febrina Mediawati. 2013. **The use of Elliptic Cuve Cryptography on Elgamal Encryption**. Thesis. Department of Mathematics Faculty of Science and Technology The State of Islamic University Maulana Malik Ibrahim Malang.
Promotor: (I) Abdussakir, M.Pd. (II) Dr. H. Ahmad Barizi, M.A.

Keywords: cryptography, elliptic curve, prime finite fields, Elgamal ECC

Elliptic curve cryptography is asymmetric key cryptography system that bases its security on elliptic curve mathematical problems. There are several methods used to define the elliptic curve equation that depends based on the finite fields are used, the prime finite field (F_p, where $p > 3$) or characteristic two finite fields (F_{2^m}). Elliptic curve cryptography can be used for multiple purposes such as key exchange protocol, digital signature and encryption schemes.

The core of this research is the process of Elgamal encryption using ECC algorithm. ECC or Elgamal Elliptic Curve Cryptography is an example of the use of elliptic curve cryptography for encryption schemes purposes.

The results of this study are the result of the acquisition of the encryption and decryption of Elgamal ECC algorithm. To obtain these results it is necessary to do the following steps, including (1) determining element elliptic curves, (2) represents a point with a symbol, (3) determine the public key and private key, (4) perform the encryption process, (5) conduct decryption process.

The discussion in this study just about the elliptic curve on prime finite field, then for further research to examine the elliptic curve in characteristic two finite fields (F_{2^m}) or elliptic curve cryptography applications in other fields.

الملخص

ستيوبود , فبرينا مدياوة. ٢٠١٣. **استخدام الترميز منحنى الاهليلجيه هو عملية التشفير الجمل**. البحث العلم. قسم الرياضيات. كلية العلوم والتكنولوجيا. جامعة الإسلامية الحكومية مولانا مالك إبراهيم مالانج. المشرف: (١) عبد الشاكرالماجستر (٢)الدكتور الحج أحمد بارز الماجستر

كلمات البحث: الترميز، منحنى الاهليلجيه، رئيس حقول محدودة، الجمل تشفير المنحنى الاهليلجيه

بما في ذلك نظام منحنى الاهليلجيه تشفير غير متماثل تشفير المفتاح أن القواعد الامنية على منحنى الاهليلجيه المشاكل الرياضية. هناك العديد من الطرق المستخدمة لتحديد المعادلة منحنى الاهليلجيه التي تعتمد على أساس مجالات محدودة واستخدامها، مجال محدود الوزراء أو في ميدان محدود من اثنين مميزة. ويمكن استخدام الترميز منحنى الاهليلجيه لأغراض متعددة مثل بروتوكول تبادل المفاتيح، التوقيع الرقمي والتشفير مخططات.

جوهر هذا البحث هو عملية استخدام خوارزمية التشفير من الجمل تشفير المنحنى الاهليلجيه .الجمل تشفير المنحنى الاهليلجيه هو مثال على استخدام الترميز منحنى الاهليلجيه لأغراض مخططات التشفير.

نتائج هذه الدراسة هي نتيجة لاكتساب التشفير وفك التشفير باستخدام خوارزمية تشفير من الجمل منحنى الاهليلجيه. للحصول على هذه النتائج لا بد من القيام بالخطوات التالية، بما في ذلك (١) منحنيات العنصر تحديد بيضاوي الشكل، (٢) يمثل نقطة مع رمز، (٣) تحديد المفتاح العام والمفتاح الخاص، (٤) تنفيذ عملية التشفير، (٥) السلوك فك التشفير العملية.

المناقشة في هذه الدراسة تغطي فقط حوالي المنحنيات الاهليلجيه في مجالات محدودة فقط رئيس، ثم يمكن للبحوث في المستقبل دراسة منحنى الاهليلجيه في ميدانيين مميزة محدود أو الاهليلجيه تطبيقات الترميز منحنى في مجالات أخرى.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi (*Cryptography*) merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi (*encrypt*) maupun dekripsi (*decrypt*) data. Teknik ini digunakan untuk mengubah data ke dalam kode-kode tertentu dengan tujuan agar informasi yang disimpan tidak dapat dibaca oleh siapapun kecuali orang-orang yang berhak. Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama maupun untuk privasi individu. Maka sudah seharusnya informasi hanya boleh disampaikan kepada orang yang berhak menerimanya saja, seperti penggalan firman Allah berikut:

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الأَمَانَاتِ إِلَى أَهْلِهَا...

Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya….(Q.S An-Nisa:58).

Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Salah satu sistem pengamanan yang dapat dimanfaatkan ialah sistem kriptografi kurva eliptik. Kriptografi kurva eliptik termasuk kedalam sistem kriptografi algoritma asimetris yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Pada sistem ini digunakan masalah logaritma diskrit kurva eliptik dengan menggunakan grup

kurva eliptik. Struktur kurva eliptik digunakan sebagai grup operasi matematis untuk melangsungkan proses enkripsi dan dekripsi. Kriptografi kurva eliptik mempunyai keuntungan jika dibandingkan dengan kriptografi algoritma asimetris lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama.

Penelitian mengenai kriptografi sudah banyak bermunculan, salah satunya yaitu *"An Application of Discrete Algorithms in Asymetric Cryptography"* dari F. Amounas dan H. El Kinani (2011). Pada jurnal penelitian tersebut membahas tentang aplikasi penyebaran kunci publik berdasarkan keamanan tergantung pada kesulitan masalah logaritma diskrit kurva eliptik. Secara khusus, jurnal milik F. Amounas ini memberikan contoh dari proses penyandian Elgamal berdasarkan kurva eliptik yang diberikan sebagai berikut: $y^2 = x^3 + 70x + 57\ (mod\ 73)$. Dari persamaan tersebut didapatkan 74 titik kurva dan akan direpresentasikan kedalam simbol alfabet yang sangat dibutuhkan dalam proses penyandian pesan.

Kurangnya penjelasan secara matematis dan banyaknya titik kurva yang digunakan dalam proses penyandian menyebabkan contoh yang diberikan menjadi sulit untuk dimengerti. Berdasarkan dari kekurangan penjelasan dalam penelitian sebelumnya tersebut, maka penulis ingin mempelajari lebih dalam lagi mengenai kriptografi kurva eliptik dan memberikan contoh yang lebih sederhana tentang penggunaan kriptografi kurva eliptik pada proses penyandian Elgamal agar lebih mudah dipahami. Sehingga penulis mengambil judul ***"Penggunaan Kriptografi Kurva Eliptik pada Proses Penyandian Elgamal"*** sebagai penelitian untuk tugas akhir.

1.2 Rumusan Masalah

Merujuk pada latar belakang, maka dapat dirumuskan masalah yang berkaitan dengan penjelasan di atas yaitu:

1. Apa hasil dari proses enkripsi menggunakan kriptografi kurva eliptik pada proses penyandian Elgamal?
2. Apa hasil dari proses dekripsi menggunakan kriptografi kurva eliptik pada proses penyandian Elgamal?

1.3 Tujuan

Dari rumusan masalah yang telah dipaparkan di atas, maka tujuan penulisan skripsi ini adalah untuk:

1. Mengetahui hasil dari proses enkripsi menggunakan kriptografi kurva eliptik pada proses penyandian Elgamal.
2. Mengetahui hasil dari proses dekripsi menggunakan kriptografi kurva eliptik pada proses penyandian Elgamal.

1.4 Batasan Masalah

Untuk memfokuskan pembahasan, maka pada skripsi ini hanya membahas penggunaan kriptografi kurva eliptik pada proses penyandian Elgamal. Persamaan kurva eliptik yang digunakan terbatas pada medan berhingga *(finite field)* prima F_p. Pada proses penyandian, penulis menggunakan 37 karakter yang terdiri dari 26 karakter berupa huruf alfabet ‘A’ sampai ‘Z’ dan 10 karakter berupa angka ‘0’

sampai ‘9’ ditambah dengan satu titik khusus yaitu titik tak hingga yang akan direpresentasikan sebagai ‘spasi’, sehingga dibutuhkan 37 titik kurva eliptik.

1.5 Manfaat

Penulisan skripsi ini diharapkan bermanfaat sebagai berikut:

1. Bagi penulis, menambah wawasan penulis untuk mengetahui tentang aplikasi kriptografi kurva eliptik pada proses penyandian.
2. Bagi lembaga, menambah bahan kepustakaan dan informasi pembelajaran mata kuliah yang berhubungan dengan kriptografi terutama kriptografi kurva eliptik.
3. Bagi mahasiswa, menambah pengetahuan keilmuan mengenai kriptografi terutama kriptografi kurva eliptik.

1.6 Metode Penelitian

Metode yang digunakan dalam skripsi ini adalah metode kajian pustaka *(library research)* yaitu dengan mengumpulkan data dan informasi dari berbagai sumber seperti buku, jurnal penelitian, tesis, disertasi, skripsi, laporan penelitian, maupun diskusi-diskusi ilmiah.

Untuk mencapai tujuan yang diinginkan maka langkah-langkah yang dilakukan adalah:

1. Mengumpulkan data yang berupa teori dasar mengenai kriptografi kurva eliptik.
2. Menentukan persamaan kurva eliptik pada medan *(field)* berhingga prima F_p.

3. Menentukan elemen-elemen grup eliptik $E(F_p)$ dengan cara menghitung nilai residu kuadrat modulo p kemudian membandingkannya dengan nilai dari $y^2 = x^3 + ax + b \ (mod\ p)$.
4. Menentukan nilai P sebagai generator dari grup eliptik $E(F_p)$.
5. Menentukan domain kurva eliptik.
6. Mencari algoritma kriptografi kurva eliptik pada skema enkripsi Elgamal.
7. Merepresentasikan titik-titik kurva eliptik dengan simbol yang diinginkan.
8. Menentukan kunci yang akan digunakan.
9. Melakukan proses enkripsi terhadap pesan yang akan disampaikan.
10. Melakukan proses dekripsi pesan.

1.7 Sistematika Penulisan

Untuk mempermudah dalam memahami skripsi ini, penulis menggunakan sistematika penulisan empat bab, masing-masing bab dijelaskan sebagai berikut:

Bab I: Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan, batasan masalah, manfaat, metode penelitian, dan sistematika penulisan.

Bab II: Kajian Pustaka

Bab ini berisi tentang kajian pustaka yang mendukung pembahasan skripsi ini, yaitu tentang konsep dasar matematika kriptografi, kriptografi, dan kurva eliptik.

Bab III: Pembahasan

Pada bab ini membahas tentang pembentukan persamaan kurva eliptik pada medan berhingga prima, menentukan elemen grup eliptik modulo prima, elemen pembangkit dari grup eliptik, parameter domain kurva eliptik, algoritama Elgamal ECC dan melakukan implementasi dalam proses penyandian pesan menggunakan Elgamal ECC.

Bab IV: Penutup

Bab ini berisi tentang kesimpulan penelitian dan saran bagi pembaca yang akan melanjutkan penelitian dalam skripsi ini.

BAB II

KAJIAN PUSTAKA

2.1 Konsep Dasar Matematika Kriptografi

Dalam kehidupan sehari-hari, matematika sering digunakan untuk membantu menyelesaikan permasalahan. Mulai dari masalah kecil dan tradisional, hingga masalah besar dan modern. Sehingga tidak heran bila ilmu matematika menjadi ilmu yang wajib untuk dipelajari. Bahkan dalam Al-Qur'an, matematika juga diajarkan oleh Allah kepada manusia secara tidak langsung. Di antara ayat-ayat yang menjelaskan tentang adanya ilmu matematika adalah Al-Qur'an surat Al-Kahfi ayat 25 berikut:

وَلَبِثُوا۟ فِى كَهْفِهِمْ ثَلَٰثَ مِا۟ئَةٍ سِنِينَ وَٱزْدَادُوا۟ تِسْعًا ﴿٢٥﴾

Dan mereka tinggal dalam gua mereka tiga ratus tahun dan ditambah sembilan tahun (lagi) (QS. Al-Kahfi:25).

Dari ayat tersebut terdapat operasi penjumlahan yaitu tiga ratus tahun dan ditambah sembilan tahun yang merupakan konsep dasar dari matematika. Untuk mempermudah pernyataan tersebut dalam ilmu matematika sering dinotasikan dengan menggunakan simbol-simbol baik berupa angka, huruf, ataupun simbol matematika lainnya.

Mengingat begitu pentingnya ilmu matematika maka sebelum membahas lebih jauh mengenai kriptografi kurva eliptik terlebih dahulu akan dipaparkan konsep dasar matematika yang berhubungan dengan persoalan kriptografi.

2.1.1 Teori Bilangan

Teori bilangan menjadi salah satu teori yang mendasari pemahaman kriptografi, khususnya teori bilangan bulat. Teori bilangan bulat dalam matematika diskrit memberikan penekanan dengan sifat pembagian. Sifat pembagian pada bilangan bulat melahirkan konsep-konsep seperti bilangan prima dan aritmetika modulo. Satu algoritma penting yang berhubungan dengan sifat pembagian ini adalah algoritma Euclidean. Bilangan prima, aritmetika modulo, dan algoritma Euclidean memainkan peran yang penting dalam ilmu kriptografi.

2.1.1.1 Bilangan Bulat dan Sifat-Sifat Pembagian

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal. Himpunan semua bilangan bulat dinotasikan dengan $\mathbb{Z}$ yang diambil dari kata *Zahlen* dari bahasa Jerman atau dinotasikan dengan I yang diambil dari huruf pertama kata *Integer* dari bahasa Inggris, adalah himpunan $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. Selanjutnya dalam penulisan skripsi ini penulis menggunakan notasi $\mathbb{Z}$ sebagai simbol untuk bilangan bulat.

Sifat-sifat yang berkaitan dengan keterbagian *(divisibility)* merupakan dasar pengembangan teori bilangan. Jika suatu bilangan bulat dibagi oleh suatu bilangan bulat yang lain, maka hasil pembagiannya adalah bilangan bulat atau bukan bilangan bulat (Hamidah, 2009).

Definisi 2.1.1.1.1

Misalnya $a, b \in \mathbb{Z}$, dengan $a \neq 0$. a dikatakan membagi b, ditulis $a|b$, jika dan hanya jika $b = ax$, untuk suatu $x \in \mathbb{Z}$ (Abdussakir, 2009:114).

Dalam penulisan skripsi ini, notasi $a|b$ dibaca a membagi b, b habis dibagi a, a faktor b, atau b kelipatan dari a. Sedangkan notasi $a \nmid b$ dibaca a tidak membagi b, b tidak habis dibagi a, a bukan faktor b, atau b bukan kelipatan dari a.

Contoh:

a. $5|20$ karena ada $4 \in \mathbb{Z}$, sehingga $20 = 5 \cdot 4$.

b. $5 \nmid 13$ karena $13 \neq 5 \cdot x$, untuk setiap $x \in \mathbb{Z}$.

Definisi 2.1.1.1.2 (Algoritma Pembagian)

Jika $a, b \in \mathbb{Z}$, dan $a > 0$, maka ada bilangan-bilangan $q, r \in \mathbb{Z}$ yang masing-masing tunggal sehingga $b = q \cdot a + r$ dengan $0 \leq r \leq a$. Jika $a \nmid b$, maka r memenuhi ketidaksamaan $0 < r < a$ (Muhsetyo, 1997:50).

Dalam definisi di atas, yaitu $b = aq + r$, $0 \leq r < a$. b disebut bilangan yang dibagi *(dividend)*, a disebut pembagi *(devisor)*, q disebut hasil bagi *(quotient)*, dan r disebut sisa pembagi *(remainder)*.

2.1.1.2 Algoritma Euclidean

Algoritma Euclidean adalah salah satu metode yang digunakan untuk mencari nilai Faktor Persekutuan Terbesar (FPB) dari dua bilangan bulat. Algoritma ini sudah dikenal sejak berabad-abad yang lalu.

Definisi 2.1.1.2.1

Ditentukan $x, y \in \mathbb{Z}$, x dan y keduanya tidak bersama-sama bernilai 0. $a \in \mathbb{Z}$ disebut pembagi (faktor) persekutuan *(common divisor, common factor)*

dari x dan y jika a adalah bilangan bulat positif terbesar yang membagi x (yaitu $a|x$) dan membagi y (yaitu $a|y$) (Muhsetyo, 1997:60).

Untuk selanjutnya, FPB dari a dan b dinotasikan dengan (a, b).

Teorema 2.1.1.2.1 (Algoritma Euclidean)

Misalkan a dan b adalah bilangan bulat dengan $a > 0$. Dengan melakukan pengulangan algoritma pembagian sampai diperoleh sisa pembagi 0. Akan didapatkan urutan persamaan berikut:

$$b = aq_1 + r_1, \quad 0 \le r_1 \le a$$
$$a = r_1q_2 + r_2, \quad 0 \le r_2 \le r_1$$
$$r_1 = r_2q_3 + r_3, \quad 0 \le r_3 \le r_2$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \le r_n \le r_{n-1}$$
$$r_{n-1} = r_nq_{n-1},$$

Maka, $(a, b) = r_n$ dan r_n adalah sisa pembagian yang tidak nol (Abdussakir, 2009:125).

Bukti:

Telah diketahui bahwa r_n adalah sisa pembagian terakhir yang tidak nol.

Jadi $r_n > 0$.

Untuk membuktikan $r_n = (a, b)$ harus menunjukkan bahwa $r_n|a$ dan $r_n|b$, serta jika $k|a$ dan $k|b$ maka $k|r_n$.

Berdasarkan pernyataan terakhir, yaitu $r_{n-1} = r_nq_{n-1}$, maka diperoleh $r_n|r_{n-1}$

Karena $r_{n-2} = r_{n-1}q_n + r_n$, maka diperoleh:

$r_{n-2} = r_{n-1}q_n + r_n$

$= (r_n q_{n+1}) q_n + r_n$

$= r_n(q_{n+1} q_n + 1)$

$= r_n p_1$, dengan $p_1 = q_{n+1} q_n + 1$

Jadi, $r_n | r_{n-3}$.

Dengan melanjutkan proses ini akan didapatkan bahwa

$r_n | r_{n-4}, r_n | r_{n-5}, \dots, r_n | r_2, r_n | r_1, r_n | a,$ dan $r_n | b$

Jadi, terbukti bahwa $r_n | a$ dan $r_n | b$

Misalkan $k | a$ dan $k | b$

Maka $k | b - aq_1$

Karena $r_1 = b - aq_1$ maka $k | r_1$

Karena $k | r_1$ dan $k | a$ maka $k | a - r_1 q_2$. Jadi $k | r_2$

Karena $k | r_1$ dan$k | r_2$ maka $k | r_1 - r_2 q_3$. Jadi $k | r_3$

Dengan melanjutkan proses ini maka akan didapatkan bahwa:

$$k | r_3, k | r_4, \dots, k | r_{n-1}, \text{dan } k | r_n$$

Terbukti bahwa $r_j = (a, b)$.

Contoh:

Akan dihitung $(1938, 570)$ menggunakan algoritma Euclidean

Jawab:

$1938 = 3 \cdot 570 + 228 \quad 0 \leq 228 \leq 570$

$570 = 2 \cdot 228 + 114 \quad 0 \leq 114 \leq 228$

$228 = 2 \cdot 114$

Jadi, $(1938, 570) = 114$

2.1.1.3 Aritmetika Modulo dan Kekongruenan

Definisi 2.1.1.3.1

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a \bmod m$, bilangan m disebut modulus atau modulo. Dan hasil aritmetika modulo m terletak di dalam himpunan $\{0,1,2,\dots,m-1\}$. $a\ (mod\ m) \equiv r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$ (Munir, 2006:38).

Aritmetika modulo mulai digunakan pada kriptografi karena dua alasan:

1. Karena nilai-nilai aritmetika modulo berada pada himpunan berhingga (0 sampai modulo m-1), maka hasilnya selalu di dalam himpunan.
2. Karena bekerja dengan bilangan bulat, maka tidak akan kehilangan informasi akibat pembulatan *(round off)* sebagaimana operasi bilangan real (Hamidah, 2009).

Definisi 2.1.1.3.2

Diketahui $a, b, m \in \mathbb{Z}$. a disebut kongruen dengan b modulo m, ditulis $a \equiv b(mod\ m)$, jika $(a - b)$ habis dibagi m, yaitu $m|(a - b)$. Jika $(a - b)$ tidak habis dibagi m, yaitu $m \nmid (a - b)$, maka ditulis $a \not\equiv b(mod\ m)$, dibaca a tidak kongruen dengan b modulo m. Karena $(a - b)$ habis dibagi oleh m jika dan hanya jika $(a - b)$ habis dibagi oleh $-m$, maka: $a \equiv b(mod\ m)$ jika dan hanya jika $b \equiv a(mod\ m)$ (Muhsetyo, 1997:138).

Contoh:

a. $23 \equiv 3(mod\ 5)$ (5 habis membagi $23 - 3 = 20 \longrightarrow 20 \div 5 = 4$)

b. $12 \equiv 4(mod\ 5)$ (5 tidak habis membagi $12 - 4 = 8$)

Definisi 2.1.1.3.3

Jika $k, p \in \mathbb{Z}, p > 0$ dan $(k, p) = 1$, maka:

1. k disebut residu kuadratis modulo p jika kongruensi $x^2 \equiv k(mod\ p)$ mempunyai penyelesaian.
2. k disebut bukan residu kuadratis modulo p jika kongruensi $x^2 \equiv k(mod\ p)$ tidak mempunyai penyelesaian (Muhsetyo, 1997:214).

Contoh:

Tentukan residu kuadratis modulo 5.

Jawab:

Anggota dari modulo 5 adalah 0, 1, 2, 3, 4 maka:

$0^2 = 0 \equiv 0\ (mod\ 5)$ $\quad$ $3^2 = 9 \equiv 4\ (mod\ 5)$

$1^2 = 1 \equiv 1\ (mod\ 5)$ $\quad$ $4^2 = 16 \equiv 1\ (mod\ 5)$

$2^2 = 4 \equiv 4\ (mod\ 5)$

Kelima keadaan di atas menunjukkan bahwa kongruensi-kongruensi:

$x^2 \equiv 1\ (mod\ 5)$ mempunyai penyelesaian yaitu $x = 1$ dan $x = 4$

$x^2 \equiv 4\ (mod\ 5)$ mempunyai penyelesaian yaitu $x = 2$ dan $x = 3$

Jadi residu kuadratis modulo 5 adalah 1 dan 4.

2 bukan residu kuadratis modulo 5 karena $x^2 \equiv 2\ (mod\ 5)$ tidak mempunyai penyelesaian.

2.1.1.4 Bilangan Prima

Definisi 2.1.1.4.1

Jika p suatu bilangan bulat positif lebih dari 1 yang hanya mempunyai pembagi positif 1 dan p, maka p disebut bilangan prima. Jika suatu bilangan bulat $q > 1$ bukan suatu bilangan prima, maka q disebut bilangan komposit (Muhsetyo,1997:92).

Dari definisi di atas bilangan prima termasuk bilangan yang sangat istimewa karena bilangan prima hanya habis dibagi dengan bilangan satu atau bilangan itu sendiri. Keistimewaan tersebut melambangkan sifat keesaan Allah yang tidak dibagikan kepada siapapun juga kecuali bagi diri-Nya sendiri. Seperti yang tercantum dalam surat Al-Ikhlas berikut:

قُلْ هُوَ ٱللَّهُ أَحَدٌ ۝١ ٱللَّهُ ٱلصَّمَدُ ۝٢ لَمْ يَلِدْ وَلَمْ يُولَدْ ۝٣ وَلَمْ يَكُن لَّهُۥ كُفُوًا أَحَدٌۢ ۝٤

Katakanlah: "Dia-lah Allah, yang Maha Esa.Allah adalah Tuhan yang bergantung kepada-Nya segala sesuatu. Dia tiada beranak dan tidak pula diperanakkan, Dan tidak ada seorangpun yang setara dengan Dia." (Al-Ikhlas:1-4).

Surat tersebut menjelaskan bahwa Allah itu Maha Esa, tidak ada yang serupa dengan-Nya, tidak ada yang sebanding dengan-Nya, tidak memiliki istri ataupun anak, dan tidak ada sekutu bagi-Nya.

Bilangan prima dalam matematika diyakini merupakan salah satu misteri alam semesta, karena hingga era komputer sekarang ini bilangan prima banyak dimanfaatkan sebagai sistem kodifikasi (penyandian) berbagai hal yang bersifat penting dan rahasia.

2.1.2 Aljabar Abstrak

Selain teori bilangan, cabang dari ilmu matematika yang berperan bagi ilmu kriptografi adalah aljabar abstrak. Materi yang dibahas dan dikembangkan dalam aljabar abstrak sangat banyak. Salah satunya adalah struktur aljabar yang pada dasarnya membahas tentang himpunan dan operasinya. Dari konsep himpunan tersebut akan berkembang menjadi bahasan yang lebih luas seperti grup, gelanggang, dan juga medan.

2.1.2.1 Grup

Suatu sistem aljabar $(G,*)$ memuat himpunan tak kosong G dan operasi biner $*$ disebut grup jika memenuhi sifat-sifat berikut:

1. Operasi $*$ bersifat asosiatif: $(a * b) * c = a * (b * c), \forall a, b, c \in G$
2. Operasi $*$ memiliki identitas: Ada sebuah elemen e di G sedemikian hingga

   $$a * e = e * a = a, \forall a \in G$$

   Pada grup penjumlahan, elemen identitas disimbolkan dengan 0. Sedangkan pada grup perkalian elemen identitas disimbolkan dengan 1.
3. Operasi $*$ memiliki invers: Untuk setiap a di G, ada sebuah elemen a^{-1} di G sedemikian hingga:

   $$a * a^{-1} = a^{-1} * a = e$$

   dimana e adalah identitas elemen di G. Pada grup penjumlahan, invers dari a dinyatakan sebagai $-a$. Sedangkan pada grup perkalian, invers a dinyatakan sebagai a^{-1} (Raisinghania dan Aggarwal, 1980:31).

Suatu grup disebut grup abelian atau grup komutatif jika operasi $*$ bersifat komutatif: $a * b = b * a, \forall a, b \in G$ (Raisinghania dan Aggarwal, 1980:31). Sebuah grup memiliki jumlah elemen berhingga disebut grup berhingga *(finite group)* dan order dari grup itu adalah banyak elemen dalam grup tersebut .

Suatu grup $(G,*)$ disebut grup siklik jika dan hanya jika terdapat $a \in G$ sedemikian sehingga setiap elemen dari G dapat dituliskan sebagai perpangkatan dari a *(integral power of a)* (Raisinghania dan Aggarwal, 1980:97). Dalam kasus ini elemen a disebut generator atau pembangkit pada grup dan ditulis sebagai $G = \langle a \rangle$ atau $G = \{a^n | n \in Z\}$, yang artinya grup G dibangkitkan oleh a.

Contoh:

Diberikan grup (M_6 , +) dengan M = {0, 1, 2, 3, 4, 5 }. Tentukan pembangkit dari grup tersebut.

Jawab:

1 = 1 …….... $1 = 1^1$
1 + 1 = 2 ……..... $2 = 1^2$
1 + 1 + 1 = 3 …….. $3 = 1^3$
1 + 1 + 1 + 1 = 4 …… $4 = 1^4$
1 + 1 + 1 + 1 + 1 = 5 …….. $5 = 1^5$
1 + 1 + 1 + 1 + 1 + 1 = 6 …. $6 = 1^6$

1 adalah generator karena 1 membangkitkan semua elemen M_6.

2 = 2
2 + 2 = 4
2 + 2 + 2 = 0
2 + 2 + 2 + 2 = 2
2 + 2 + 2 + 2 + 2 = 4
2 + 2 + 2 + 2 + 2 + 2 = 0

2 hanya membangkitkan 0, 2, 4 dan tidak membangkitkan 1, 3, 5 berarti 2 bukan generator M

Dengan cara yang sama dapat diketahui bahwa:

3 hanya membangkitkan 0 dan 3 yang berarti 3 bukan generator dari M_6

4 hanya membangkitkan 0, 2 dan 4 yang berarti 4 bukan generator dari M_6

5 membangkitkan 0,1,2,3,4,5 yang berarti 5 adalah generator dari M_6

0 hanya membangkitkan 0 yang berarti 0 bukan generator dari M_6

Karena M_6 dibangkitkan oleh 1 dan 5 maka ditulis sebagai $M_6 = \langle 1 \rangle = \langle 5 \rangle$

2.1.2.2 Gelanggang *(Ring)*

Definisi 2.1.2.2.1

Misalkan R adalah suatu himpunan tak kosong dengan dua operasi biner yang didefinisikan dengan penjumlahan dan perkalian. Maka sistem $(R, +, \times)$ disebut *ring* jika memenuhi sifat-sifat berikut:

1. $(R, +)$ adalah grup abelian
2. Operasi $\times$ bersifat asosiatif: $(a \times b) \times c = a \times (b \times c), \forall a, b, c \in R$
3. Operasi $\times$ bersifat distributif terhadap operasi $+$ baik distributif kiri maupun kanan:

$$a \times (b + c) = (a \times b) + (a \times c), \forall a, b, c \in R \quad \ldots\text{Distributif Kanan}$$

$$(a + b) \times c = (a \times c) + (b \times c), \forall a, b, c \in R \quad \ldots\text{Distributif Kiri}$$

(Raisinghania dan Aggarwal, 1980:313)

Definisi 2.1.2.2.2

Suatu *ring* $(R, +, \times)$ disebut *Ring Komutatif* (RK) jika dan hanya jika operasi kedua (operasi $\times$) bersifat komutatif di R (Raisinghania dan Aggarwal, 1980:314).

Definisi 2.1.2.2.3

Suatu *ring* $(R, +, \times)$ disebut *Ring dengan Elemen Satuan (RS)* jika dan hanya jika R punya elemen identitas terhadap operasi kedua (operasi $\times$) (Raisinghania dan Aggarwal, 1980:314).

Definisi 2.1.2.2.4

Suatu *ring* $(R, +, \times)$disebut *Ring Komutatif dengan Elemen Satuan (RKS)* jika dan hanya jika operasi kedua bersifat komutatif dan *R* punya elemen identitas terhadap operasi kedua, dengan kata lain merupakan *Ring Komutatif* (RK) sekaligus *Ring dengan Elemen Satuan* (RS) (Raisinghania dan Aggarwal, 1980:314).

Definisi 2.1.2.2.5

Suatu *ring* $(R, +, \times)$ disebut dengan pembagi nol (DPN) jika terdapat dua elemen $a, b \in R$ sedemikian sehingga $a \neq 0, b \neq 0$ dan $a \times b = 0$ (Raisinghania dan Aggarwal, 1980:314).

Definisi 2.1.2.2.6

Suatu *ring* $(R, +, \times)$ disebut tanpa pembagi nol (TPN) jika tidak mungkin untuk menemukan dua elemen $a, b \in R$ sedemikian sehingga $a \neq 0, b \neq 0$ dan $a \times b = 0$. Dengan kata lain $(R, +, \times)$ disebut tanpa pembagi nol jika dan hanya jika $a \times b = 0 \Rightarrow a = 0$ atau $b = 0$ (Raisinghania dan Aggarwal, 1980:314).

Definisi 2.1.2.2.7

Suatu *ring* disebut integral domain jika *ring* komutatif (RK), dengan elemen satuan (RS) dan tanpa pembagi nol (TPN) (Raisinghania dan Aggarwal, 1980:314).

Definisi 2.1.2.2.8

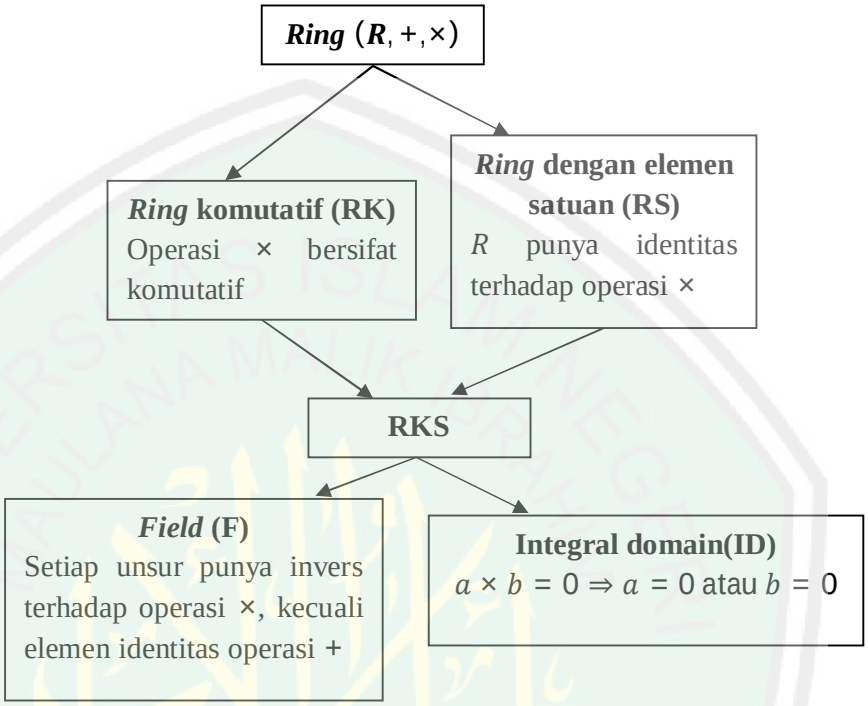
Suatu *ring* $(R, +, \times)$ dengan paling sedikit dua elemen disebut medan jika *ring* komutatif dengan elemen satuan (RKS) dan untuk setiap elemen tak nol mempunyai invers terhadap operasi kedua (Raisinghania dan Aggarwal, 1980:314).

Medan berhingga *(finite field)* adalah medan yang memiliki jumlah elemen berhingga. Order pada suatu medan berhingga adalah jumlah elemen pada medan. Terdapat suatu medan berhingga F dengan order q dimana $q = p^m$ untuk p adalah bilangan prima dan m adalah suatu bilangan bulat.

Jika $m = 1$ maka F disebut medan berhingga prima *(prime finite field)* yang dinotasikan dengan F_P. Medan berhingga prima (F_P) adalah suatu medan berhingga yang berisi p elemen. Anggota-anggota dari Fp direpresentasikan sebagai himpunan bilangan bulat dari 0 sampai p-1 atau ditulis {0,1,2,…,p-1} (Hankerson dkk, 2003:26).

Jika $m \geq 2$, maka F disebut medan yang diperluas. Medan berhingga dengan order 2^m disebut dengan medan berhingga biner (*binary finite field)* atau karakteristik dua medan berhingga *(characteristic-two finite fields)* dan dinotasikan dengan F_{2^m} (Hankerson dkk, 2003:26).

Untuk mempermudah memahami tentang *ring* berikut akan diberikan gambar tentang jenis-jenis *ring*:



Gambar 2.1 Jenis-Jenis *Ring*

2.2 Kriptografi

Salah satu contoh kemajuan teknologi komputer yang paling nyata dan dapat digunakan oleh semua orang adalah internet. Karena bisa digunakan oleh semua orang maka tingkat keamanannya relatif rendah, sehingga sangat rawan untuk terjadinya penyadapan informasi oleh pihak-pihak yang tidak berhak untuk mengetahui informasi tersebut. Bagi pengguna internet yang sangat luas, misalnya pada bidang pemerintahan, militer, perbankkan, pendidikan, industri dan lainnya yang kebanyakan mengandung informasi rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Rahasia adalah sebuah amanat dan menjaga rahasia sangat dianjurkan oleh Allah SWT seperti dalam firman-Nya:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu Mengetahui (Al-Anfal:27).

Kriptografi hadir untuk mengatasi masalah keamanan tersebut. Kriptografi merupakan ilmu untuk menyamarkan suatu pesan demi menjaga kerahasiaannya. Berikut akan dipaparkan lebih jelas mengenai kriptografi, sejarah serta macam-macamnya.

2.2.1 Tinjauan Umum Kriptografi

Kriptografi *(cryptography)* berasal dari bahasa Yunani, yang terdiri dari kata *cryptos* yang berarti tersembunyi dan *graphein* yang berarti menulis atau tulisan. Secara terminologi, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2006:9). Sedangkan menurut Schneier (1996) kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim dapat disampaikan kepada penerima dengan aman.

Menurut sejarahnya, kriptografi sudah lama digunakan oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang disebut *scytale*. Alat ini terdiri dari sebuah gulungan pita panjang dari daun *papyrus* yang dililitkan pada batang silinder (Munir, 2010).

Salah satu konsep dari kriptografi adalah kerahasiaan. Allah mempunyai banyak rahasia yang hanya Allah saja yang mengetahuinya. Sebagai contoh, segala rahasia tentang ajal, jodoh, rizki, atau segala rahasia apapun dari masa

depan manusia semuanya sudah tertulis di dalam kitab *Lauhul Mahfudz*. Allah berfirman:

۞ وَعِندَهُۥ مَفَاتِحُ ٱلۡغَيۡبِ لَا يَعۡلَمُهَآ إِلَّا هُوَۚ وَيَعۡلَمُ مَا فِي ٱلۡبَرِّ وَٱلۡبَحۡرِۚ وَمَا تَسۡقُطُ مِن وَرَقَةٍ إِلَّا يَعۡلَمُهَا وَلَا حَبَّةٖ فِي ظُلُمَٰتِ ٱلۡأَرۡضِ وَلَا رَطۡبٖ وَلَا يَابِسٍ إِلَّا فِي كِتَٰبٖ مُّبِينٖ ٥٩

Dan pada sisi Allah-lah kunci-kunci semua yang ghaib; tidak ada yang mengetahuinya kecuali dia sendiri, dan dia mengetahui apa yang di daratan dan di lautan, dan tiada sehelai daun pun yang gugur melainkan dia mengetahuinya (pula), dan tidak jatuh sebutir biji-pun dalam kegelapan bumi, dan tidak sesuatu yang basah atau yang kering, melainkan tertulis dalam Kitab yang nyata (Lauh Mahfudz)"(Al-An'aam:59).

Informasi dari Allah tidak bisa diberitahukan kepada sembarang orang, hanya orang-orang yang terpilih saja yang bisa mengetahui rahasia tersebut. Berikut adalah konsep kriptografi yang juga merupakan aspek keamanan informasi:

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah.
3. Autentikasi, adalah berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri.
4. Non-repudiasi, atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat (Ariyus, 2006:7).

2.2.2 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut . Algoritma kriptografi ini bekerja dalam kombinasi dengan menggunakan kunci *(key)* seperti kata, nomor atau frase tertentu.

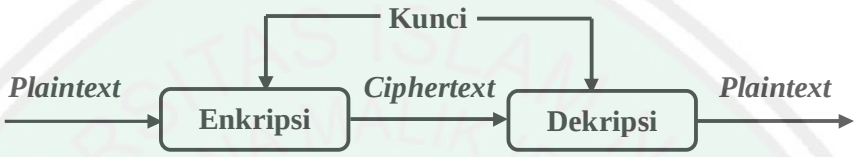
Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu:

1. Enkripsi, merupakan hal yang sangat penting dalam kriptografi yang merupakan pengamanan data yang dikirimkan terjaga rahasianya. Pesan asli disebut plainteks yang dirubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *chipper* atau kode.
2. Dekripsi, merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan kebentuk asalnya *(plaintext)* disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.
3. Kunci, adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi jadi dua bagian yaitu kunci privat *(private key)* dan kunci umum atau kunci publik *(public key)* (Ariyus, 2006:13).

2.2.2.1 Algoritma Simetri

Algoritma ini juga disebut dengan algoritma klasik, karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsinya. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci, jika kunci tersebut diketahui oleh orang lain maka, orang tersebut bisa melakukan enkripsi dan dekripsi

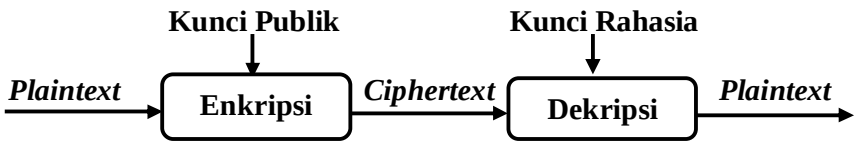
terhadap pesan tersebut. Algoritma yang memakai kunci simetri diantaranya adalah *Data Encryption Standart* (DES), *International Data Encryption Algorithm* (IDEA), *Advanced Encryption Standart* (AES), *One Time Pad* (OTP), dan lain sebagainya (Ariyus, 2006:14). Secara sederhana proses pengiriman pesan dengan algoritma simetris dapat digambarkan sebagai berikut:



Gambar 2.2 Skema Algoritma Simetri

2.2.2.2 Algoritma Asimetri

Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsinya berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu kunci publik *(public key)* dan kunci pribadi *(private key)*. Kunci publik adalah kunci yang semua orang boleh mengetahui sedangkan kunci pribadi adalah kunci yang dirahasiakan, hanya boleh diketahui oleh satu orang. Algoritma yang memakai kunci publik diantaranya adalah *Digital Signature Algorithm* (DSA), RSA, Diffie-Hellman (DH), ElGamal, *Elliptic Curve Cryptography* (ECC), dan lain sebagainya (Ariyus, 2006:15). Secara sederhana proses pengiriman pesan dengan algoritma asimetris dapat digambarkan sebagai berikut:



Gambar 2.3 Skema Algoritma Asimetris

2.3 Kriptografi Kurva Eliptik

Kurva eliptik bukan elips. Dinamakan demikian karena kurva eliptik digambarkan oleh persamaan kubik, mirip dengan yang digunakan untuk menghitung lingkar elips. Secara umum, persamaan kubik untuk kurva eliptik diberikan dalam bentuk:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

dimana a, b, c, d, e adalah bilangan real dan x, y mengambil nilai-nilai dalam bilangan real. Secara sederhana, persamaan kurva eliptik cukup ditulis sebagai berikut:

$$y^2 = x^3 + ax + b$$

Persamaan tersebut merupakan persamaan kubik atau berderajat 3, karena pangkat tertinggi yang termuat adalah 3 (Stallings, 2003:298).

Untuk menggambar kurva , maka perlu dihitung:

$$y = \sqrt{x^3 + ax + b}$$

Untuk nilai a dan b yang diberikan, gambar akan bernilai positif dan negatif pada y untuk setiap nilai x. Sehingga setiap kurva eliptik akan berbentuk simetris terhadap sumbu x atau garis $y = 0$. Kurva eliptik juga dapat dipandang sebagai suatu himpunan yang terdiri dari titik-titik (x, y) yang memenuhi persamaan $y^2 = x^3 + ax + b$. Himpunan tersebut dinotasikan dengan $E(a, b)$. Untuk setiap nilai a dan b yang berbeda, dihasilkan himpunan $E(a, b)$ yang berbeda pula (Stallings, 2003:298).

Kriptografi kurva eliptik memanfaatkan kurva eliptik di mana variabel dan koefisien semua terbatas pada unsur-unsur medan berhingga. Ada dua macam

jenis kurva eliptik yang digunakan dalam aplikasi kriptografi, yaitu kurva prima yang didefinisikan melalui F_p dan kurva biner yang dibangun atas F_{2^m}.

2.3.1 Kurva Eliptik pada F_p

Misalkan $p > 3$ adalah bilangan prima ganjil, dan $a, b \in F_p$ memenuhi $4a^3 + 27b^2 \neq 0 (mod\ p)$ maka sebuah kurva eliptik pada F_p dinotasikan dengan $E(F_p)$ merupakan himpunan titik-titik $P(x, y)$ dan sebuah titik khusus $\varphi(\infty, \infty)$ merupakan titik tak hingga, dimana $x, y \in F_p$ yang memenuhi persamaan:

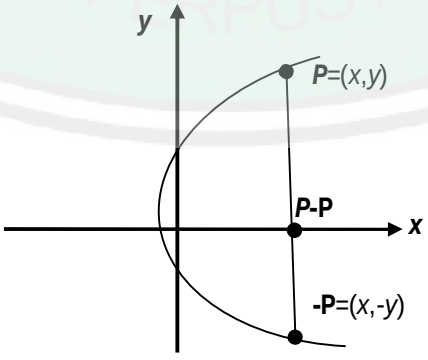
$$y^2 = x^3 + ax + b$$

(Ariyus, 2009:295)

Operasi penjumlahan pada $E(F_p)$ didefinisikan sebagai berikut:

a. $P + \varphi = \varphi + P = P$ untuk setiap $P \in E(F_p)$ dan φ merupakan titik tak hingga atau titik nol.

b. Jika $P = (x, y) \in E(F_p)$, maka $(x, y) + (x, -y) = \varphi$ (titik $(x, -y) \in E(F_p)$ dinotasikan sebagai $-P$, disebut negatif dari P). Secara geometris dapat digambarkan sebagai berikut:



Gambar 2.4 Negatif dari *P*

c. Misalkan $P = (x_1, y_1) \in E(F_p), Q = (x_2, y_2) \in E(F_p)$, dan $P \neq Q$, maka $P + Q = (x_3, y_3)$ dimana $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ dan $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

(Ariyus, 2009: 295)

Bukti:

Diketahui dua titik $P = (x_1, y_1) \in E(F_p), Q = (x_2, y_2) \in E(F_p)$, dan $P \neq Q$.

Misal $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-y_3 - y_1}{x_3 - x_1} = \frac{-y_3 - y_2}{x_3 - x_2}$

Persamaan kurva: $y^2 = x^3 + ax + b$

$$y_1^2 = x_1^3 + ax_1 + b \text{ .....(1)}$$

$$y_2^2 = x_2^3 + ax_2 + b \text{ .....(2)}$$

$$y_3^2 = x_3^3 + ax_3 + b \text{ .....(3)}$$

Persamaan (3) dikurangkan dengan persamaan (1) kemudian kedua ruas dibagi dengan $(x_3 - x_1)$, sehingga diperoleh:

$$y_3^2 - y_1^2 = (x_3^3 - x_1^3) + a(x_3 - x_1)$$

$$\frac{y_3^2 - y_1^2}{x_3 - x_1} = \frac{x_3^3 - x_1^3}{x_3 - x_1} + a\frac{x_3 - x_1}{x_3 - x_1}$$

$$\frac{(-y_3 - y_1)(-y_3 + y_1)}{x_3 - x_1} = \frac{(x_3^2 + x_1x_3 + x_1^2)(x_3 - x_1)}{x_3 - x_1} + a$$

$$(-y_3 + y_1)\lambda = (x_3^2 + x_1x_3 + x_1^2) + a \text{ .....(4)}$$

Persamaan (3) dikurangkan dengan persamaan (2) kemudian kedua ruas dibagi dengan $(x_3 - x_2)$, sehingga diperoleh:

$$y_3^2 - y_2^2 = (x_3^3 - x_2^3) + a(x_3 - x_2)$$

$$\frac{y_3^2 - y_2^2}{x_3 - x_2} = \frac{x_3^3 - x_2^3}{x_3 - x_2} + a\frac{x_3 - x_2}{x_3 - x_2}$$

$$\frac{(-y_3 - y_2)(-y_3 + y_2)}{x_3 - x_2} = \frac{(x_3^2 + x_2x_3 + x_2^2)(x_3 - x_2)}{x_3 - x_2} + a$$

$$(-y_3 + y_2)\lambda = (x_3^2 + x_2x_3 + x_2^2) + a \text{ .....(5)}$$

Jika persamaan (4) dan dikurangkan dengan persamaan (5) kemudian kedua ruas dibagi dengan $(x_1 - x_2)$, sehingga diperoleh:

$$[(-y_3 + y_1) - (-y_3 + y_2)]\lambda = [(x_3^2 + x_1x_3 + x_1^2) + a\,] - [(x_3^2 + x_2x_3 + x_2^2) + a]$$

$$(y_1 - y_2)\lambda = x_1^2 + x_1x_3 - x_2x_3 - x_2^2$$

$$(y_1 - y_2)\lambda = (x_1^2 - x_2^2) + x_3(x_1 - x_2)$$

$$\frac{(y_1 - y_2)\lambda}{(x_1 - x_2)} = \frac{(x_1^2 - x_2^2)}{(x_1 - x_2)} + \frac{x_3(x_1 - x_2)}{(x_1 - x_2)}$$

$$\lambda^2 = \frac{(x_1 - x_2)(x_1 + x_2)}{(x_1 - x_2)} + x_3$$

$$\lambda^2 = x_1 + x_2 + x_3$$

$$x_3 = \lambda^2 - x_1 - x_2 \text{ .....(6)}$$

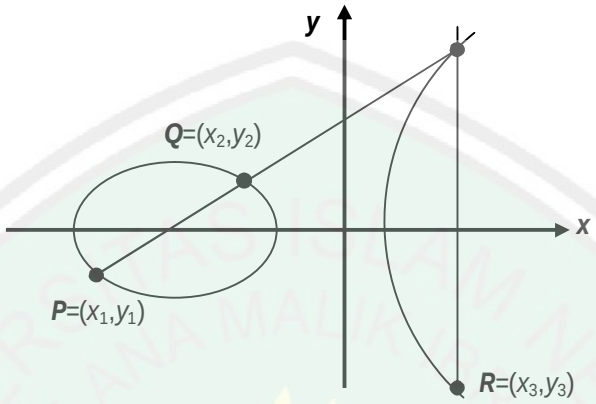
Dan dari pemisalan bahwa $\lambda = \frac{-y_3 - y_1}{x_3 - x_1}$, maka diperoleh:

$$\lambda(x_3 - x_1) = -y_3 - y_1$$

$$y_3 = \lambda(x_3 - x_1) - y_1 \text{ .....(7)}$$

Aturan penjumlahan sangat baik dijelaskan secara geometrik. Misalkan P = (x_1,y_1) dan Q = (x_2,y_2) menjadi sebuah titik yang nyata pada kurva eliptik E . Kemudian hasil jumlah dari P dan Q didenotasikan sebagai R = (x_3,y_3), yang didefinisikan sebagai berikut. Pertama gambarkan sebuah garis melalui P dan Q. Garis ini memotong kurva eliptik pada sebuah titik ketiga. Kemudian R

mencerminkan titik ini terhadap sumbu x. Kurva eliptik dalam gambar berikut terdiri dari dua bagian, bagian elips dan kurva tak hingga.



Gambar 2.5 Operasi Penjumlahan Titik Kurva Eliptik

d. Penggandaan titik *(doubling a point)*. Misalkan $P = (x_1, y_1) \in E(F_p)$, maka $P + P = 2P = (x_3, y_3)$ dimana $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$, dan $\lambda = \frac{3x_1^2 + a}{2y_1}$

Bukti:

Misal $\lambda = \frac{-y_3 - y_1}{x_3 - x_1}$ …….(8)

Dari (8) diperoleh:

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1}$$

$$\lambda(x_3 - x_1) = -y_3 - y_1$$

$$y_3 = \lambda(x_3 - x_1) - y_1 \text{ …….(9)}$$

Dari persamaan kurva $y^2 = x^3 + ax + b$ diturunkan terhadap x diperoleh:

$$2y\frac{dy}{dx} = 3x^2 + a \Leftrightarrow \frac{dy}{dx} = \frac{3x^2 + a}{2y} \Leftrightarrow \lambda = \frac{3x^2 + a}{2y} \text{ …….(10)}$$

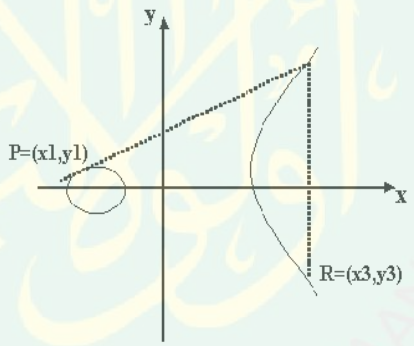
Dari persamaan (6) karena penjumlahan dilakukan pada titik yang sama maka $x_1 = x_2$ sehingga:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$x_3 = \lambda^2 - x_1 - x_1$$

$$x_3 = \lambda^2 - 2x_1 \ldots\ldots\ldots(11)$$

Secara geometris, aturan penggandaan titik akan dijabarkan sebagai berikut: Jika P = (x1,y1) , kemudian *double* dari P, didenotasikan R = (x3,y3) yang didefinisikan sebagai berikut. Pertama gambarkan sebuah garis tangen menuju kurva eliptik pada P. Garis ini memotong kurva eliptik pada sebuah titik kedua. Kemudian R mencerminkan titik ini terhadap sumbu x.



Gambar 2. 6 Operasi Penggandaan Titik Kurva Eliptik

2.3.2 Kurva Eliptik pada F_{2^m}

Sebuah kurva eliptik E pada F_{2^m} didefinisikan sebagai sebuah persamaan dalam bentuk:

$$y^2 + xy = x^3 + ax^2 + b$$

dimana $a, b \in F_{2^m}$, dan $b \neq 0$. Himpunan $E(F_{2^m})$ terdiri dari seluruh titik (x, y) dimana $x, y \in F_{2^m}$ yang memenuhi persamaan kurva elipik tersebut, bersamaan

dengan titik khusus $\varphi(\infty, \infty)$ disebut titik tak hingga *(point at infinity)* (Ariyus, 2009:296).

Sebagaimana kurva-kurva eliptik pada F_p, ada aturan-aturan untuk menjumlahkan titik-titik pada kurva kurva eliptik $E(F_{2^m})$ untuk mendapatkan sebuah titik ketiga kurva eliptik. Rumus aljabar untuk menjumlahkan dua titik dan menggandakan dua titik adalah:

a. $P + \varphi = \varphi + P = P$ untuk setiap $P \in E(F_{2^m})$. Jika $P(x, y) \in E(F_{2^m})$, maka $(x, y) + (x, x + y) = \varphi$ (titik $(x, x + y) \in E(F_p)$ dinotasikan sebagai $-P$, disebut negatif dari P).

b. Misalkan $P(x_1, y_1) \in E(F_{2^m}), Q(x_2, y_2) \in E(F_{2^m})$, dan $P \neq Q$, maka $P + Q = (x_3, y_3)$ dimana: $x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a$

$$y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1$$

c. Penggandaan titik *(doubling a point)*. Misalkan $P(x_1, y_1) \in E(F_p)$, maka $P + P = 2P = (x_3, y_3)$ dimana: $x_3 = {x_1}^2 + \frac{b}{{x_1}^2}$,

$$y_3 = {x_1}^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3$$

(Ariyus, 2009:296)

BAB III

PEMBAHASAN

Elliptik Curve Cryptography (ECC) atau kriptografi kurva eliptik dikembangkan secara terpisah oleh Victor Miller pada tahun 1986 dan oleh Neil Koblitz pada tahun 1987. Kriptografi kurva eliptik dapat digunakan untuk beberapa keperluan seperti protokol pertukaran kunci, tanda tangan digital, dan skema enkripsi Elgamal. Pada skripsi ini akan dibahas mengenai penggunaan kriptografi kurva eliptik pada proses penyandian Elgamal dan implementasinya dalam proses pengiriman pesan rahasia. Untuk mempersempit masalah, pada pembahasan penulis hanya menggunakan kurva eliptik pada medan berhingga prima (F_p).

3.1 Persamaan Kurva Eliptik pada Medan Berhingga Prima (F_p)

Misalkan $p > 3$ adalah bilangan prima ganjil, dan $a, b \in F_p$ memenuhi $4a^3 + 27b^2 \neq 0 (mod\ p)$ maka sebuah kurva eliptik pada medan berhingga prima (F_p) dinotasikan dengan $E(F_p)$ menurut Ariyus (2009) merupakan himpunan titik-titik $P(x, y)$ dan sebuah titik khusus $\varphi(\infty, \infty)$ yang merupakan titik tak hingga, dimana $x, y \in F_p$ yang memenuhi persamaan $y^2 = x^3 + ax + b$. Titik-titik pada $E(F_p)$ membentuk suatu grup eliptik modulo prima yang mana titik-titik tersebut nantinya akan digunakan untuk proses penyandian.

Teorema 3.1.1: Kurva eliptik $E(F_p)$ dengan operasi biner $+$ disimbolkan dengan $(E(F_p), +)$ merupakan grup

Bukti:

Untuk membuktikan $(E(F_p), +)$ adalah grup, maka harus memenuhi sifat-sifat berikut:

1. Operasi $+$ bersifat asosiatif

   Diketahui $P, Q, R \in E(F_p)$. Maka $(P + Q) + R = P + (Q + R) \in E(F_p)$

2. Operasi $+$ memiliki identitas

   Unsur identitas dari operasi $+$ pada $E(F_p)$ adalah titik nol atau titik tak hingga $\varphi(\infty, \infty) \in E(F_p)$. Sedemikian sehingga $P + \varphi = \varphi + P = P$

3. Operasi $+$ memiliki invers

   Unsur invers dari operasi $+$ pada $E(F_p)$ adalah $-P$ untuk setiap $P \in E(F_p)$. Sedemikian sehingga $P + (-P) = (-P) + P = \varphi$.

Karena ketiga sifat diatas udah terpenuhi, maka terbukti bahwa $(E(F_p), +)$ adalah grup.

Teorema 3.1.2: $(F_p, +, \times)$ adalah medan *(field)* dimana p adalah suatu bilangan prima

Bukti:

Diketahui $F_p = \{0, 1, 2, \dots, p-1\}$. Misalkan $a \times b = 0, \text{dan } a, b \in F_p$ artinya $0 \ (mod\ p)$ maka $p|ab$. Karena p bilangan prima dan $p|ab$ maka $p|a$ atau $p|b$. Jadi $a \equiv 0 \ (mod\ p)$ atau $b \equiv 0 \ (mod\ p)$ artinya $a = 0$ atau $b = 0$. Jadi terbukti

bahwa $(F_p, +, \times)$ tanpa pembagi nol yang artinya $(F_p, +, \times)$ adalah domain integral sehingga $(F_p, +, \times)$ adalah medan.

Berdasarkan teorema 3.1.2 di atas maka terbukti bahwa grup eliptik modulo prima $E(F_p)$ dengan operasi penjumlahan dan perkalian $(E(F_p), +, \times)$ akan membentuk suatu medan berhingga prima.

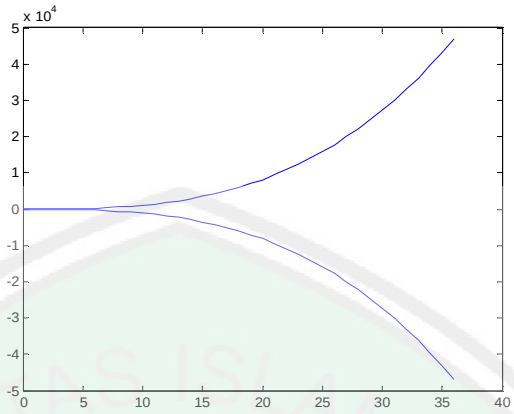
Inti dari proses penyandian adalah merubah pesan *(plaintext)* menjadi sandi *(ciphertext)* sehingga hal yang paling dibutuhkan adalah simbol baik itu berupa huruf maupun angka dan karakter lainnya. Agar lebih mudah dipahami, penulis akan menggunakan simbol yang berupa huruf dan angka, yang meliputi huruf 'A' sampai 'Z' dan angka '0' sampai '9'. Sehingga dibutuhkan minimal 36 titik $P(x, y)$ dimana $x, y \in F_p$. Dengan memilih sebarang bilangan prima p dan $a, b \in F_p$ secara acak dimana $p = 37, a = 8, b = 25$ maka :

$$4a^3 + 27b^2 = 4 \cdot 8^3 + 27 \cdot 25^2$$
$$\equiv 18923 \ (mod\ 37)$$
$$\equiv 16 (mod\ 37) \not\equiv 0 (mod\ 37)$$

Jadi persamaan kurva eliptik pada F_{37} yang akan digunakan yaitu:

$$y^2 = x^3 + 8x + 25$$

Secara geometris, kurva eliptik pada F_{37} diatas digambarkan sebagai berikut:



Gambar 3.1 Kurva eliptik $y^2 = x^3 + 8x + 25$

3.2 Elemen Grup Eliptik Modulo Prima $E(F_{37})$

Pada pembahasan sebelumnya ditetapkan bahwa nilai $p = 37, a = 8, b = 25$ sehingga persamaan kurva eliptik pada F_{37} adalah $y^2 = x^3 + 8x + 25$. Langkah-langkah untuk menentukan elemen pada $E(F_{37})$ adalah sebagai berikut:

1. Mencari residu kuadratis modulo 37 (QR_{37})

Tabel 3.1 Residu Kuadratis Modulo 37 (QR_{37})

$y \in F_{37}$	$y^2 (mod\ 37)$	QR_{37}	$y \in F_{37}$	$y^2 (mod\ 37)$	QR_{37}
0	$0^2 (mod\ 37)$	0	19	$19^2 (mod\ 37)$	28
1	$1^2 (mod\ 37)$	1	20	$20^2 (mod\ 37)$	30
2	$2^2 (mod\ 37)$	4	21	$21^2 (mod\ 37)$	34
3	$3^2 (mod\ 37)$	9	22	$22^2 (mod\ 37)$	3
4	$4^2 (mod\ 37)$	16	23	$23^2 (mod\ 37)$	11
5	$5^2 (mod\ 37)$	25	24	$24^2 (mod\ 37)$	21
6	$6^2 (mod\ 37)$	36	25	$25^2 (mod\ 37)$	33
7	$7^2 (mod\ 37)$	12	26	$26^2 (mod\ 37)$	10
8	$8^2 (mod\ 37)$	27	27	$27^2 (mod\ 37)$	26
9	$9^2 (mod\ 37)$	7	28	$28^2 (mod\ 37)$	7
10	$10^2 (mod\ 37)$	26	29	$29^2 (mod\ 37)$	27
11	$11^2 (mod\ 37)$	10	30	$30^2 (mod\ 37)$	12
12	$12^2 (mod\ 37)$	33	31	$31^2 (mod\ 37)$	36
13	$13^2 (mod\ 37)$	21	32	$32^2 (mod\ 37)$	25
14	$14^2 (mod\ 37)$	11	33	$33^2 (mod\ 37)$	16
15	$15^2 (mod\ 37)$	3	34	$34^2 (mod\ 37)$	9
16	$16^2 (mod\ 37)$	34	35	$35^2 (mod\ 37)$	4
17	$17^2 (mod\ 37)$	30	36	$36^2 (mod\ 37)$	1
18	$18^2 (mod\ 37)$	28			

Berdasarkan tabel 3.1 di atas, himpunan residu kuadratis modulo 37 adalah:

$$QR_{37} = \{0, 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36\}$$

2. Menentukan nilai dari $y^2 = x^3 + 8x + 25 \ (mod\ 37)$

Pada pembahasan ini nilai y^2 merupakan nilai dari persamaan kurva eliptik yang telah ditentukan sebelumnya. Dengan mensubtitusi setiap nilai $x \in F_{37}$ ke persamaan $y^2 = x^3 + 8x + 25 \ (mod\ 37)$ maka akan di dapatkan hasil sebagai berikut:

Tabel 3.2 Nilai $y^2 = x^3 + 8x + 25 \ (mod\ 37)$

$x \in F_{37}$	y^2	$x \in F_{37}$	y^2	$x \in F_{37}$	y^2
0	25	13	32	26	12
1	34	14	32	27	18
2	12	15	5	28	1
3	2	16	31	29	4
4	10	17	5	30	33
5	5	18	7	31	20
6	30	19	6	32	8
7	17	20	8	33	3
8	9	21	19	34	11
9	12	22	8	35	1
10	32	23	18	36	16
11	1	24	18	36	16
12	36	25	14		

3. Menentukan pasangan berurutan $(x, y) \in E_{37}(8, 25)$

Berdasarkan tabel 3.2, untuk $x = 0$ diperoleh nilai $y^2 = 0^3 + 0 + 25 \ (mod\ 37) = 25$. Setelah di cocokkan dengan nilai residu kuadratis modulo 37 pada tabel 3.1, ternyata $y^2 = 25$ juga terdapat pada QR_{37} yaitu untuk nilai $y = 5$ dan $y = 32$ maka didapatkan pasangan titik $(x, y) = (0, 5)$ dan $(x, y) = (0, 32)$ yang merupakan elemen dari grup eliptik $E_{37}(8,\ 25)$.

Tidak semua $x \in F_{37}$ akan menghasilkan nilai y^2 yang merupakan elemen QR_{37}. Contohnya, untuk $x = 3$ diperoleh nilai $y^2 = 3^3 + 3 + 25 \ (mod\ 37) = 2$,

sedangkan $y^2 = 2$ tidak termuat pada QR_{37}. Sehingga untuk $x = 3$ tidak terdapat nilai y yang sesuai.

Oleh karena itu perlu dilakukan pengecekan apakah setiap $x \in F_{37}$yang dapat menghasilkan nilai $y^2 \in QR_{37}$. Sehingga dengan cara yang sama, didapatkan hasil sebagai berikut:

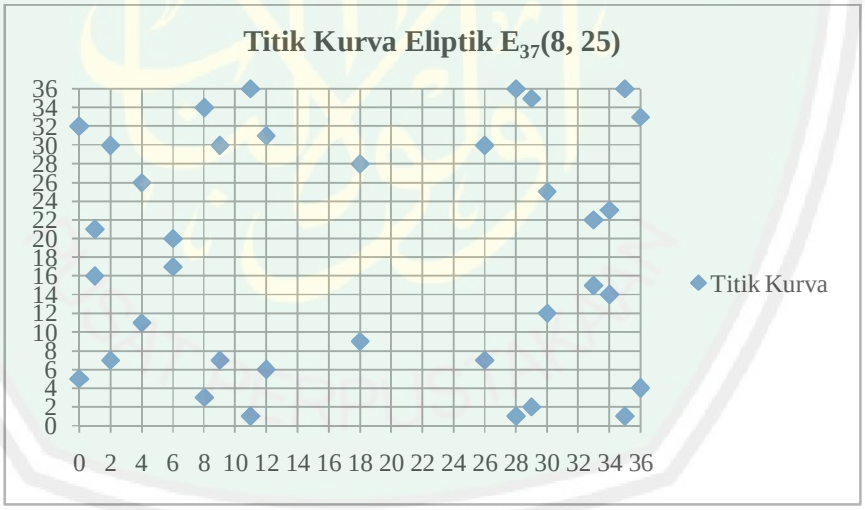
Tabel 3.3 Elemen $E_{37}(8, 25)$

$x \in F_{37}$	$y^2 = x^3 + 8x + 25 \ (mod\ 37)$	$y^2 \in QR_{37}$	$(x, y) \in E_{37}(8, 25)$
0	25	Ya	$(0, 5)$ dan $(0, 32)$
1	34	Ya	$(1, 16)$ dan $(1, 21)$
2	12	Ya	$(2, 7)$ dan $(2, 30)$
3	2	Bukan	-
4	10	Ya	$(4, 11)$ dan $(4, 26)$
5	5	Bukan	-
6	30	Ya	$(6, 17)$ dan $(6, 20)$
7	17	Bukan	-
8	9	Ya	$(8, 3)$ dan $(8, 34)$
9	12	Ya	$(9, 7)$ dan $(9, 30)$
10	32	Bukan	-
11	1	Ya	$(11, 1)$ dan $(11, 36)$
12	36	Ya	$(12, 6)$ dan $(12, 31)$
13	32	Bukan	-
14	32	Bukan	-
15	5	Bukan	-
16	31	Bukan	-
17	5	Bukan	-
18	7	Ya	$(18, 9)$ dan $(18, 28)$
19	6	Bukan	-
20	8	Bukan	-
21	19	Bukan	-
22	8	Bukan	-
23	18	Bukan	-
24	18	Bukan	-
25	14	Bukan	-
26	12	Ya	$(26, 7)$ dan $(26, 30)$

Tabel 3.3 Elemen $E_{37}(8,25)$ (Lanjutan)

27	18	Bukan	-
28	1	Ya	$(28,1)$ dan $(28,36)$
29	4	Ya	$(29,2)$ dan $(29,35)$
30	33	Ya	$(30,12)$ dan $(30,25)$
31	20	Bukan	-
32	8	Bukan	-
33	3	Ya	$(33,15)$ dan $(33,22)$
34	11	Ya	$(34,14)$ dan $(34,23)$
35	1	Ya	$(35,1)$ dan $(35,36)$
36	16	Ya	$(36,4)$ dan $(36,33)$

Berdasarkan tabel 3.3 di atas didapatkan 36 pasangan berurutan $(x,y) \in E_{37}(8,25)$ yang merupakan elemen dari grup eliptik modulo prima $E(F_{37})$ dan satu titik khusus yaitu (∞,∞) yang merupakan titik tak hingga. Secara geometri, titik-titik tersebut dapat digambarkan sebagai berikut:



Gambar 3.2 Titik Kurva Eliptik $E_{37}(8, 25)$

3.3 Generator Grup Eliptik $E(F_{37})$

Misalkan $P \in E(F_{37})$, maka P disebut generator atau pembangkit dari $E(F_{37})$ jika setiap elemen $E(F_{37})$ dapat dituliskan sebagai perpangkatan dari P

atau $E(F_{37}) = \{P^n | n \in F_{37}\}$ dimana F_{37} merupakan medan berhingga prima dengan elemen $\{0, 1, 2, \dots, 36\}$. Pada pembahasan sebelumnya, telah didapatkan 36 titik $P(x, y)$ sehingga pembangkit dari grup eliptik $E(F_{37})$ dapat dicari dengan melakukan penjumlahan dan penggandaan titik kurva eliptik dengan rumus sebagai berikut:

a. Penjumlahan Titik Kurva Eliptik

   Misalkan $P = (x_1, y_1) \in E(F_p), Q = (x_2, y_2) \in E(F_p)$, dan $P \neq Q$, maka $P + Q = (x_3, y_3)$ dimana $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ dan $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

b. Penggandaan titik *(doubling a point)*. Misalkan $P = (x_1, y_1) \in E(F_p)$, maka $P + P = 2P = (x_3, y_3)$ dimana $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$, dan $\lambda = \frac{3x_1^2 + a}{2y_1}$

Dari 36 titik kurva yang ada ternyata semua titik tersebut merupakan generator dari grup eliptik $E(F_{37})$. Hasil perhitungan generator dari grup eliptik $E(F_{37})$ akan disajikan dalam lampiran 1.

3.4 Parameter Domain Kurva Eliptik

Sebelum mengimplementasikan kriptografi kurva eliptik, terlebih dahulu perlu dipersiapkan infrastruktur yang dibutuhkan oleh sistem kriptografi tersebut. Infrastruktur yang dimaksud adalah parameter-parameter domain kurva eliptik. Sehingga seluruh pengguna sistem dapat mengetahui beberapa parameter yang

akan digunakan bersama. Parameter ini bersifat umum dan boleh diketahui oleh setiap pengguna dalam sistem tersebut.

Parameter-parameter domain kurva eliptik atas F_p didefinisikan sebagai *six-tupel* $D = (p, a, b, P, n, h)$. Parameter tersebut adalah:

Tabel 3.4 Parameter Domain Kurva Eliptik

Parameter	Keterangan
p	Bilangan prima
a, b	Koefisien persamaan kurva eliptik dimana $a, b \in F_p$
P	Titik dasar, yaitu elemen pembangkit (generator) grup $E_p(a, b)$
n	Order dari P, yaitu bilangan bulat positif terkecil sedemikian sehingga $nP = \varphi$, dimana φ merupakan titik nol atau titik tak hingga.
h	Kofaktor $h = \#E(F_p)/n$, $\#E$adalah jumlah titik dalam grup eliptik $E(F_p)$

Kekuatan kriptografi kurva eliptik tergantung dari pemilihan parameter-parameter domain yang digunakan. Pemilihan parameter ini dilakukan sedemikian sehingga dapat terhindar dari serangan-serangan terhadap kekuatan algoritma kriptografi kurva eliptik. Parameter-parameter tersebut ditentukan secara acak menggunakan program yang dibuat sendiri oleh penulis.

3.5 Algoritma ElGamal *Elliptic Curve Cryptography* (ECC)

Ada tiga algoritma ElGamal *Elliptic Curve Cryptography* (ECC), yaitu:

1. Algoritma pembentukan kunci

   Input: Parameter-parameter domain kurva eliptik (p, E, P, n).

   Output: Kunci publik Q dan kunci privat d.

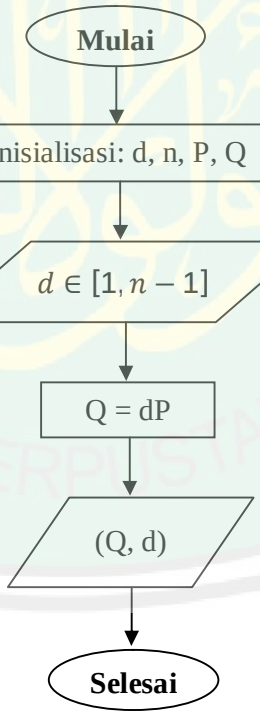
a. Pilih $d \in [1, n-1]$.

b. Hitung $Q = dP$.

c. Hasil (Q, d).

Parameter-parameter domain umum kurva eliptik (p, E, P, n) menjelaskan bahwa misalkan E merupakan suatu kurva eliptik yang didefinisikan atas medan berhingga F_p. Misalkan P adalah sebuah titik pada $E(F_p)$, dan misalkan P mempunyai order prima n, maka subgrup siklik K dari $E(F_p)$ yang dibangkitkan oleh P adalah $\langle P \rangle = \{\varphi, P, 2P, 3P, \dots, (n-1)P\}$.

Untuk mempermudah pemahaman dan proses pembuatan program, berikut disajikan diagram alir dari algoritma pembentukan kunci Elgamal ECC:



Gambar 3.3 Diagram Alir Algoritma Pembentukan Kunci Elgamal ECC

2. Algoritma enkripsi

Input: Parameter domain (p, E, P, n), kunci publik Q, pesan m.

Output: Ciperteks (C_1, C_2).

a. Representasikan pesan sebagai sebuah titik M pada $E(F_p)$.

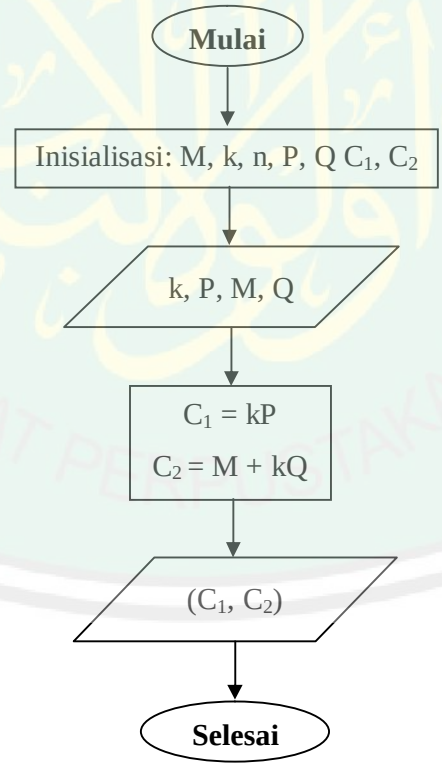
b. Pilih $k \in [1, n-1]$.

c. Hitung $C_1 = kP$.

d. Hitung $C_2 = M + kQ$.

e. Hasil (C_1, C_2).

Untuk mempermudah pemahaman dan proses pembuatan program, berikut disajikan diagram alir dari algoritma enkripsi dari Elgamal ECC:



Gambar 3.4 Diagram Alir Algoritma Enkripsi Elgamal ECC

3. Algoritma dekripsi

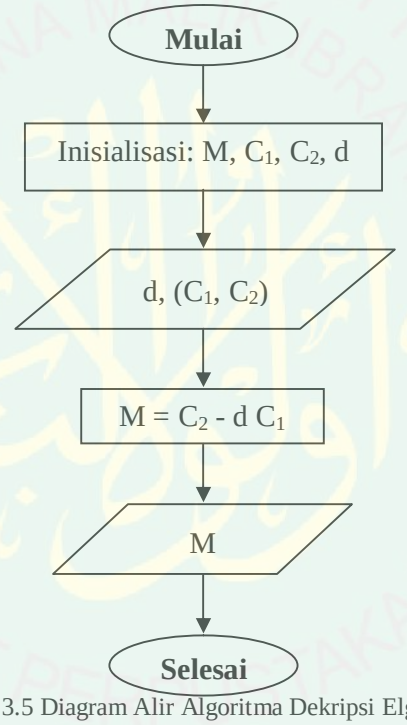
Input: Parameter domain (p, E, P, n), kunci privat d, ciperteks (C_1, C_2).

Output: Pesan m.

a. Hitung $M = C_2 - dC_1$

b. Hasil (M).

Untuk mempermudah pemahaman dan proses pembuatan program, berikut disajikan diagram alir dari algoritma dekripsi dari Elgamal ECC:



Gambar 3.5 Diagram Alir Algoritma Dekripsi Elgamal ECC

3.6 Implementasi Elgamal ECC

Setelah mengetahui segala sesuatu yang dibutuhkan dalam penyandian menggunakan kriptografi kurva eliptik yang diaplikasikan pada skema enkripsi Elgamal, berikut akan dibahas mengenai implementasi Elgamal ECC dengan menggunakan contoh agar lebih mudah dipahami. Misalkan, Ali ingin membagi

sebuah informasi rahasia tentang *password* komputer perusahaan yang berbunyi "MATEMATIKA" kepada Budi. Pesan ini merupakan pesan rahasia yang tidak boleh diketahui oleh sembarang orang. Jika pesan tersebut bocor maka keamanan perusahaan bisa terganggu. Oleh karena itu yang perlu Ali dan Budi lakukan adalah:

1. Representasi Titik

Diketahui persamaan kurva eliptik atas medan berhingga F_p yaitu $y^2 = x^3 + 8x + 25 \ (mod\ 37)$. Dari persamaan tersebut didapat pasangan titik-titik kurva eliptik sebanyak 36 titik dan satu titik tak hingga yang dapat dilihat pada tabel 3.3.

Untuk merepresentasikan titik menjadi simbol alfabet, angka, atau simbol lainnya maka perlu dipilih satu titik P yang merupakan elemen pembangkit dari grup eliptik $E_{37}(8,25)$. Representasi titik ini tergantung pada elemen pembangkit yang dipilih. Sehingga, permisalan ini tidak bisa berlaku umum.

Misalkan jika dipilih $P = (6, 17)$ yang merepresentasikan huruf A, dan 2P merepresentasikan huruf B, maka akan dihasilkan tabel representasi dari 37 titik kurva yang ada sebagai berikut:

Tabel 3.5 Representasi Titik Kurva dan Simbol

Titik Kurva	Simbol	Titik Kurva	Simbol
0P=(∞, ∞).	(Spasi)	5P=(33, 22)	E
$P = (6, 17)$	A	6P=(26, 30)	F
2P=(36, 33)	B	7P=(2, 30)	G
3P=(4, 26)	C	8P=(28, 36)	H
4P=(1, 16)	D	9P=(0, 5)	I

Tabel 3.5 Representasi Titik Kurva dan Simbol (Lanjutan)

Titik Kurva	Simbol	Titik Kurva	Simbol
10P=(35, 36)	J	24P=(9, 30)	X
11P=(8, 34)	K	25P=(12, 31)	Y
12P=(12, 6)	L	26P=(8, 3)	Z
13P=(9, 7)	M	27P=(35, 1)	0
14=(29, 35)	N	28P=(0, 32)	1
15P=(18, 9)	O	29P=(28, 1)	2
16=(34, 14)	P	30P=(2, 7)	3
17P=(30, 12)	Q	31P=(26, 7)	4
18P=(11, 1)	R	32P=(33, 15)	5
19P=(11, 36)	S	33P=(1, 21)	6
20P=(30, 25)	T	34P=(4, 11)	7
21P=(34, 23)	U	35P=(36, 4)	8
22P=(18, 28)	V	36P=(6, 20)	9
23P=(29, 2)	W		

Jika diketahui $P = (6, 17)$, maka untuk menentukan 2P hingga 36P dapat dihitung menggunakan rumus penggandaan titik kurva eliptik seperti yang sudah dijelaskan pada sub bab 3.3. Berikut ini akan ditunjukkan proses perhitungan untuk nilai 2P dan 3P:

a. Misalkan $P(x_1 = 6, y_1 = 17) \in E(F_{37})$, maka $P + P = 2P = (x_3, y_3)$ dimana:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$= \left(\frac{3 \cdot 6^2 + 8}{2 \cdot 17}\right)^2 - 2 \cdot 6 = \left(\frac{116}{34}\right)^2 - 12 = (5 \cdot 34^{-1})^2 - 12$$

$$= (5 \cdot 12)^2 - 12 = 23^2 - 12 = 11 - 12 = -1(mod\ 37) = 36$$

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

$$= \left(\frac{116}{34}\right)(6 - 36) - 17 = 23 \cdot (-30) - 17$$

$$= 23 \cdot 7 - 17 = 13 - 17 = -4(mod\ 37) = 33$$

Jadi $2P = (36, 33)$.

b. Misalkan $P(x_1 = 6, y_1 = 17) \in E(F_p), Q(x_2 = 36, y_2 = 33) \in E(F_p)$, dan $P \neq Q$, maka $P + Q = (x_3, y_3)$ dimana:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$= \left(\frac{33 - 17}{36 - 6}\right)^2 - 6 - 36 = \left(\frac{16}{30}\right)^2 - 6 - 36$$

$$= (16 \cdot 30^{-1})^2 - 6 - 36 = (16 \cdot 21)^2 - 6 - 36$$

$$= (16 \cdot 21)^2 - 6 - 36 = 3^2 - 6 - 36 = -33(mod\ 37) = 4$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

$$= 3 \cdot (6 - 4) - 17 = 3 \cdot 2 - 17$$

$$= 6 - 17 = -11(mod\ 37) = 26$$

Jadi $3P = (4, 26)$.

2. Menentukan Kunci publik dan Kunci Privat

Kunci publik merupakan kunci yang boleh diketahui oleh banyak orang sedangkan kunci privat hanya boleh diketahui oleh satu orang saja. Kunci publik

dapat ditentukan dengan menghitung nilai $Q = dP$, dimana d adalah kunci privat milik Budi dan P merupakan generator dari grup eliptik.

Untuk melakukan proses enkripsi, Budi sebagai penerima pesan harus mengirimkan kunci publik kepada Ali. Misalkan Budi memilih satu bilangan acak $d \in [1, n-1]$, yaitu $d = 7$, maka kunci publik $Q = 7P = 7 \cdot (6,17) = (2,30)$. Dari kunci publik ini maka setiap orang dapat melakukan proses enkripsi, tapi hanya orang yang tahu kunci privat d saja yang dapat mendekripsikan pesan tersebut.

3. Proses Enkripsi

Enkripsi adalah suatu proses penyandian pesan menjadi suatu kode yang tidak dimengerti. Dalam kasus ini, Ali ingin menyampaikan pesan berupa kata "MATEMATIKA" kepada Budi. Diketahui kunci publik yaitu $Q = (2,30)$, maka untuk melakukan proses dekripsi perlu dilakukan hal-hal sebagai berikut:

a. Memilih satu bilangan acak $k \in [1, n-1]$, misal $k = 4$.
b. Menghitung nilai (C_1, C_2) yang merupakan ciperteks atau kode dari pesan yang akan disampaikan, dimana $C_1 = kP$. Karena diketahui $k = 4$ dan $P = (6,17)$ maka $C_1 = kP = 4 \cdot (6,17) = (1,16)$ dimana titik $(1,16)$ merupakan representasi dari huruf 'D'.
c. Menghitung nilai C_2 dengan rumus $C_2 = M + kQ$, dan berikut adalah perhitungan dari nilai C_2:

Tabel 3.6 Proses Enkripsi

Plainteks (M)	**Titik Kurva**	C_2	(C_1, C_2)
M	$(9, 7)$	$C_2 = M + kQ$ $= (9,7) + 4 \cdot (2,30)$ $= (9,7) + (0,32)$ $= (1,16) = D$	DD
A	$(6, 17)$	$C_2 = M + kQ$ $= (6,17) + 4 \cdot (2,30)$ $= (6,17) + (0,32)$ $= (28,1) = 2$	D2
T	$(30, 25)$	$C_2 = M + kQ$ $= (30,25) + 4 \cdot (2,30)$ $= (30,25) + (0,32)$ $= (8,34) = K$	DK
E	$(33, 22)$	$C_2 = M + kQ$ $= (33,22) + 4 \cdot (2,30)$ $= (33,22) + (0,32)$ $= (1,21) = 6$	D6
M	$(9, 7)$	$C_2 = M + kQ$ $= (9,7) + 4 \cdot (2,30)$ $= (9,7) + (0,32)$ $= (1,16) = D$	DD
A	$(6, 17)$	$C_2 = M + kQ$ $= (6,17) + 4 \cdot (2,30)$ $= (6,17) + (0,32)$ $= (28,1) = 2$	D2
T	$(30, 25)$	$C_2 = M + kQ$ $= (30,25) + 4 \cdot (2,30)$ $= (30,25) + (0,32)$ $= (8,34) = K$	DK
I	$(0, 5)$	$C_2 = M + kQ$ $= (0,5) + 4 \cdot (2,30)$ $= (0,5) + (0,32)$ $= (0,32) = 1$	D1
K	$(8, 34)$	$C_2 = M + kQ$ $= (8,34) + 4 \cdot (2,30)$ $= (8,34) + (0,32)$ $= (36,33) = B$	DB
A	$(6, 17)$	$C_2 = M + kQ$ $= (6,17) + 4 \cdot (2,30)$ $= (6,17) + (0,32)$ $= (28,1) = 2$	D2

Maka dari tabel 3.5 pesan “MATEMATIKA” diubah menjadi kode yang tidak dapat dimengerti, yaitu “DDD2DKD6DDD2DKD1DBD2”.

4. Proses Dekripsi

Dekripsi merupakan suatu proses untuk merubah ciperteks atau kode menjadi plainteks atau pesan yang dapat dimengerti. Untuk membaca pesan yang dikirimkan oleh Ali, maka Budi harus menggunakan kunci privatnya untuk melakukan proses dekripsi. Proses dekripsi dapat dilakukan dengan menghitung nilai $M = C_2 - dC_1$. Diketahui sebelumnya bahwa nilai $d = 7$ dan $C_1 = (1, 16)$, maka hasil dari $dC_1 = 7 \cdot (1, 16) = (0, 32)$.

Misalkan $P = (x, y) \in E(F_p)$ maka negatif dari P adalah $-P = (x, y)$. Sehingga nilai dari $-dC_1 = (0, 32)$, maka hasil dari $M = C_2 - dC_1$ adalah sebagai berikut:

Tabel 3.7 Proses Dekripsi

Ciperteks	(C_1, C_2)	Titik Kurva	Plainteks (M)
DD	$[(1, 16), (1, 16)]$	$M = C_2 - dC_1$ $= (1, 16) + (0, -32)$ $= (9, 7) = \text{M}$	M
D2	$[(1, 16), (28, 1)]$	$M = C_2 - dC_1$ $= (28, 1) + (0, -32)$ $= (6, 17) = \text{A}$	A
DK	$[(1, 16), (8, 34)]$	$M = C_2 - dC_1$ $= (8, 34) + (0, -32)$ $= (30, 25) = \text{T}$	T
D6	$[(1, 16), (6, 20)]$	$M = C_2 - dC_1$ $= (6, 20) + (0, -32)$ $= (33, 22) = \text{E}$	E
DD	$[(1, 16), (1, 16)]$	$M = C_2 - dC_1$ $= (1, 16) + (0, -32)$ $= (9, 7) = \text{M}$	M

Tabel 3.7 Proses Dekripsi (Lanjutan)

Ciperteks	(C_1, C_2)	Titik Kurva	Plainteks (M)
D2	$[(1,16),(28,1)$	$M = C_2 - dC_1$ $= (28,1) + (0,-32)$ $= (6,17) = A$	A
DK	$[(1,16),(8,34)]$	$M = C_2 - dC_1$ $= (8,34) + (0,-32)$ $= (30,25) = T$	T
D1	$[(1,16),(0,32)]$	$M = C_2 - dC_1$ $= (0,32) + (0,-32)$ $= (0,5) = I$	I
DB	$[(1,16),(36,33)]$	$M = C_2 - dC_1$ $= (36,33) + (0,-32)$ $= (8,34) = K$	K
D2	$[(6,17),(28,1)]$	$M = C_2 - dC_1$ $= (28,1) + (0,-32)$ $= (6,17) = A$	A

Berdasarkan tabel 3.6 kode atau ciperteks telah diubah menjadi pesan yang memiliki arti, yaitu menjadi kata “MATEMATIKA”.

BAB IV

PENUTUP

4.1 Kesimpulan

Elgamal ECC *(Elliptic Curve Cryptography)* menggunakan konsep kurva eliptik untuk merepresentasikan simbol atau kode yang nantinya digunakan untuk melakukan proses enkripsi. Kesimpulan yang dapat diambil penulis setelah menyelesaikan pembuatan skripsi ini adalah:

1. Proses enkripsi dengan menggunakan kriptografi kurva eliptik pada proses penyandian Elgamal akan menghasilkan *cipper* atau kode yang tidak dapat dimengerti. Dalam hal ini diberikan sebuah contoh kasus yaitu kata "MATEMATIKA" yang berubah menjadi "DDD2DKD6DDD2DKD1DBD2". Hasil ini bergantung pada nilai kunci privat k, kunci publik Q, serta elemen pembangkit P yang dipilih. Dengan nilai parameter yang berbeda akan dihasilkan kode yang berbeda pula, meskipun menggunakan kata yang sama.
2. Proses dekripsi merupakan kebalikan dari proses enkripsi. Kode atau *cipper* yang dihasilkan dari proses enkripsi akan diubah kembali ke bentuk asalnya. Kode "DDD2DKD6DDD2DKD1DBD2" akan kembali menjadi kata "MATEMATIKA". Hasil ini bergantung pada nilai kunci privat d yang telah dipilih. Jika menggunakan nilai parameter yang berbeda pada proses dekripsi maka kode tersebut tidak bisa kembali ke bentuk asal dan akan tetap menjadi kode rahasia yang tidak bisa dibaca dan dimengerti artinya.

4.2 Saran

Dalam skripsi ini hanya dibahas mengenai aplikasi kriptografi kurva eliptik pada proses penyandian Elgamal saja dan hanya terbatas pada medan berhingga F_p. Sehingga untuk skripsi selanjutnya dapat membahas mengenai penggunaan kriptografi kurva eliptik untuk tanda tangan digital, maupun pertukaran kunci, atau dapat pula membahas mengenai kriptografi kurva eliptik pada medan berhingga F_{2^m}.

DAFTAR PUSTAKA

Al-Qur'an dan Terjemahannya. 1998. Departemen Agama.

Abdussakir. 2009. *Matematika 1 Kajian Integratif Matematika dan Al-Qur'an.* Malang: UIN Malang Press.

Amounas, F dan El Kinani, E. H. 2011. An Application of Discrete Algorithms in Asymmetric Cryptography. *International Mathematical Forum*, 6: 2409-2418.

Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

Ariyus, D. 2009. *Keamanan Multimedia.* Yogyakarta: CV Andi Offset.

Hamidah, Siti Nur. 2009. Konsep Matematis dan Proses Penyandian Kriptografi ElGamal. *Skripsi* Tidak diterbitkan. Malang: UIN Malang.

Hankerson, Darrel. dkk. 2003. *Guide to Elliptic Curve Cryptography*. New York: Springer.

Menezes, A., P. van Oorschot & S. Vanstone. 1997. *Handbook of Applied Cryptography*. New York: CRC Press.

Muhsetyo, G. 1997. *Dasar-Dasar Teori Bilangan*. Jakarta: PGSM.

Munir, R. 2010. *Matematika Diskrit.* Bandung: Informatika Bandung.

Raisinghania, M. D. dan Aggarwal, R.S. 1980. *Modern Algebra*. New Delhi: S. Chand & Company Ltd.

Schneier, B. 1996. *Applied Cryptography Protocols, Algorithm and Source code in C, Second Edition*. Amerika: John Willey & Sons, inc.

Stalling, W. 1999. *Cryptography and Network Security, Principal and Practice, Second Edition*. New Jersey: Prentice Hall.

LAMPIRAN

Lampiran 1: Tabel Generator Grup Eliptik $E(F_{37})$

P	(0, 5)	(0, 32)	(1, 16)	(1, 21)	(2, 7)	(2, 30)	(4, 11)
2P	(11, 1)	(11, 36)	(28, 36)	(28, 1)	(29, 2)	(29, 35)	(26, 7)
3P	(35, 1)	(35, 36)	(12, 6)	(12, 31)	(34, 14)	(34, 23)	(0, 32)
4P	(6, 20)	(6, 17)	(34, 14)	(34, 23)	(0, 5)	(0, 32)	(12, 31)
5P	(28, 36)	(28, 1)	(30, 25)	(30, 12)	(36, 33)	(36,4)	(18, 28)
6P	(30, 12)	(30, 25)	(9, 30)	(9, 7)	(33, 15)	(33, 12)	(11, 36)
7P	(8, 3)	(8, 34)	(0, 32)	(0, 5)	(12, 31)	(12, 6)	(34, 14)
8P	(36, 4)	(36, 33)	(33, 15)	(33, 22)	(11, 1)	(11, 36)	(9, 7)
9P	(2, 30)	(2, 7)	(6, 20)	(6, 17)	(8, 34)	(8, 3)	(35, 36)
10P	(34, 14)	(34, 23)	(4, 26)	(4, 11)	(1, 16)	(1, 21)	(2, 30)
11P	(12, 31)	(12, 6)	(2, 30)	(2, 7)	(4, 11)	(4, 26)	(1, 16)
12P	(4, 11)	(4, 26)	(8, 34)	(8, 3)	(35, 1)	(35, 36)	(6, 17)
13P	(26, 30)	(26, 7)	(18, 9)	(18, 28)	(30, 25)	(30, 12)	(36, 4)
14P	(18, 9)	(18, 28)	(11, 36)	(11, 1)	(9, 7)	(9, 30)	(33, 15)
15P	(9, 30)	(9, 7)	(29, 2)	(29, 35)	(26, 30)	(26, 7)	(28, 1)
16P	(1, 21)	(1, 16)	(35, 1)	(35, 36)	(6, 20)	(6 , 17)	(8, 3)
17P	(33, 22)	(33, 15)	(26, 7)	(26, 30)	(28, 1)	(28, 36)	(29, 2)
18P	(29, 35)	(29, 2)	(36, 4)	(36, 33)	(18, 28)	(18, 9)	(30, 25)
19P	(29, 2)	(29, 35)	(36, 33)	(36, 4)	(18, 9)	(18, 28)	(30, 12)
20P	(33, 15)	(33, 22)	(26, 30)	(26, 7)	(28, 36)	(28, 1)	(29, 35)
21P	(1, 16)	(1, 21)	(35, 36)	(35, 1)	(6, 17)	(6, 20)	(8, 34)
22P	(9, 7)	(9, 30)	(29, 35)	(29, 2)	(26, 7)	(26, 30)	(28, 36)
23P	(18, 28)	(18, 9)	(11, 1)	(11, 36)	(9, 30)	(9, 7)	(33, 22)
24P	(26, 7)	(26, 30)	(18, 28)	(18, 9)	(30, 12)	(30, 25)	(36, 33)
25P	(4, 26)	(4, 11)	(8, 3)	(8, 34)	(35, 36)	(35, 1)	(6, 20)
26P	(12, 6)	(12, 31)	(2, 7)	(2, 30)	(4, 26)	(4, 11)	(1, 21)
27P	(34, 23)	(34, 14)	(4, 11)	(4, 26)	(1, 21)	(1, 16)	(2, 7)
28P	(2, 7)	(2, 30)	(6, 17)	(6, 20)	(8, 3)	(8, 34)	(35, 1)
29P	(36, 33)	(36, 4)	(33, 22)	(33, 15)	(11, 36)	(11, 1)	(9, 30)
30P	(8, 34)	(8, 3)	(0, 5)	(0, 32)	(12, 6)	(12, 31)	(34, 23)
31P	(30, 25)	(30, 12)	(9, 7)	(9, 30)	(33, 22)	(33, 15)	(11, 1)
32P	(28, 1)	(28, 36)	(30, 12)	(30, 25)	(36, 4)	(36, 33)	(18, 9)
33P	(6, 17)	(6, 20)	(34, 23)	(34, 14)	(0, 32)	(0, 5)	(12, 6)
34P	(35, 36)	(35, 1)	(12, 31)	(12, 6)	(34, 23)	(34, 14)	(0, 5)
35P	(11, 36)	(11, 1)	(28, 1)	(28, 36)	(29, 35)	(29, 2)	(26, 30)
36P	(0, 32)	(0, 5)	(1, 21)	(1, 16)	(2, 30)	(2, 7)	(4, 26)

Lampiran 1: Tabel Generator Grup Eliptik $E(F_p)$ (Lanjutan)

P	(4, 26)	(6, 17)	(6, 20)	(8, 3)	(8, 34)	(9, 7)	(9, 30)
2P	(26, 30)	(36, 33)	(36, 4)	(18, 9)	(18, 28)	(8, 3)	(8, 34)
3P	(0, 5)	(4, 26)	(4, 11)	(1, 16)	(1, 21)	(36, 33)	(36, 4)
4P	(12, 6)	(1, 16)	(1, 21)	(2, 7)	(2, 30)	(18, 9)	(18, 28)
5P	(18, 9)	(33, 22)	(33, 15)	(11, 36)	(11, 1)	(0, 32)	(0, 5)
6P	(11, 1)	(26, 30)	(26, 7)	(28, 36)	(28, 1)	(1, 16)	(1, 21)
7P	(34, 23)	(2, 30)	(2, 7)	(4, 11)	(4, 26)	(30, 12)	(30, 25)
8P	(9, 30)	(28, 36)	(28, 1)	(29, 2)	(29, 35)	(2, 7)	(2, 30)
9P	(35, 1)	(0, 5)	(0, 32)	(12, 6)	(12, 31)	(26, 30)	(26, 7)
10P	(2, 7)	(35, 36)	(35, 1)	(6, 17)	(6, 20)	(11, 36)	(11, 1)
11P	(1, 21)	(8, 34)	(8, 3)	(35, 1)	(35, 36)	(33, 15)	(33, 22)
12P	(6, 20)	(12, 6)	(12, 31)	(34, 14)	(34, 23)	(28, 36)	(28, 1)
13P	(36, 33)	(9, 7)	(9, 30)	(33, 22)	(33, 15)	(34, 23)	(34, 14)
14P	(33, 22)	(29, 35)	(29, 2)	(26, 7)	(26, 30)	(4, 11)	(4, 26)
15P	(28, 36)	(18, 9)	(18, 28)	(30, 25)	(30, 12)	(35, 36)	(35, 1)
16P	(8, 34)	(34, 14)	(34, 23)	(0, 5)	(0, 32)	(29, 2)	(29, 35)
17P	(29, 35)	(30, 12)	(30, 25)	(36, 4)	(36, 33)	(6, 20)	(6 , 17)
18P	(30, 12)	(11, 1)	(11, 36)	(9, 30)	(9, 7)	(12, 6)	(12, 31)
19P	(30, 25)	(11, 36)	(11, 1)	(9, 7)	(9, 30)	(12, 31)	(12, 6)
20P	(29, 2)	(30, 25)	(30, 12)	(36, 33)	(36, 4)	(6, 17)	(6, 20)
21P	(8, 3)	(34, 23)	(34, 14)	(0, 32)	(0, 5)	(29, 35)	(29, 2)
22P	(28, 1)	(18, 28)	(18, 9)	(30, 12)	(30, 25)	(35, 1)	(35, 36)
23P	(33, 15)	(29, 2)	(29, 35)	(26, 30)	(26, 7)	(4, 26)	(4, 11)
24P	(36, 4)	(9, 30)	(9, 7)	(33, 15)	(33, 22)	(34, 14)	(34, 23)
25P	(6, 17)	(12, 31)	(12, 6)	(34, 23)	(34, 14)	(28, 1)	(28, 36)
26P	(1, 16)	(8, 3)	(8, 34)	(35, 36)	(35, 1)	(33, 22)	(33, 15)
27P	(2, 30)	(35, 1)	(35, 36)	(6, 20)	(6, 17)	(11, 1)	(11, 36)
28P	(35, 36)	(0, 32)	(0, 5)	(12, 31)	(12, 6)	(26, 7)	(26, 30)
29P	(9, 7)	(28, 1)	(28, 36)	(29, 35)	(29, 2)	(2, 30)	(2, 7)
30P	(34, 14)	(2, 7)	(2, 30)	(4, 26)	(4, 11)	(30, 25)	(30, 12)
31P	(11, 36)	(26, 7)	(26, 30)	(28, 1)	(28, 36)	(1, 21)	(1, 16)
32P	(18, 28)	(33, 15)	(33, 22)	(11, 1)	(11, 36)	(0, 5)	(0, 32)
33P	(12, 31)	(1, 21)	(1, 16)	(2, 30)	(2, 7)	(18, 28)	(18, 9)
34P	(0, 32)	(4, 11)	(4, 26)	(1, 21)	(1, 16)	(36, 4)	(36, 33)
35P	(26, 7)	(36, 4)	(36, 33)	(18, 28)	(18, 9)	(8, 34)	(8, 3)
36P	(4, 11)	(6, 20)	(6, 17)	(8, 34)	(8, 3)	(9, 30)	(9, 7)

Keterangan: Warna Merah merupakan generator yang dipilih penulis secara acak dan digunakan dalam implementasi Elgamal ECC.

Lampiran 1: Tabel Generator Grup Eliptik $E(F_p)$ (Lanjutan)

P	(11, 1)	(11, 36)	(12, 6)	(12, 31)	(18, 9)	(18, 28)	(26, 7)
2P	(6, 20)	(6, 17)	(9, 30)	(9, 7)	(2, 7)	(2, 30)	(12, 31)
3P	(30, 12)	(30, 25)	(6, 20)	(6, 17)	(28, 36)	(28, 1)	(11, 36)
4P	(36, 4)	(36, 33)	(8, 34)	(8, 3)	(29, 2)	(29, 35)	(9, 7)
5P	(34, 14)	(34, 23)	(29, 2)	(29, 35)	(6, 17)	(6, 20)	(2, 30)
6P	(4, 11)	(4, 26)	(36, 4)	(36, 33)	(34, 14)	(34, 23)	(6, 17)
7P	(18, 9)	(18, 28)	(35, 36)	(35, 1)	(26, 7)	(26, 30)	(33, 15)
8P	(1, 21)	(1, 16)	(18, 28)	(18, 9)	(0, 5)	(0, 32)	(8, 3)
9P	(29, 35)	(29, 2)	(4, 11)	(4, 26)	(9, 30)	(9 , 7)	(30, 25)
10P	(33, 15)	(33, 22)	(0, 5)	(0, 32)	(36, 33)	(36, 4)	(29, 35)
11P	(9, 7)	(9, 30)	(34, 23)	(34, 14)	(30, 12)	(30, 25)	(28, 36)
12P	(26, 7)	(26, 30)	(1, 21)	(1, 16)	(33, 15)	(33, 22)	(36, 33)
13P	(12, 6)	(12, 31)	(28, 36)	(28, 1)	(35, 36)	(35, 1)	(1, 21)
14P	(2, 7)	(2, 30)	(30, 25)	(30, 12)	(12, 31)	(12, 6)	(35, 1)
15P	(8, 34)	(8, 3)	(33, 15)	(33, 22)	(4, 26)	(4, 11)	(34, 23)
16P	(28, 1)	(28, 36)	(2, 30)	(2, 7)	(11, 1)	(11, 36)	(18, 9)
17P	(35, 36)	(35, 1)	(11, 36)	(11, 1)	(1, 21)	(1, 16)	(0, 5)
18P	(0, 32)	(0, 5)	(26, 7)	(26, 30)	(8, 34)	(8, 3)	(4, 26)
19P	(0, 5)	(0, 32)	(26, 30)	(26, 7)	(8, 3)	(8, 34)	(4, 11)
20P	(35, 1)	(35, 36)	(11, 1)	(11, 36)	(1, 16)	(1, 21)	(0, 32)
21P	(28, 36)	(28, 1)	(2, 7)	(2, 30)	(11, 36)	(11, 1)	(18, 28)
22P	(8, 3)	(8, 34)	(33, 22)	(33, 15)	(4, 11)	(4, 26)	(34, 14)
23P	(2, 30)	(2, 7)	(30, 12)	(30, 25)	(12, 6)	(12, 31)	(35, 36)
24P	(12, 31)	(12, 6)	(28, 1)	(28, 36)	(35, 1)	(35, 36)	(1, 16)
25P	(26, 30)	(26, 7)	(1, 16)	(1, 21)	(33, 22)	(33, 15)	(36, 4)
26P	(9, 30)	(9, 7)	(34, 14)	(34, 23)	(30, 25)	(30, 12)	(28, 1)
27P	(33, 22)	(33, 15)	(0, 32)	(0, 5)	(36, 4)	(36, 33)	(29, 2)
28P	(29, 2)	(29, 35)	(4, 26)	(4, 11)	(9, 7)	(9, 30)	(30, 12)
29P	(1, 16)	(1, 21)	(18, 9)	(18, 28)	(0, 32)	(0, 5)	(8, 34)
30P	(18, 28)	(18, 9)	(35, 1)	(35, 36)	(26, 30)	(26, 7)	(33, 22)
31P	(4, 26)	(4, 11)	(36, 33)	(36, 4)	(34, 23)	(34, 14)	(6, 20)
32P	(34, 23)	(34, 14)	(29, 35)	(29, 2)	(6, 20)	(6, 17)	(2, 7)
33P	(36, 33)	(36, 4)	(8, 3)	(8, 34)	(29, 35)	(29, 2)	(9, 30)
34P	(30, 25)	(30, 12)	(6, 17)	(6, 20)	(28, 1)	(28, 36)	(11, 1)
35P	(6, 17)	(6, 20)	(9, 7)	(9, 30)	(2, 30)	(2, 7)	(12, 6)
36P	(11, 36)	(11, 1)	(12, 31)	(12, 6)	(18, 28)	(18, 9)	(26, 30)

Lampiran 1: Tabel Generator Grup Eliptik $E(F_p)$ (Lanjutan)

P	(26, 30)	(28, 1)	(28, 36)	(29, 2)	(29, 35)	(30, 12)	(30, 25)
2P	(12, 6)	(34, 23)	(34, 14)	(0, 5)	(0, 32)	(4, 11)	(4, 26)
3P	(11, 1)	(9, 7)	(9, 30)	(33, 15)	(33, 22)	(29, 35)	(29, 2)
4P	(9, 30)	(33, 22)	(33, 15)	(11, 1)	(11, 36)	(26, 7)	(26, 30)
5P	(2, 7)	(4, 11)	(4, 26)	(1, 16)	(1, 21)	(8, 34)	(8, 3)
6P	(6, 20)	(8, 3)	(8, 34)	(35, 1)	(35, 36)	(0, 32)	(0, 5)
7P	(33, 22)	(11, 1)	(11, 36)	(9, 7)	(9, 30)	(28, 36)	(28, 1)
8P	(8, 34)	(35, 36)	(35, 1)	(6, 20)	(6, 17)	(12, 31)	(12, 6)
9P	(30, 12)	(36, 33)	(36, 4)	(18, 28)	(18, 9)	(33, 22)	(33, 15)
10P	(29, 2)	(26, 7)	(26, 30)	(28, 36)	(28, 1)	(18, 28)	(18, 9)
11P	(28, 1)	(29, 2)	(29, 35)	(26, 7)	(26, 30)	(36, 33)	(36, 4)
12P	(36, 4)	(18, 9)	(18, 28)	(30, 12)	(30, 25)	(11, 36)	(11, 1)
13P	(1, 16)	(2, 30)	(2, 7)	(4, 26)	(4, 11)	(6, 20)	(6, 17)
14P	(35, 36)	(6, 20)	(6, 17)	(8, 3)	(8, 34)	(34, 14)	(34, 23)
15P	(34, 14)	(0, 32)	(0, 5)	(12, 6)	(12, 31)	(1, 21)	(1, 16)
16P	(18, 28)	(30, 25)	(30, 12)	(36, 4)	(36, 33)	(9, 7)	(9, 30)
17P	(0, 32)	(12, 6)	(12, 31)	(34, 23)	(34, 14)	(2, 7)	(2, 30)
18P	(4, 11)	(1, 16)	(1, 21)	(2, 30)	(2, 7)	(35, 36)	(35, 1)
19P	(4, 26)	(1, 21)	(1, 16)	(2, 7)	(2, 30)	(35, 1)	(35, 36)
20P	(0, 5)	(12, 31)	(12, 6)	(34, 14)	(34, 23)	(2, 30)	(2, 7)
21P	(18, 9)	(30, 12)	(30, 25)	(36, 33)	(36, 4)	(9, 30)	(9, 7)
22P	(34, 23)	(0, 5)	(0, 32)	(12, 31)	(12, 6)	(1, 16)	(1, 21)
23P	(35, 1)	(6, 17)	(6, 20)	(8, 34)	(8, 3)	(34, 23)	(34, 14)
24P	(1, 21)	(2, 7)	(2, 30)	(4, 11)	(4, 26)	(6, 17)	(6, 20)
25P	(36, 33)	(18, 28)	(18, 9)	(30, 25)	(30, 12)	(11, 1)	(11, 36)
26P	(28, 36)	(29, 35)	(29, 2)	(26, 30)	(26, 7)	(36, 4)	(36, 33)
27P	(29, 35)	(26, 30)	(26, 7)	(28, 1)	(28, 36)	(18, 9)	(18, 28)
28P	(30, 25)	(36, 4)	(36, 33)	(18, 9)	(18, 28)	(33, 15)	(33, 22)
29P	(8, 3)	(35, 1)	(35, 36)	(6, 17)	(6, 20)	(12, 6)	(12, 31)
30P	(33, 15)	(11, 36)	(11, 1)	(9, 30)	(9, 7)	(28, 1)	(28, 36)
31P	(6, 17)	(8, 34)	(8, 3)	(35, 36)	(35, 1)	(0, 5)	(0, 32)
32P	(2, 30)	(4, 26)	(4, 11)	(1, 21)	(1, 16)	(8, 3)	(8, 34)
33P	(9, 7)	(33, 15)	(33, 22)	(11, 36)	(11, 1)	(26, 30)	(26, 7)
34P	(11, 36)	(9, 30)	(9, 7)	(33, 22)	(33, 15)	(29, 2)	(29, 35)
35P	(12, 31)	(34, 14)	(34, 23)	(0, 32)	(0, 5)	(4, 26)	(4, 11)
36P	(26, 7)	(28, 36)	(28, 1)	(29, 35)	(29, 2)	(30, 25)	(30, 12)

Lampiran 1: Tabel Generator Grup Eliptik $E(F_p)$ (Lanjutan)

P	(33, 15)	(33, 22)	(34, 14)	(34, 23)	(35, 1)	(35, 36)	(36, 4)	(36, 33)
2P	(35, 1)	(35, 36)	(33, 15)	(33, 22)	(30, 12)	(30, 25)	(1, 21)	(1, 16)
3P	(18, 28)	(18, 9)	(8, 34)	(8, 3)	(2, 30)	(2, 7)	(26, 7)	(26, 30)
4P	(30, 12)	(30, 25)	(35, 1)	(35, 36)	(4, 11)	(4, 26)	(28, 1)	(28, 36)
5P	(12, 6)	(12, 31)	(26, 30)	(26, 7)	(9, 30)	(9, 7)	(35, 1)	(35, 36)
6P	(2, 30)	(2, 7)	(18, 28)	(18, 9)	(29, 35)	(29, 2)	(12, 31)	(12, 6)
7P	(36, 33)	(36, 4)	(6, 17)	(6, 20)	(1, 16)	(1, 21)	(29, 2)	(29, 35)
8P	(4, 11)	(4, 26)	(30, 12)	(30, 25)	(26, 7)	(26, 30)	(34, 23)	(34, 14)
9P	(28, 1)	(28, 36)	(1, 21)	(1, 16)	(34, 23)	(34, 14)	(11, 36)	(11, 1)
10P	(9, 30)	(9, 7)	(12, 6)	(12, 31)	(8, 34)	(8, 3)	(30, 12)	(30, 25)
11P	(11, 36)	(11, 1)	(0, 32)	(0, 5)	(6, 17)	(6, 20)	(18, 9)	(18, 28)
12P	(29, 35)	(29, 2)	(2, 30)	(2, 7)	(0, 32)	(0, 5)	(9, 7)	(9, 30)
13P	(0, 5)	(0, 32)	(29, 2)	(29, 35)	(11, 1)	(11, 36)	(8, 34)	(8, 3)
14P	(1, 16)	(1, 21)	(36, 33)	(36, 4)	(28, 36)	(28, 1)	(0, 5)	(0, 32)
15P	(6, 20)	(6, 17)	(11, 1)	(11, 36)	(36, 4)	(36, 33)	(2, 30)	(2, 7)
16P	(26, 7)	(26, 30)	(4, 11)	(4, 26)	(12, 31)	(12, 6)	(33, 22)	(33, 15)
17P	(8, 3)	(8, 34)	(9, 7)	(9, 30)	(18, 9)	(18, 28)	(4, 26)	(4, 11)
18P	(34, 23)	(34, 14)	(28, 1)	(28, 36)	(33, 22)	(33, 15)	(6, 17)	(6, 20)
19P	(34, 14)	(34, 23)	(28, 36)	(28, 1)	(33, 15)	(33, 22)	(6, 20)	(6 , 17)
20P	(8, 3)	(9, 30)	(9, 7)	(18, 28)	(18, 9)	(18, 9)	(4, 11)	(4, 26)
21P	(26, 30)	(26, 7)	(4, 26)	(4, 11)	(12, 6)	(12, 31)	(33, 15)	(33, 22)
22P	(6, 17)	(6, 20)	(11, 36)	(11, 1)	(36, 33)	(36, 4)	(2, 7)	(2, 30)
23P	(1, 21)	(1, 16)	(36, 4)	(36, 33)	(28, 1)	(28, 36)	(0, 32)	(0, 5)
24P	(0, 32)	(0, 5)	(29, 35)	(29, 2)	(11, 36)	(11, 1)	(8, 3)	(8, 34)
25P	(29, 2)	(29, 35)	(2, 7)	(2, 30)	(0, 5)	(0, 32)	(9, 30)	(9, 7)
26P	(11, 1)	(11, 36)	(0, 5)	(0, 32)	(6, 20)	(6, 17)	(18, 28)	(18, 9)
27P	(9, 7)	(9, 30)	(12, 31)	(12, 6)	(8, 3)	(8, 34)	(30, 25)	(30, 12)
28P	(28, 36)	(28, 1)	(1, 16)	(1, 21)	(34, 14)	(34. 23)	(11, 1)	(11, 36)
29P	(4, 26)	(4, 11)	(30, 25)	(30, 12)	(26, 30)	(26, 7)	(34, 14)	(34, 23)
30P	(36, 4)	(36, 33)	(6, 20)	(6, 17)	(1, 21)	(1, 16)	(29, 35)	(29, 2)
31P	(2, 7)	(2, 30)	(18, 9)	(18, 28)	(29, 2)	(29, 35)	(12, 6)	(12, 31)
32P	(12, 31)	(12, 6)	(26, 7)	(26, 30)	(9, 7)	(9, 30)	(35, 36)	(35, 1)
33P	(30, 25)	(30, 12)	(35, 36)	(35, 1)	(4, 26)	(4, 11)	(28, 36)	(28, 1)
34P	(18, 9)	(18, 28)	(8, 3)	(8, 34)	(2, 7)	(2, 30)	(26, 30)	(26, 7)
35P	(35, 36)	(35, 1)	(33, 22)	(33, 15)	(30, 25)	(30, 12)	(1, 16)	(1, 21)
36P	(33, 22)	(33, 15)	(34, 23)	(34, 14)	(35, 36)	(35, 1)	(36, 33)	(36, 4)

Lampiran 2: Program Java untuk Menentukan Elemen-Elemen Grup Eliptik $E_{37}(8, 25)$

```
package titik_kurva;
public class Titik_kurva {
    public static void main(String[] args) {
        int p=43;
        int a=8;
        int b=25;
        int []qr=new int [p];
        int []kurva=new int [p];
        System.out.println("=========Titik-Titik Kurva
Eliptik===============");
        System.out.println("x"+"\t"+"y");
        for(int i=0; i<p; i++){
            qr[i]=(i*i)%p;
            kurva[i]=((i*i*i)+a*i+b)%p;
        }
        for(int x=0; x<p; x++){
            for(int y=0; y<p; y++){
                if(kurva[x]==qr[y]){
                    System.out.println(x+"\t"+y);
                }
            }
        }
    }
}
```

Lampiran 3: Program Java Penjumlahan Dua Titik Kurva Eliptik

```
package ganda;
public class Ganda {
    public static void main(String[] args) {
        int p=37;
        int x=6;
        int y=17;
        System.out.println("x"+"\t"+"y");
        System.out.println("===============");
        System.out.println(x+"\t"+y);
        int atas=((3*(x*x))+8)%p;
        int bawah=(2*y)%p;
        int belakang=2*x%p;
        for(int z=0; z<p; z++){
            if((bawah*z)%p==1){
                int depan=(atas*z)%p;
                int dk=depan*depan%p;
                int x2=dk-belakang%p;
                if(x2<0){
                    int mq=p*(-1);
                    int h=x2-mq;
                    System.out.print(h+"\t");
                }else{
```

```
                System.out.print(x2+"\t");
            }
            int y2=((depan*(x-x2))-y)%p;
            if(y2<0){
                int mq=p*(-1);
                int h=y2-mq;
                System.out.println(h);
            }else{
                System.out.println(y2);
            }
            x2=36;
            y2=33;
            int top=(y2-y)%p;
            int bottom=(x2-x)%p;
            for(int k=0; k<p; k++){
                if((bottom*k)%p==1){
                    int front=(top*k)%p;
                    int fk=(front*front)%p;
                    int x3=(fk-x-x2)%p;
                    if(x3<0){
                        int temp=p*(-1);
                        int r=x3-temp;
                        System.out.print(r+"\t");
                    }else{
                        System.out.print(x3+"\t");
                    }
                    int awal=(x-x3)%p;
                    int kali=(front*awal)%p;
                    int y3=(kali-y)%p;
                    if(y3<0){
                        int temp=p*(-1);
                        int r=y3-temp;
                        System.out.println(r);
                    }else{
                        System.out.println(y3);
                    }
                }
            }
        }
    }
}
```

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang (0341)551345 Fax.(0341)572533

BUKTI KONSULTASI SKRIPSI

Nama : Febrina Mediawati Setyobudi
NIM : 09610007
Fakultas/ Jurusan : Sains dan Teknologi/ Matematika
Judul Skripsi : Penggunaan Kriptografi Kurva Eliptik pada Proses Penyandian Elgamal
Pembimbing I : Abdussakir, M.Pd
Pembimbing II : Dr. H. Ahmad Barizi, MA

No	Tanggal	Hal	Tanda Tangan
1.	9 November 2012	Konsultasi Bab I, II	1.
2.	27 November 2012	Konsultasi Keagamaan Bab I	2.
3.	13 Desember 2012	Revisi Keagamaan Bab I	3.
4.	14 Desember 2012	ACC Proposal	4.
5.	14 Januari 2013	Revisi Proposal	5.
6.	17 Januari 2013	Konsultasi Keagamaan Bab II	6.
7.	21 Januari 2013	Revisi Keagamaan Bab II	7.
8.	23 Januari 2013	Konsultasi Bab I, II, III	8.
9.	30 Januari 2013	Revisi Bab III	9.
10.	9 Februari 2013	Konsultasi Bab III	10.
11.	12 Februari 2013	Konsultasi Bab I, II, III	11.
12.	13 Februari 2013	Revisi Bab I, II, III	12.

Malang, 13 Februari 2013

Mengetahui,
Ketua Jurusan Matematika

Abdussakir, M.Pd
NIP. 19751006 200312 1 001