SKRIPSI

KRIPTOGRAFI KUNCI PUBLIK KURVA ELIPTIK ATAS LAPANGAN HINGGA DAN IMPLEMENTASINYA MENGGUNAKAN BAHASA PEMROGRAMAN PYTHON UNTUK MEMBUAT *PYTHON PACKAGES*

DAVID IMAN FAUZAN

14610015

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2019

KRIPTOGRAFI KUNCI PUBLIK KURVA ELIPTIK ATAS LAPANGAN HINGGA DAN IMPLEMENTASINYA MENGGUNAKAN BAHASA PEMROGRAMAN PYTHON UNTUK MEMBUAT *PYTHON PACKAGES*

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

DAVID IMAN FAUZAN

14610015

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2019

ABSTRAK

Kriptografi Kunci Publik Kurva Eliptik atas Lapangan Hingga dan Implementasinya Menggunakan Bahasa Pemrograman Python untuk membuat *Python Packages*

Oleh

DAVID IMAN FAUZAN

14610015

Internet merupakan jalur komunikasi yang berguna sebagai sarana untuk saling bertukar informasi. Akan tetapi, internet merupakan jalur komunikasi yang tidak aman, sehingga informasi yang dikirimkan melalui internet mudah disalah gunakan oleh pihak-pihak yang tidak berwenang. Kriptografi Kurva Eliptik *(ECC: Elliptic Curve Cryptography)* memberikan solusi terhadap permasalahan keamanan informasi. *ECC* merupakan salah satu metode untuk melakukan kriptografi kunci publik yang secara independen ditemukan pada tahun 1985 oleh Neal Koblitz dan Victor S. Miller.

Penelitian ini bertujuan untuk memahami konsep dari kriptografi kunci publik kurva eiptik. Kurva Eliptik E yang digunakan didefinisikan atas Lapangan Hingga $\mathbb{Z}_p$, kemudian diaplikasikan pada Protokol Pertukaran Kunci Diffie-Hellman, sistem kriptografi El-Gamal, *(Elliptic Curve Integrated Encryption Scheme)*, dan algoritma tanda tangan digital berdasar pada Kurva Eliptik atas Lapangan Hingga $\mathbb{Z}_p$.

Hasil dari penelitian ini yaitu implementasi kriptografi kunci publik kurva eliptik dalam bentuk Python *Package* (Paket yang dibuat berdasarkan bahasa pemrograman Python) yang dapat dipakai dan dikembangkan secara bebas.

Kata kunci: lapangan hingga, kurva eliptik, diffie-hellman, elgamal, enkripsi/dekripsi, tanda tangan digital, python.

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : David Iman Fauzan

NIM : 14610015

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 31 Januari 2019

Yang Menyatakan

David Iman Fauzan

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : 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 : David Iman Fauzan
NIM : 14610015
Judul Skripsi : Kriptografi Kunci Publik Kurva Eliptik atas Lapangan Hingga dan Implementasinya Menggunakan Bahasa Pemrograman Python untuk membuat Python Packages

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 dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 31 Januari 2019
Pembimbing

M Zaki Riyanto, M.Sc.
NIP: 19840113 201503 1 001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-579/Un.02/DST/PP.00.9/02/2019

Tugas Akhir dengan judul : KRIPTOGRAFI KUNCI PUBLIK KURVA ELIPTIK ATAS LAPANGAN HINGGA DAN IMPLEMENTASINYA MENGGUNAKAN BAHASA PEMROGRAMAN PYTHON UNTUK MEMBUAT PYTHON PACKAGES

yang dipersiapkan dan disusun oleh:

Nama : DAVID IMAN FAUZAN
Nomor Induk Mahasiswa : 14610015
Telah diujikan pada : Rabu, 06 Februari 2019
Nilai ujian Tugas Akhir : A

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

Penguji I

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

Penguji II

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

Yogyakarta, 06 Februari 2019
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
DEKAN

Dr. Murtono, M.Si.
NIP. 19691212 200003 1 001

HALAMAN MOTTO

"Tunjukkanlah bukti kebenaranmu jika kamu adalah orang yang benar."

(QS. Al-Baqarah :111)

HALAMAN PERSEMBAHAN

Karya sederhana ini penulis persembahkan

untuk Almamater Universitas Islam Negeri Sunan

Kalijaga Yogyakarta tercinta

PRAKATA

Assalamu 'alaikum wr. wb.

Dengan menyebut nama Allah Yang Maha Pemurah lagi Maha Penyayang, puji syukur kami ucapkan kehadirat-Nya. Sholawat serta salam senantiasa tercurah kepada Rasulullah SAW beserta para sahabat, keluarga, dan Insya Allah semua umatnya yang tegar mengemban dakwah hingga akhir zaman. Dan berkat Rahmat Allah SWT, penulis dapat menyusun dan menyelesaikan skripsi ini.

Penulisan skripsi ini dilakukan untuk memenuhi salah satu syarat guna mencapai gelar Sarjana Matematika Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Penulis menyadari banya kesulitan yang ditemui dalam menyelesaikan skripsi ini. Tanpa bantuan dan bimbingan dari berbagai pihak sejak penyusunan proposal sampai dengan terselesaikannya laporan hasil skripsi ini. Untuk itu penulis menyampaikan terimakasih yang sebesar-besarnya serta penghargaan yang setinggi-tingginya kepada:

1. Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta, Bapak Prof. Drs. Yudian Wahyudi, M.A., Ph.D. yang telah memberi kesempatan kepada penulis untuk membina ilmu di Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

2. Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta, Bapak Dr. Murtono, M.Si. yang telah menyediakan sarana dan prasarana kepada penulis sehingga dapat menyelesaikan tugas ini dengan lancar.

3. Bapak Dr. Muhammad Wakhid Musthofa, S.Si., M.Si. selaku ketua Prodi Matematika Universitas Islam Negeri Sunan Kalijaga Yogyakarta yang telah memberi kesempatan kepada penulis untuk belajar di Prodi Matematika Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
4. Ibu Malahayati, S.Si., M.Sc. selaku Dosen Pembimbing Akademik penulis yang telah memberikan arahan terkait akademik kepada penulis selama menempuh pendidikan di Prodi Matematika Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
5. Bapak Muhamad Zaki Riyanto, S.Si., M.Sc. selaku Dosen Pembimbing Skripsi yang telah menyediakan waktu, tenaga, dan pikiran untuk membimbing penulis dalam menyusun skripsi ini.
6. Seluruh Doden Prodi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
7. Seluruh staf pengajar Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta yang telah memberi bekal pengetauan kepada penulis.
8. Kedua orangtua penulis dan keluarga yang senantiasa memberikan dukungan moral maupun materi.
9. Kepada semua sahabat penulis, element math 14 yang tidak henti-hentinya mendoakan dan selalu memberikan semangat.
10. Serta semua pihak yang tidak mungkin penulis sebutkan satu-persatu atas bantuannya secara langsung maupun tidak langsung sehingga skripsi ini dapat terselesaikan dengan baik.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Penulis berharap semoga skripsi ini dapat bermanfaat bagi kita semua.

Yogyakarta, 30 November 2018

David Iman Fauzan

DAFTAR ISI

DAFTAR TABEL

DAFTAR LAMBANG

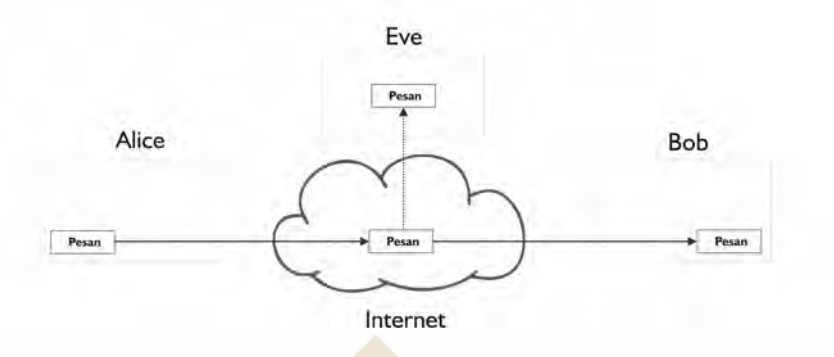
$\mathbb{Z}$	: Himpunan semua bilangan bulat
$\mathbb{Z}_m$	: Himpunan semua bilangan bulat modulo m
$x \in A$	: x anggota himpunan A
$a \mid n$	: a membagi habis n
$<$	: kurang dari
$>$	: lebih besar dari
$\leq$	: lebih kecil dari atau sama dengan
$\geq$	: lebih besar dari atau sama dengan
$\lvert a \rvert$	: 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
$a \mod b$	: a modulo b
$a \equiv b \pmod{m}$	: a kongruen b modulo m
$a \not\equiv b \pmod{m}$	: a tidak kongruen b modulo m
a^{-1}	: invers dari a
$(G, *)$	: grup G disertai operasi biner $*$
$\lvert G \rvert$	: banyaknya elemen G
$(R, +, \cdot)$	: ring R disertai perasi penjumlahan dan perkalian biasa
$E(\mathbb{Z}_p)$	: kurva eliptik atas lapangan hingga $\mathbb{Z}_p$
■	: akhir suatu bukti

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Di zaman yang serba modern ini segala macam informasi dengan mudah dapat kita peroleh melalui berbagai media, salah satunya adalah media elektronik seperti komputer dan *smartphone*. Teknologi informasi tidak hanya terbatas pada teknologi komputer yang digunakan untuk memproses dan menyimpan informasi, melainkan juga mencakup teknologi komunikasi untuk mengirimkan informasi. Pesatnya perkembangan teknologi dan komunikasi memberikan kemudahan kepada manusia untuk saling bertukar informasi ataupun data. Jalur komunikasi yang populer saat ini adalah internet, dimana internet merupakan jaringan komputer yang saling terhubung antara satu komputer dengan komputer yang lain. Namun, internet merupakan jalur komunikasi yang tidak aman *(insecure channel)* (di ilustrasikan pada gambar 1.1), sehingga kemudahan ini juga dimanfaatkan oleh pihak-pihak yang tidak berwenang untuk menyadap informasi ataupun data yang dikirimkan melalui internet. Apalagi penyadapan ini akan sangat berbahaya apabila informasi yang disadap merupakan informasi rahasia seperti data pemerintahan, kemiliteran, perbankan, dan data rahasia lainnya.



Gambar 1.1 Komunikasi melalui internet

Untuk mencegah terjadinya penyadapan informasi maka perlu adanya sistem keamanan jaringan yang dapat melindungi beberapa aspek penting. Beberapa aspek penting tersebut ialah Kerahasiaan *(confidentiality)* untuk memastikan bahwa informasi elektronik tidak diketahui/bocor kepada pihak yang tidak berhak mengetahuinya, Integritas *(integrity)* untuk memastikan bahwa informasi elektronik tidak mengalami perubahan/modifikasi selama disimpan atau dikirimkan, Keaslian *(authenticity)* untuk memastikan bahwa informasi elektronik dibuat atau dikirimkan oleh pihak yang sah/asli. (Stallings, 2014)

Kriptografi Kurva Eliptik *(ECC: Elliptic Curve Cryptography)* memberikan solusi terhadap permasalahan keamanan informasi. *ECC* merupakan salah satu metode untuk melakukan kriptografi kunci publik yang secara independen ditemukan pada tahun 1985 oleh Neal Koblitz dan Victor S. Miller. Salah satu keunggulan dari kriptografi kurva eliptik mereka adalah tingkat keamanan yang setara dengan RSA dengan kunci yang jauh lebih kecil. Sebagai contoh, telah diperkirakan bahwa kunci kurva eliptik 313-bit seaman kunci RSA 4096-bit. (Bauer, 2013)

Dalam skripsi ini akan dibahas mengenai Protokol pertukaran kunci Diffie-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES (Elliptic Curve Integrated Encryption Scheme)*, dan Algoritma Tanda Tangan Digital Kurva Eliptik

(ECDSA: Elliptic Curve Digital Signature Algorithm) yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$ yang kemudian akan diimplementasikan menggunakan bahasa pemrograman Python dengan membuat Paket Python (*Python Packages*). Python merupakan bahasa pemrograman interpretatif multiguna. Tidak seperti bahasa lain yang susah untuk dibaca dan dipahami, python lebih menekankan pada keterbacaan kode agar lebih mudah untuk memahami sintaks. Sedangkan Paket Python *(Python Packages)* adalah suatu folder yang berisikan modul-modul yang memuat definisi dari fungsi maupun variabel yang dapat digunakan dalam membuat suatu program python ataupun menjalankannya langsung dalam intepreter.

1.2. Batasan Masalah

Batasan masalah sangat diperlukan untuk memfokuskan sebuah pembahasan guna menghindari meluas dan kesimpangsiuran pembahasan. Berdasarkan latar belakang masalah, penelitian ini difokuskan untuk membahas konsep matematis yang melandasi Protokol pertukaran kunci Diffie-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES*, dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$. Diberikan pula implementasi dari sistem kriptografi tersebut menggunakan bahasa pemrograman Python dengan membuat *Python Packages*.

1.3. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan, maka dirumuskan permasalahan-permasalahan sebagai berikut:

1. Bagaimana konsep matematis yang melandasi Protokol pertukaran kunci Diffie-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES* dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$.

2. Bagaimana proses Algoritma Protokol pertukaran kunci Diffi-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES* , dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$.

3. Bagaimana implementasi dari Algoritma Protokol pertukaran kunci Diffie-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES* , dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$ menggunakan bahasa pemrograman Python dalam bentuk *Python Packages*.

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disebutkan, tujuan dari penulisan skripsi ini adalah sebagai berikut:

1. Mengkaji konsep matematis yang melandasi Protokol pertukaran kunci Diffie-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES* dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$.

2. Mengetahui proses Algoritma Protokol pertukaran kunci Diffi-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES* , dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$.

3. Mengimplementasikan Algoritma Protokol pertukaran kunci Diffi-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES*, dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$ menggunakan bahasa pemrograman Python dalam bentuk *Python Packages*.

1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat membemberi manfaat, diantaranya sebagai berikut :

1. Memberi pengetahuan tentang teori bilangan khususnya bilangan bulat dan struktur aljabar khususnya teori grup, ring, dan lapangan.

2. Memberi pengetahuan tentang konsep kurva elliptik mulai dari kurva eliptik atas bilangan real, kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$, sampai masalah logaritma diskrit yang ada pada kurva eliptik sehingga dapat diaplikasikan kedalam kriptografi kunci puplik.

3. Memberi pengetahuan tentang kriptografi kunci publik kurva elliptik khususnya Protokol pertukaran kunci Diffi-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES* , dan *ECDSA* yang dibangun berdasar kurva eliptik atas Lapangan Hingga $\mathbb{Z}_p$.

1.6. Tinjauan Pustaka

Penulisan skripsi ini terinspirasi dari paper yang ditulis oleh Manoj Kumar dan Pratik Gupta (2016) yang membahas tentang Skema Kriptografi berdasar Kurva Eliptik atas Ring $\mathbb{Z}_p[i]$ mulai dari konsep dasar matematis, sistem pertukaran kunci, pembentukan kunci, enkripsi hingga dekripsi dengan terperinci sehingga sangat membantu penulis dalam memahami skema kriptografi kurva eliptik secara umum. Selain itu terdapat skripsi yang ditulis M. Zaki Riyanto, M.Sc. (2007) yang membahas tentang pengamanan pesan rahasia menggunakan algoritma kriptografi ElGamal atas grup perkalian $\mathbb{Z}_p^*$ mulai dari konsep dasar matematis yaitu bilangan bulat, struktur aljabar, hingga algoritma kriptografi ElGamal atas grup perkalian $\mathbb{Z}_p^*$ dengan terperinci sehingga sangat membantu penulis dalam memahami algoritma kriptografi ElGamal atas grup perkalian $\mathbb{Z}_p^*$. Terdapat juga paper yang ditulis oleh Ounasser Abid, Jaouad Ettanfouhi, Omar Khadir (2012) yang membahas tentang protokol tanda tangan digital berdasar kurva eliptik mulai dasar matematis, kurva eliptik, hingga variasi protokol tanda tangan digital ElGamal berdasar kurva eliptik

atas lapangan hingga $\mathbb{Z}_p$.

Perbedaan penelitian ini dengan penelitian sebelumnya adalah menggunakan kurva eliptik atas lapangan hingga $\mathbb{Z}_p$ sebagai dasar kriptografi kunci publik yang terdiri dari Protokol pertukaran kunci Diffi-Hellman, Sistem kriptografi kunci publik ElGamal, *ECIES* , dan *ECDSA*.

1.7. Metode Penelitian

Metode yang digunakan dalam penyusunan tugas akhir ini adalah metode studi literatur. Penelitian ini dilakukan dengan cara membahas dan menjabarkan teorema-teorema dan materi yang bersumber dari buku, jurnal maupun catatan kuliah. Secara umum pembahasan dalam penelitian ini terdiri dari dua bagian, yaitu kriptografi dan struktur aljabar.

Pembahasan awal dari tugas akhir ini adalah mengkaji tentang beberapa hal yang berhubungan dengan kriptografi. Kemudian mengkaji konsep dasar tentang grup, ring, daerah integral, dan lapangan beserta sifat-sifatnya yang dinyatakan dalam beberapa definisi dan teorema. Konsep-konsep ini nantinya digunakan sebagai dasar dalam memahami lapangan hingga *(finite field)*. Kemudian dipelajari tentang kurva eliptik, mulai dari aritmatika kurva eliptik, kurva eliptik atas bilanga real, kurva eliptik atas lapangan hingga, hingga pembentukan grup yang beranggotakan titik-titik pada kurva eliptik.

Selanjutnya, dipelajari tentang aspek-aspek yang berhubungan dengan kriptografi, masalah logaritma diskrit, protokol pertukaran kunci Diffie-Hellman, dan pengamanan pesan rahasia dengan algoritma kriptografi ElGamal, *ECIES*, dan *ECDSA* yang didefinisikan menggunakan kurva eliptik atas lapangan hingga. Setelah itu, konsep algoritma kriptografi yang sudah dibahas diimplementasikan menggunakan bahasa pemrograman Python dalam bentuk *Python Packages*.

1.8. Sistematika Penulisan

Dalam penulisan tugas akhir ini akan di bagi menjadi lima bab yang disusun secara runtun dan sistematis. Berikut ini rincian masing-masing bab ynag akan dijelaskan secara umum, yaitu:

1. BAB I: bab ini membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

2. BAB II: bab ini membahas mengenai kriptografi secara umum, bilangan bulat, dan struktur aljabar yang meliputi konsep dasar tentang grup, ring, daerah integral, dan konsep tentang lapangan hingga.

3. BAB III: bab ini membahas mengenai aritmatika penjumlahan kurva eliptik atas bilangan real dan lapangan berhingga, dan Masalah logaritma diskrit yang berlaku pada kurva eliptik.

4. BAB IV: bab ini membahas mengenai penerapan kurva eliptik pada sistem pertukaran kunci Diffie-Hellman, sistem kriptografi ElGamal, *ECIES*, dan *ECDSA*.

5. BAB V: bab ini membahas mengenai implementasi sistem kriptografi kurva eliptik menggunakan bahasa pemrograman Python dalam bentuk *Python Packages*.

6. BAB VI: bab ini berisi tentang kesimpulan yang merupakan jawaban secara umum dari rumusan masalah dan saran dari penulis mengenai penelitian yang dilakukan.

BAB VI

PENUTUP

6.1. Kesimpulan

Berdasarkan hasil studi literatur tentang kriptografi kunci publik kurva eliptik atas lapangan hingga yang dilakukan penulis dapat ditarik kesimpulan sebagai berikut:

1. Konsep matematis yang melandasi kriptografi kunci publik kurva eliptik dibagi menjadi dua bagian yaitu bilangan bulat dan struktur aljabar. Bilangan bulat meliputi: pembagi persekutuan terbesar, algoritma Euclid dan algoritma Euclid yang diperluas, dan persamaan kongruen. Struktur aljabar meliputi: grup, ring, dan lapangan hingga.

2. Penerapan kriptografi kunci publik kurva eliptik dalam penelitian ini dibagi menjadi empat bagian. Yang pertama yaitu Protokol Pertukaran Kunci Diffie-Hellman yang didasarkan pada kurva eliptik atas lapangan hingga $\mathbb{Z}_p$ yang berguna sebagai pembentukan kunci rahasia yang dapat digunakan dalam penyandian pesan . Kemudian sistem kriptografi El-Gamal berdasar kurva eliptik atas lapangan hingga $\mathbb{Z}_p$ yang dapat digunakan untuk enkripsi dan dekripsi pesan. Sistem kriptografi El-Gamal biasa masih kurang efisien dikarenakan ruang pesan (plainteks) terdiri dari titik-titik pada kurva eliptik. Sistem kriptografi ElGamal yang lebih efisien digunakan dalam kriptografi kurva eliptik adalah *ECIES (Elliptic Curve Integrated Encryption Scheme)* yang didalamya disertakan sistem *Point Compression* dan ruang pesan (plainteks) yang

digunakan yaitu elemen tak nol pada suatu lapangan hingga. Yang terakhir adalah algoritma tanda tangan digital kurva eliptik *(ECDSA: Elliptic Curve Digital Signature Algorithm)* yang berfungsi untuk menandatangani sebuah pesan.

3. Implementasi dari kriptografi kunci publik kurva eliptik atas lapangan hingga menggunakan bahasa pemrograman Python versi 3 dibuat dalam bentuk *packages* yang berisikan modul yang memuat fungsi-fungsi yang dibuat menurut algoritma-algoritma yang telah dipaparkan pada pembahasan. Fungsi-fungsi yang digunakan untuk mencari nilai seperti fungsi sisa kuadratik, tes keprimaan biasa, dan lain-lain masih menggunakan teknik perulangan biasa sehingga program akan berjalan lambat apabila menggunakan parameter bilangan yang besar.

6.2. Saran

Setelah menyelesaikan penelitian ini, saran-saran yang dapat disampaikan adalah sebagai berikut :

1. Penelitian ini hanya membahas kriptografi kunci publik kurva eliptik atas lapangan hingga $\mathbb{Z}_p$. Oleh karena itu, perlu diteliti lebih lanjut menggunakan lapangan hingga yang lain.
2. Implementasi dari kriptografi kunci publik kurva eliptik dalam penelitian ini menggunakan program berbasis teks, sehingga perlu dilakukan penelitian lebih lanjut dengan menggunakan program berbasis desktop, web, maupun mobile.

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

kriptografi kunci publik kurva eliptik.

DAFTAR PUSTAKA

Hoffstein, J., Pipher, J. dan Silverman, J.H. 2008. *An Introduction to Mathematical Cryptography"*. New York: Springer Science + Business Media, LLC.

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

Malik, D. S., Mordeson, Jhon N. dan Sen, M. K. 2007. *Introduction to Abstract Algebra*. USA: Creighton University.

Stinson, Douglas R. 2006. *Cryptography - Theory and Practice, Tird Edition*. New York: CRC Press.

Rosen, Kenneth H. 2011. *Elementary Number Theory and its Applications, Sixth Edition*. USA: Pearson Education, Inc.

Stallings, William. 2014. *Cryptography and Network Security: Principles and Practice, Sixth Edition*. New Jersey: Pearson Education, Inc.

Bauer, Craig P. 2013. *Secret History: The Story of Cryptology*. New York: CRC Press.

A. Menezes,A., Oorschot,P. van, and Vanstone,S. 1996. *Handbook of Applied Cryptography*. New York: CRC Press.

Paar, Christof. Pelzl, Jan. 2009. *Understanding Cryptography*. USA: Springer-Verlag Inc.

Fraleigh, John B. 2003. *A First Course in Abstract Algebra, Seventh Edition*. USA: Addison Wesley Publishing Company, Inc.

Riyanto, M. Zaki. 2007. *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi ElGamal atas Grup Pergandaan* $\mathbb{Z}_p^*$. Yogyakarta: Universitas Gadjah Mada.

Kumar,M., Gupta,P. 2016. *Cryptographic Schemes Based on Elliptic Curves over the Ring* $\mathbb{Z}_p[i]$. Uttrakhand: Scientific Research Publishing Inc.

Linux Mint. 2018. *About Linux Mint*. https://linuxmint.com/about.php. 11 Januari 2018. 10:00.

Python. 2018. *Python Documentation*. https://docs.python.org/3/. 11 Januari 2018. 10:00.