PENERAPAN METODE *NOISELESS STEGANOGRAPHY* DAN *ELLIPTIC CURVES CRYPTOGRAPHY DIGITAL SIGNATURE ALGORITHM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

OLEH
MOHAMAD FEBRY ANDREAN
NIM. 18610103

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

PENERAPAN METODE *NOISELESS STEGANOGRAPHY* DAN *ELLIPTIC CURVES CRYPTOGRAPHY DIGITAL SIGNATURE ALGORITHM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

OLEH
MOHAMAD FEBRY ANDREAN
NIM. 18610103

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

PENERAPAN METODE *NOISELESS STEGANOGRAPHY* DAN *ELLIPTIC CURVES CRYPTOGRAPHY DIGITAL SIGNATURE ALGORITHM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

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

Oleh
Mohamad Febry Andrean
NIM. 18610103

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

PENERAPAN METODE *NOISELESS STEGANOGRAPHY* DAN *ELLIPTIC CURVES CRYPTOGRAPHY DIGITAL SIGNATURE ALGORITHM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

Oleh
Mohamad Febry Andrean
NIM. 18610103

Telah Diperiksa dan Disetujui untuk Diuji
Malang, 20 Juni 2022

Dosen Pembimbing I	Dosen Pembimbing II
Juhari, M.Si.	Ach. Nashichuddin, M.A.
NIDT. 19840209 20160801 1 055	NIP. 19730705 200003 1 001

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, S.Pd., M.Sc,
NIP. 19741129 200012 2 005

PENERAPAN METODE *NOISELESS STEGANOGRAPHY* DAN *ELLIPTIC CURVES CRYPTOGRAPHY DIGITAL SIGNATURE ALGORITHM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

Oleh
Mohamad Febry Andrean
NIM. 18610103

Telah Dipertahankan di Depan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S. Mat)
Tanggal 24 Juni 2022

Ketua Penguji	: Ari Kusumastuti, M.Pd., M.Si.	.....
Anggota Penguji I	: Dr. Heni Widayani, M. Si.	.....
Anggota Penguji II	: Juhari, M.Si.	.....
Anggota Penguji III	: Ach. Nashichuddin, M.A.	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Lily Susanti, M.Sc
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertandatangan di bawah ini:

Nama	: Mohamad Febry Andrean
NIM	: 18610103
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Penerapan Metode *Noiseless Steganography* dan *Elliptic Curves Cryptography Digital Signature Algorithm* Pada Pengamanan Pesan Teks

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

Malang, 16 Juni 2022

Yang membuat pernyataan,

Mohamad Febry Andrean

NIM. 18610103

MOTO

“Memulai dengan Penuh Keyakinan, Menjalankan dengan Penuh Keikhlasan,

Menyelesaikan dengan Penuh Kebahagiaan**”**

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Kedua orang tua tercinta yaitu Alm. Bapak Jazuli dan Ibu Supi'ani serta adik Ayunda Yuniastanti, yang tidak pernah putus dalam memanjatkan do'a dan memberikan restu serta nasihat kepada penulis.

Seluruh keluarga dan para karyawan yang senantiasa memberi dukungan dan nasihat kepada penulis. Sahabat-sahabat penulis dan seluruh teman-teman HIMMAH dan AKSIOMA yang telah memberi semangat kepada penulis dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Segala puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayahnya sehingga penulis dapat menyelesaikan proposal skripsi ini sebagai syarat untuk mendapatkan gelar sarjana di bidang matematika Fakultas Sains dan Teknologi di Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Tak lupa pula ucapan terima kasih untuk pihak-pihak yang telah membantu dan memotivasi kepada penulis, yakni kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Juhari, M.Si, selaku Dosen Pembimbing I.
5. Ach. Nashichuddin, M.A, selaku Dosen Pembimbing II.
6. Ari Kusumastuti, M.Pd., M.Si., selaku Ketua Penguji dalam Ujian Skripsi.
7. Dr. Heni Widayani, M. Si., selaku Penguji Utama dalam Ujian Skirpsi.
8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
9. Orang tua dan seluruh keluarga yang selalu memberikan dukungan baik moral maupun moril, serta semangat dan doa.
10. Sahabat dan teman-teman yang selalu membantu, menemani dan memberikan dukungan sehingga skripsi ini dapat diselesaikan.
11. Seluruh mahasiswa prodi Matematika angkatan 2018.

Malang, 25 Mei 2022

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ABSTRAK

Andrean, Mohamad Febry. 2022. **Penerapan Metode *Noiseless Steganography* dan *Elliptic Curves Cryptography Digital Signature Algorithm***. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Juhari, M.Si. (II) Ach. Nashichuddin, M.A.

Kata Kunci : Kriptografi, Steganografi, Algoritma, Kurva Eliptik, Digital Signature

Kriptografi kurva eliptik termasuk sistem kriptografi kunci simetris yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Ada beberapa cara yang dapat digunakan untuk mendefinisikan persamaan kurva eliptik yang tergantung pada medan berhingga yang digunakan yaitu salah satunya medan berhingga prima (F_P dimana $p > 3$). Kriptografi kurva eliptik dapat digunakan untuk beberapa keperluan protokol, tanda tangan digital, dan skema enkripsi. Tujuan penelitian ini untuk mengetahui proses penyembunyian pesan terenkripsi menggunakan metode *Noiseless Steganography* serta pembangkitan kunci privat dan kunci publik dan proses verifikasi keabsahan *Elliptic Curves Cryptography Digital Signature Algorithm* (ECDSA). Hasil dari skripsi ini adalah didapatkan sebuah grafik garis yang menyimpan atau menyembunyikan sebuah pesan menggunakan metode *steganography* dan sebuah keaslian pesan dari proses pembangkitan kunci dan verifikasi keabsahan dengan menggunakan metode ECDSA. Dengan memilih tiga sampel yang terdiri dari satu sampel uji dan dua sampel pembeda didapatkan grafik garis, nilai *hash* MD5, dan nilai pada titik $M(r, s)$ berbeda. Secara berturut-turut diperoleh nilai $M(r, s)$ untuk pesan "Matematika 2018", "MATEMATIKA 2018", dan "2018 matematika" adalah $M(94{,}67), M(15{,}17), dan\ M(9{,}16)$. Pembahasan dalam skripsi ini hanya meliputi tentang kurva eliptik pada medan berhingga prima saja. Maka untuk skripsi selanjutnya dapat melakukan pembahsan mengenai kurva eliptik pada medan berhingga (F_{2^m}) atau penerapan kriptografi kurva eliptik dan metode steganografi lainya.

ABSTRACT

Andrean, Mohamad Febry. 2022. **On the Application of Noiseless Steganography Method and Elliptic Curves Cryptography Digital Signature Algorithm**. Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisors: (I) Juhari, M.Si. (II) Ach. Nashichuddin, M.A.

Keywords : Cryptography, Steganography, Algorithm, Elliptic Curve, Digital Signature

Elliptic curve cryptography includes symmetric key cryptography systems that base their security on mathematical problems of elliptic curves. There are several ways that can be used to define the elliptic curve equation that depends on the infinite field used, one of which is the infinite field prima (F_P where $p > 3$). Elliptic curve cryptography can be used for multiple protocol purposes, digital signatures, and encryption schemes.The purpose of this study is to determine the process of hiding encrypted messages using the *Noiseless Steganography* method as well as the generation of private keys and public keys and the process of verifying the validity of *the Elliptic Curves Cryptography Digital Signature Algorithm* (ECDSA). The result of this thesis is that a line graph is obtained that stores or hides a message using *the steganography* method and a message authenticity from the process of key generation and verification of validity using the ECDSA method. By selecting three samples consisting of one test sample and two differentiating samples, a line graph, an MD5 hash value, and a value at the point are obtained $M(r, s)$ different. Successively obtained values $M(r, s)$ to message "Matematika 2018", "MATEMATIKA 2018", and "2018 matematika" are $M(94,67)$, $M(15,17)$, and $M(9,16)$. The discussion in this thesis only covers the elliptic curves on prime finite field. So for the next thesis, the next researcher can do a discussion about the elliptic curve on the finite field (F_{2^m}) or the application of elliptic curve cryptography and other steganographic methods.

المستخلص البحث

أندريان، محمد فيبري. 2022 .**تطبيق إخفاء المعلومات بدون ضجيج وترميز المنحنيات الإهليلجية طرق خوارزمية التوقيع الرقمي**. البث الجامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الدولة الإسلامية جامعة مالانغ. المشرف : (I) جوهاري, الماجستير. (II) احمد نصيح الدين, الماجستير

الكلمات المفتاحية : التشفير, إخفاء المعلومات, الخوارزمية, المنحنى (*Kurva Eliptik*), التوقيع الرقمي

يتضمن تشفير المنحنى الإهليلجي أنظمة تشفير رئيسية متماثلة تستند إلى أمنها على المشكلات الرياضية للمنحنيات الإهليلجية. هناك عدة طرق يمكن استخدامها لتحديد معادلة المنحنى الإهليلجي التي تعتمد على الحقل اللانهائي المستخدم ، أحدها هو حقل اللانهاية الرئيسي (F_P أين $p > 3$). يمكن استخدام تشفير المنحنى الإهليلجي لأغراض بروتوكول متعددة وتوقيعات رقمية وأنظمة تشفير. الغرض من هذه الدراسة هو تحديد عملية إخفاء الرسائل المشفرة باستخدام طريقة *إخفاء المعلومات بدون ضوضاء* وكذلك توليد المفاتيح الخاصة والمفاتيح العامة وعملية التحقق من صحة *خوارزمية التوقيع الرقمي لتشفير المنحنيات الإهليلجية* .(ECDSA) نتيجة هذه الأطروحة هي أنه يتم الحصول على رسم بياني خطي يخزن أو يخفي رسالة باستخدام طريقة *إخفاء المعلومات* وأصالة الرسالة من عملية توليد المفاتيح والتحقق من صحتها باستخدام الطريقة .ECDSA من خلال اختيار ثلاث عينات تتكون من عينة اختبار واحدة وعينتين مختلفتين تم الحصول عليهما على رسم بياني خطي ، فإن القيمة *hash* MD5 ، والقيمة عند النقطة $M(r,s)$ مختلف. القيم التي تم الحصول عليها على التوالي$M(r,s)$ إلى الرسالة ,"Matematika 2018" ,"MATEMATIKA 2018"و "matematika 2018" كن ,$M(15,17), M(94,67)$ و .$M(9,16)$ تغطي المناقشة في هذه الأطروحة فقط المنحنيات الإهليلجية على التضاريس المهيأة. لذلك بالنسبة للأطروحة التالية ، يمكنك إجراء مناقشة حول المنحنى الإهليلجي على التضاريس اللانهائية (F_{2^m}) أو تطبيق تشفير المنحنيات الإهليلجية وغيرها من طرق إخفاء المعلومات

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era sekarang bentuk komunikasi ini telah melalui beberapa tahap perkembangan. Hal ini terlihat jelas dari cara masyarakat menggunakan berbagai perangkat digital sebagai alat komunikasi. Berkat perangkat komunikasi digital, orang dapat berkomunikasi dari jarak jauh melalui suara, teks, gambar, dan video. Berbagai jenis pesan yang dikirim hanya untuk pihak tertentu bersifat rahasia. Rahasia adalah hal tersembunyi yang terjadi di antara kita dan orang lain maka sudah seharusnya informasi hanya boleh disampaikan kepada orang yang berhak menerima saja, seperti halnya Hadist yang di riwayatkan Abi Hurairah, bahwa Nabi Muhammad Rasullullah Saw bersabda yang Artinya :

"Adapun tandanya orang munafik yaitu ada tiga: ketika menceritakan maka berdusta dan ketika berjanji tidak menepati dan ketika dipercaya maka berkhianat." (H.R. Imam Bukhāri dan Muslim dari Riwayat Abī Huraīrah)(Al-Hasyīmī, n.d., hal. 3).

Salah satu perintah Allah dalam Surah An-Nisa ayat 58 yaitu menyampaikan amanat kepada pihak yang berhak menerima amanat tersebut. Oleh karena itu dalam mengirimkan sebuah pesan atau informasi perlu diperhatikan keautentikan nya atau keaslian agar pesan yang ingin disampaikan diterima kepada orang yang tepat sehingga dibutuhkan suatu algoritma untuk menjaga keaslian pesan atau informasi, yaitu *Elliptic Curves Cryptography Digital Signature Algorithm*.

Suatu nilai kriptografis yang bergantung pada isi pesan dan pengirim pesan disebut tanda tangan digital atau *digital signature*. *Digital signature* menghasilkan tanda tangan yang berbeda pada setiap dokumen. Hal ini *digital signature* diambil

dari dokumen itu sendiri. Pada dasarnya penggunaan *digital signature* fungsinya sama seperti tanda tangan pada dokumen cetak yaitu sebagai proses untuk otentikasi. Dalam penggunaan *digital signature* menggabungkan dua algoritma kriptografi sekaligus yaitu yang pertama algoritma fungsi *hash* satu arah yang akan menghasilkan *message digest* dan algoritma yang kedua adalah algoritma kunci publik yang digunakan untuk mengenkripsi *message digest* tersebut.

Fungsi *hash* adalah fungsi yang yang menerima *input string* yang panjangnya sembarang lalu memampatkan menjadi pesan ringkas (*message digest*) berukuran tetap (*fixed*). Salah satu fungsi *Hash* satu arah yang digunakan adalah MD5 (*message digest* 5) yang merupakan perbaikan dari MD4. Secara garis besar pembuatan MD5 mempunyai empat langkah yaitu penambahan bit-bit pengganjal, penambahan nilai panjang pesan semula, inisialisasi *buffer* MD, dan pengolahan pesan.

Algoritma kunci publik dalam penerapannya menggunakan sepasang kunci yaitu kunci publik yang dapat disebarkan dan kunci pribadi yang diketahui oleh pemiliknya saja. Kriptografi kurva eliptik atau Elliptic Curve Cryptography (ECC) merupakan kriptografi yang beroperasi pada domain kurva eliptik. Dalam proses pengerjaan algoritma kriptografi kurva eliptik membutuhkan konsep matematika yaitu Aljabar abstrak meliputi teori grup, cincin (*ring)*, dan Medan (*Field)*. Selain konsep aljabar abstrak terdapat teori bilangan terutama pada konsep modular aritmatika. Pada penerapan kriptografi kurva eliptik Salah satunya yaitu itu algoritma tanda tangan digital kurva eliptik atau *elliptic Curve digital Signature algorithm* yang didasarkan pada algoritma *ElGamal Signature*. Hasil dari algoritma ini berupa keaslian sebuah pesan M.

Metode untuk menjaga kerahasiaan sebuah pesan tidak hanya dengan menggunakan kriptografi. Teknik lain yang dapat digunakan selain kriptografi yaitu steganografi. Steganografi dapat dipandang sebagai pelengkap kriptografi karena keduanya saling melengkapi. Keamanan sebuah pesan dapat ditingkatkan dengan menggabungkan kriptografi dan steganografi. Pada umumnya teknik yang digunakan yaitu dengan mengenkripsi pesan terlebih dahulu dengan algoritma kriptografi, selanjutnya pesan yang sudah terenkripsi disembunyikan di dalam media lain (suara, teks, video, dan gambar) dengan metode steganografi. Jika penyembunyian pesan pada steganografi konvensional dapat menurunkan kualitas *cover,* maka penyembunyian pesan pada metode *Noiseless Steganography* atau *NoStega* tidak menimbulkan kerusakan.

Penelitian mengenai kriptografi kurva eliptik sudah banyak dibahas, salah satunya yang telah dilakukan pada penelitian yang dilakukan oleh Annisa Hardiningsih HR (2021), pembuatan dan verifikasi tanda tangan digital menggunakan fungsi *hash* MD5 dan kriptografi algoritma RSA pada suatu dokumen. Hasilnya menunjukan bahwa setiap dokumen elektronik menghasilkan tanda tangan yang berbeda-beda, walaupun ditandangani oleh orang yang sama serta dokumen elektronik yang tidak mengalami perubahan pada isinya menghasilkan nilai dekripsi tanda tangan digital dan message digest modulo n bernilai sama (Hardiningsih, 2021).

Pada penelitian Febrina Mediawati Setyobudi (2013), skripsi penelitian tersebut membahas tentang kriptografi kurva eliptik dan diberikan contoh sederhana tentang penggunaan kriptografi kurva eliptik pada proses penyandian ElGamal agar lebih mudah dipahami (Setyobudi, 2013). Dalam skripsi penelitian

tersebut hanya membahas penerapan kriptografi kurva eliptik pada proses penyandian ElGamal saja dan terbatas pada medan berhingga F_p. pada penelitiannya Andy Triwinarko (2005), membahas tentang tingkat keamanan dan performansi dari algoritma kriptografi *Elliptic Curves Cryptography Digital Signature Algorithm* (ECDSA) maupun algoritma Rivest-Shamir-Adleman (RSA) (Triwinarko, 2005).

Berdasarkan pada penelitian sebelumnya, maka penulis ingin mempelajari mengenai kriptografi kurva eliptik algoritma tanda tangan digital dan memberikan contoh sederhana agar mudah dipahami. Pada penelitian ini akan dilakukan kombinasi kriptografi dan metode steganografi tanpa membutuhkan *cover* untuk menyembunyikan pesan. Metode steganografi yang digunakan adalah *Noiseless Steganography (NoStega)* dan metode kriptografi yang digunakan yaitu *Elliptic Curves Cryptography Digital Signature Algorithm (ECDSA).* Sehingga penulis mengambil judul *"*Penerapan Metode *Noiseless Steganography* dan *Elliptic Curves Cryptography Digital Signature Algorithm* Pada Pengamanan Pesan Teks*"* sebagai penelitian untuk tugas akhir.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, maka rumusan masalah yang diambil dalam penelitian ini adalah :

1. Bagaimana proses penyembunyian pesan terenkripsi dengan menggunakan metode steganografi?
2. Bagaimana proses pembangkitan kunci privat dan kunci publik pada *Elliptic Curves Cryptography Digital Signature Algorithm*?

3. Bagaimana proses verifikasi keabsahan *Elliptic Curves Cryptography Digital Signature Algorithm*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan di atas, maka tujuan penyusunan skripsi ini adalah :

1. Mengetahui proses penyembunyian pesan terenkripsi dengan menggunakan metode steganografi.
2. Mengetahui proses pembangkitan kunci privat dan kunci publik pada *Elliptic Curves Cryptography Digital Signature Algorithm*.
3. Mengetahui proses verifikasi keabsahan *Elliptic Curves Cryptography Digital Signature Algorithm*.

1.4 Manfaat Penelitian

Hasil penulisan ini di harapkan mampu memberikan manfaat pada pembaca umumnya dan penulis khususnya, selain itu diharapkan:

1. Sebagai bahan belajar dan penelitian tentang keamanan data dalam bentuk pesan teks.
2. Sebagai bahan referensi dalam pengembangan penelitian lebih lanjut tentang kriptografi, khususnya kriptografi kurva eliptik.
3. Sebagai sarana pengembangan keilmuan dibidang matematika aljabar mengenai kriptografi.

1.5 Batasan Masalah

Untuk memfokuskan pembahasan, maka pada skripsi ini hanya membahas penggunaan metode steganografi dan *Elliptic Curves Cryptography Digital Signature Algorithm* pada pengamanan pesan teks. Persamaan kurva eliptik yang

digunakan dibatasi pada medan berhingga *(finite field)* atau *Galois Field* prima F_p atau $GF(p)$. Dalam proses penyandian, penulis menggunakan 97 karakter yang terdiri dari 10 karakter berupa angka ‘0’ sampai ‘9’, 52 karakter berupa huruf alfabet ‘A’ sampai ‘Z’ maupun ‘a’ sampai ‘z’, dan 35 karakter simbol. Pada proses penggunaan metode steganografi penulis menggunakan metode *GraphStega* atau *Graph Steganography* untuk menyembunyikan sebuah pesan $M(r,s)$ yang telah direpresentasikan ke dalam biner menggunakan kode ASCII 8-bit.

1.6 Definisi Istilah

Definisi istilah yang dipakai dalam penelitian ini, secara garis besar dapat ditulis sebagai berikut:

1. Algoritma yang diartikan sebagai alur pemikiran untuk pemecahan masalah yang terdiri atas sejumlah langkah matematis Pada dasarnya, algoritma merupakan deskripsi proses untuk mengerjakan sesuatu yang disusun dalam sederet aksi. Secara sederhana, prinsip kerja algoritma terbagi menjadi, masukan (*input*), proses, dan keluaran (*output*).
2. Modulo yang diartikan sebagai sebuah operasi yang menghasilkan sisa pembagian dari suatu bilangan terhadap bilangan lainnya. Dalam bahasa pemrograman operasi ini umumnya dilambangkan dengan simbol %, mod atau modulo, tergantung bahasa pemrograman yang digunakan.
3. *Chiper* yang diartikan sebagai sebuah algoritma kriptografi (*Cryptography Algorithm*), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.

4. *Enchipering* yang diartikan sebagai proses menyandikan *plainteks* menjadi *chiperteks*.
5. *Dechipering* yang diartikan sebagai proses mengembalikan *chiperteks* menjadi *plainteks* semula.
6. *Plainteks* yang diartikan Pesan atau informasi yang dapat dibaca atau pesan asli.
7. *Chiperteks* yang diartikan Pesan yang tidak dapat dibaca atau pesan yang telah di enkripsi
8. *Cryptosystem* yang diartikan sebagai rangkaian algoritma kriptografi yang diperlukan untuk mengimplementasikan layanan keamanan tertentu. Biasanya, sebuah kriptosistem terdiri dari tiga algoritma: satu untuk pembangkitan kunci, satu untuk enkripsi, dan satu untuk dekripsi.
9. Verifikasi yang diartikan suatu konfirmasi yang dilakukan dengan menyediakan dengan bukti yang objektif yang menunjukkan bahwa persyaratan telah dipenuhi.
10. *String* yang diartikan sebagai bentuk data yang biasa dipakai dalam bahasa pemrograman untuk keperluan menampung dan memanipulasi data teks, misalnya untuk menampung (menyimpan) suatu kalimat.
11. *Biner* yang diartikan sebagai bilangan yang berbasis 2 yang hanya mempunyai 2 digit yaitu 0 dan 1. 0 dan 1 disebut sebagai bilangan *binary digit* atau bit.
12. *Checksum* yang diartikan sebagai blok data berukuran kecil yang berasal dari blok data digital lain untuk tujuan mendeteksi kesalahan yang mungkin telah terjadi selama transmisi atau penyimpanannya.

BAB II
KAJIAN TEORI

2.1 Teori Pedukung

2.1.1 Aritmatika Modulo

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a \bmod m$ memberikan sisa apabila a dibagi dengan m. Bilangan m disebut modulus atau modulo, dan hasil operasi modulo m terletak pada himpunan $\{0, 1, 2, 3, \dots, m-1\}$ (Munir, 2019, hal. 63).

2.1.1.1 Kekongruenan

Definisi 2.1.1.2.2

Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka $a \equiv b \ (mod\ m)$ jika $m|(a-b)$. Jika a tidak kongruen dengan b dalam modulo m. Maka dapat ditulis $a \not\equiv b \ (mod\ m)$ (Munir, 2019, hal. 64).

Teorema 2.1.1.2.1

Andaikan a, b dan c adalah bilangan bulat dan m bilangan asli, maka:

1. Refleksi, $a \equiv a \ (mod\ m)$
2. Simetris, Jika $a \equiv b \ (mod\ m)$, maka:

   $b \equiv a \ (mod\ m)$ dan $a - b \equiv 0 \ (mod\ m)$ adalah pernyataan yang ekivalen.
3. Transitif, Jika $a \equiv b \ (mod\ m)$ dan $b \equiv c \ (mod\ m)$, maka $a \equiv c \ (mod\ m)$

Bukti:

1. Jika $m \neq 0$ maka $m|0$ yang dapat dituliskan sebagai $m|a-a$.

   maka, $a \equiv a \ (mod\ m)$, karena $a - a = 0$ dan $m|0$.

2. $a \equiv b \ (mod\ m)$ berarti $m|a-b$, menurut definisi 1 ada keterbagian bilangan bulat t sehingga:

   $m|a-b$ dapat dinyatakan $a-b=tm$

   $$\leftrightarrow -(a-b) = -tm$$

   $$\leftrightarrow b-a = (-t)m$$

   Menurut definisi, maka $b \equiv a \ (mod\ m)$.

3. Menurut definisi 1 pada keterbagian ada bilangan bulat t_1 dan t_2 sehingga:

   $m|a=b$ dapat dinyatakan $a-b=t_1 m\ , \forall\ t_1$

   $m|b-c$ dapat dinyatakan $b-c=t_2 m\ , \forall\ t_2$

   $$a-c=(t_1+t_2)m$$

   Ini berarti, menurut definisi menjadi $a \equiv c\ mod(m)$

Teorema 2.1.1.2.2

Jika $a \equiv b \ (mod\ m)$, maka $a+c \equiv b+c \ (mod\ m)$

Bukti

$a \equiv b \ (mod\ m)$ berarti $m|a-b$ (menurut definisi)

menurut definisi pada keterbagian ada bilangan bulat t sehingga:

$m|a-b$ dapat dinyatakan $a-b=tm$

$$\leftrightarrow (a-b)+0 = tm$$

$$\leftrightarrow (a-b)+(c-c) = tm$$

$$\leftrightarrow (a+c)-(b+c) = tm$$

Sesuai definisi maka diperoleh $a+c \equiv b+c \ (mod\ m)$

Teorema 2.1.1.2.3

Jika $a \equiv b \ (mod\ m)$, maka $ac \equiv bc \ (mod\ m)$

Bukti

$a \equiv b\ (mod\ m)$ berarti $m|a - b$ (menurut definisi)

Menurut definisi pada keterbagian ada bilangan bulat t sehingga:

$$M|a - b \text{ dapat dinyatakan } a - b = tm$$

$$\leftrightarrow (a - b)c = (tm)c$$

$$\leftrightarrow ac - bc = (tc)m$$

Sesuai definisi maka diperoleh $ac \equiv bc\ (mod\ m)$

2.1.1.2 Balikan Modulo (*Modulo Invers*)

Balikan (invers) perkalian di dalam bilangan riil dapat ditunjukkan sebagai balikan dari a adalah $1/a$ sedemikian sehingga $a \times \frac{1}{a} = 1$. Bilangan bulat a memiliki balikan dalam modulus m hanya jika a dan m relatif prima dan $m > 1$. Balikan dari $a\ (mod\ m)$ adalah sebuah bilangan bulat a^{-1} sedemikan sehingga

$$\mathrm{a} \times \mathrm{a}^{-1} \equiv 1\ (\mathrm{mod\ m}) \qquad (2.1)$$

Jadi, dapat ditulis $a^{-1}(mod\ m)$ balikan dari $a(mod\ m)$.

2.1.1.3 Kongruensi Linier

Kongruensi mempunyai sifat yang sama dengan persamaan dalam aljabar. Dalam Kongruensi linier akan ditentukan bilangan bulat x sehingga memenuhi kongruensi $f(x) \equiv 0\ (mod\ m)$, dimana $f(x)$ adalah polynomial dengan koefisien bilangan bulat.

Definisi 2.1.1.2.3

Misalkan $s_1, s_2, s_3, \dots, s_m$ adalah suatu sistem residu lengkap modulo m. Banyaknya selesaian dari $f(x) \equiv 0(mod\ m)$ adalah banyaknya s_i yang memenuhi $f(s_i) \equiv 0(mod\ m)$ (Irawan et al., 2014, hal. 81).

Contoh:

Tentukan x yang memenuhi kongruensi $f(x) = x^3 + 5x - 4 \equiv 0(mod\ 7)$

Untuk mendapatkan selesaian tersebut dengan subsitusi x dari 1,2,3, ... 6 (residu lengkap dari modulo 7)

$x = 0$ maka $f(0) = 0 + 0 - 4 = -4 \not\equiv 0\ (mod\ 7)$, jadi 0 bukan selesaian

$x = 1$ maka $f(1) = 1 + 5 - 4 = 2 \not\equiv 0\ (mod\ 7)$, jadi 1 bukan selesaian

$x = 2$ maka $f(2) = 8 + 10 - 4 = 14 \equiv 0\ (mod\ 7)$, jadi 2 adalah selesaian

$x = 3$ maka $f(3) = 27 + 15 - 4 = 38 \not\equiv 0\ (mod\ 7)$, jadi 3 bukan selesaian

$x = 4$ maka $f(4) = 64 + 20 - 4 = 80 \not\equiv 0\ (mod\ 7)$, jadi 4 bukan selesaian

$x = 5$ maka $f(5) = 125 + 25 - 4 = 146 \not\equiv 0\ (mod\ 7)$, jadi 5 bukan selesaian

Jadi selesaiannya hanya $x \equiv 2\ (mod\ 7)$.

2.1.2 Grup

Grup $(G,*)$ terdiri dari himpunan G bersama-sama dengan operasi biner $*$ pada G, yang memenuhi empat aksioma berikut:

1. Tertutup

   operasi biner $*$ menghasilkan nilai di dalam G, yaitu untuk semua a dan b di dalam G, $a * b$ juga berada di dalam G.

2. Asosiatif

   untuk semua $a, b,$ dan c di dalam $G, (a * b) * c = a * (b * c)$.

3. Elemen identitas

   terdapat elemen identitas e sedemikian sehingga untuk semua a di dalam G, maka berlaku $e * a = a * e = a$.

4. Invers

   untuk semua a di dalam G, terdapat elemen $a' \in G$ sedemikian sehingga $a * a' = a' * a = e$, yang dalam hal ini a adalah elemen identitas.

Suatu grup disebut grup abelian atau grup komutatif jika $\forall a, b \in G, a * b = b * a$, maka $(G,*)$ bersifat komutatif. Suatu grup dengan jumlah elemen berhingga disebut grup hingga (*finite group*) dan orde dari grup ini adalah jumlah elemen dalam grup tersebut.

2.1.3 *Ring* (Gelanggang)

Ring $(R,+,\times)$ terdiri dari himpunan R dengan dua operasi biner $+$ dan $\times$ sedemikian sehingga memenuhi aksioma sebagai berikut:

1. $(R,+)$ adalah grup abelian dengan elemen identitas adalah 0.
2. Operasi perkalian bersifat asosiatif, yaitu $a \times (b \times c) = (a \times b) \times c$ untuk semua $a, b, c \in R$.
3. Terdapat elemen identitas perkalian yang dinyatakan dengan 1, dimana $1 \neq 0$, sedemikian sehingga $1 \times a = a \times 1 = a, \forall\, a \in R$.
4. Operasi $\times$ bersifat distributif terhadap penjumlahan, yaitu:

   $a \times (b + c) = (a \times b) + (a \times c)$ dan $(b + c) \times a = (b \times a) + (c \times a), \forall\, a, b, c \in R$.

Sebuah *ring* dikatakan ring komutatif jika berlaku $a \times b = b \times a, \forall\, a, b \in R$.

2.1.4 Medan F_p

Medan F adalah sebuah ring komutatif dimana setiap elemen tak-nol mempunyai balikan perkalian. Balikan perkalian adalah untuk setiap $a \neq 0$ yang

termasuk di dalam F, terdapat elemen $a^{-1} \in F$ sedemikian sehingga $a \times a^{-1} = 1$ (Munir, 2019, hal. 84).

2.1.5 Medan Berhingga F_p

Untuk p bilangan prima, maka F_p adalah medan berhingga berorde p dengan anggotanya adalah $Z_P = \{0, 1, 2, p-1\}$, yang dalam hal ini operasi penjumlahan dan perkalian dapat dilakukan dalam modulus p, yang didefinisikan sebagai berikut:

1. Penjumlahan

   jika $a, b \in F_p$, maka $a + b = r$, yang dalam hal ini $r = (a + b) mod\ p$.

2. Perkalian

   jika $a, b\ \in F_p$, maka $a \times b = s$, yang dalam hal ini $s = (a \times b) mod\ p$.

Semua operasi penjumlahan dan perkalian di dalam F_p selalu menghasilkan nilai di dalam himpunan $\{0, 1, 2, p-1\}$.

2.1.6 Tinjauan Umum Kriptografi

Kemajuan teknologi memang sangat penting bagi kehidupan manusia saat ini. Karena teknologi adalah salah satu dukungan terhadap kemajuan manusia. Di banyak bagian masyarakat, teknologi telah membantu meningkatkan ekonomi, makanan, komputer, dan banyak lagi. Bagi pengguna internet yang sangat luas yang sebagian besar berisi informasi atau pesan rahasia, jadi keamanan harus menjadi faktor nomor satu yang perlu dipertimbangkan. Hal tersembunyi yang terjadi di antara kita dan orang lain maka sangat dianjurkan untuk menjaganya dapat disebut rahasia seperti halnya Hadist yang diriwayatkan oleh At-Turmudzi dari Jabir bin Abdullah, yang Artinya:

"Jika seseorang menceritakan suatu peristiwa kemudian ia berpaling, maka cerita itu menjadi amanah." (HR. At-Turmudzi dari Jabir bin Abdullah).

Adanya kriptografi maka masalah keamanan tersebut dapat diatasi. Kriptografi adalah ilmu untuk menjaga rahasia suatu pesan dengan cara mengubah ke dalam bentuk yang tidak dipahami lagi maknanya. Berikut ini dengan jelas menunjukkan kriptografi, sejarahnya dan berbagai jenisnya.

Kriptografi berasal dari bahasa Yunani "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphien*" artinya "*writing*" tulisan. Jadi, kritografi secara harfiah adalah tulisan rahasia (Munir, 2019). Menurut *Schneir* (1996), kriptografi adalah ilmu yang mempelajari tentang bagaimana pesan yang dikirim dapat dikirimkan dengan aman ke penerima. Ada banyak istilah penting atau istilah umum dalam kriptografi, yaitu pesan, *plaintext*, *ciphertext*, pengirim, penerima, enkripsi, dekripsi, *cipher*, kode, kunci, sistem kriptografi, penyadap, kriptanalisis, dan kriptologi.

Kriptografi dan kriptanalisis adalah cabang dari ilmu yang disebut kriptologi. *Cryptology* adalah ilmu kriptografi dan kriptanalisis. Keduanya saling terkait satu sama lain. Kriptografi mengacu pada 11 aplikasi teknik kriptografi yang efisien, sementara kriptologi mengacu pada subjek sebagai bidang studi.

2.1.7 Fungsi *Hash* Satu Arah

Salah satu landasan dalam kriptografi modern adalah fungsi *hash* kriptografi yang umumnya dikenal sebagai fungsi *hash* satu arah. Fungsi *hash* adalah fungsi dengan masukan *string biner* yang panjangnya sembarang dan menghasilkan *string biner* dengan panjang yang tetap. Fungsi *hash* yang paling

banyak digunakan dalam kriptografi adalah untuk integritas data dan tanda tangan digital (Hayati et al., 2017, hal. 53).

Fungsi *hash* dapat menerima *input string* apa pun. Jika *string* M mewakili sebuah pesan, setiap pesan M berukuran bebas dikompresi oleh fungsi *hash* H dapat ditulis sebagai:

$$h = H(M) \qquad (2.2)$$

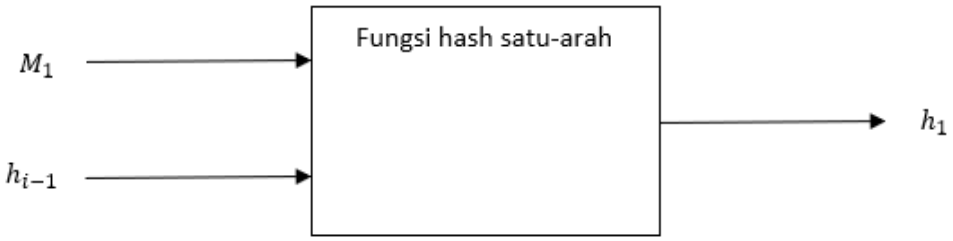
Output fungsi *hash* disebut juga nilai *hash* atau pesan ringkas (*message digest*). Pada persamaan (2.2), h adalah nilai *hash* atau *message digest* dari pesan M. Nama lain fungsi *hash* adalah fungsi kompresi atau kontraksi (*compression function*), cetak jari (*fingerprint*) *cryptographic checksum*, *Message Integrity Check* (MIC), *Manipulation Detection Code* (MDC). Fungsi utama fungsi *hash* adalah untuk memeriksa keaslian pesan dengan cara membandingkan pesan asli dengan pesan yang diduga sudah diubah (Munir, 2019).

Sifat-sifat fungsi hash satu-arah adalah sebagai berikut (Schneier, 1994):

1. Fungsi H dapat diterapkan pada blok data berukuran berapa saja.
2. H menghasilkan nilai (h) dengan panjang tetap.
3. $H(x)$ mudah dihitung untuk setiap nilai x yang di berikan.
4. Untuk setiap h yang diberikan, tidak mungkin menemukan x sedemikian sehingga $H(x) = h$. Itulah penyebab fungsi H dikatakan fungsi hash satu-arah.
5. Untuk setiap x yang diberikan, tidak mungkin mencari $y \neq x$ sedemikian sehingga $H(y) = H(x)$.
6. Secara komputasi tidak memungkinkan untuk mencari pasangan x dan y sedemikian sehingga $H(x) = H(y)$.

Fungsi *hash* bekerja secara iteratif. Masukan untuk fungsi *hash* adalah blok pesan (M) dan luaran dari *hashing* blok pesan sebelumnya (h_{i-1}), atau dapat dinyatakan sebagai

$$h_i = H(M_i, h_{i-1}) \qquad (2.3)$$



Gambar 2.1 Fungsi *Hash* satu arah

2.1.8 Algoritma *MD5*

*MD*5 adalah salah satu fungsi *hash* yang paling banyak digunakan. *MD*5 merupakan versi perbaikan dari *MD*4 yang dirancang oleh Ron Rivest pada tahun 1991. *MD*5 merupakan pengembangan dari *MD*4 dimana ada penambahan satu putaran. *MD*5 umumnya digunakan sebagai *checksum* untuk memverifikasi *file* yang diunduh dari internet.

*MD*5 memproses teks masukan ke dalam blok menjadi 512 bit, kemudian dibagi menjadi 16 buah sub blok sebesar 32 bit. *Output* dari algoritma *MD*5 adalah sebuah set dari 4 buah blok masing-masing 32 bit, yang kemudian menghasilkan nilai *hash* 128 bit (Dhany et al., 2018, hal. 281).

Secara garis besar *message digest* diperoleh dengan cara sebagai berikut: (Munir, 2019)

1. Penambahan bit-bit pengganjal (*padding bits*).
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi penyangga (*buffer*) MD.

4. Pengolahan pesan dalam blok berukuran 512 bit.

2.1.9 Tanda-tangan Digital

Salah satu bentuk kriptografi modern adalah tanda tangan digital (*digital signature*). Tanda tangan digital bukanlah tanda tangan yang dipindai dengan pemindai (dinamakan sebagai *digitized signature*) atau dibuat dengan pena elektronik. Tanda tangan digital adalah nilai kriptografi yang bergantung pada isi pesan dan pengirim pesan. Ini berarti bahwa tanda tangan digital untuk pesan yang berbeda akan memiliki tanda tangan yang berbeda, bahkan dari pengirim yang sama.

Tanda Tangan Digital pertama kali dijelaskan oleh Whitfield Diffie dan Matin Hellman pada tahun 1976. Dan dilanjutkan Ronald Shamir dan Adleman (penemu RSA), mengklaim bahwa algoritma tersebut dapat diimplementasikan pada skema tanda tangan digital.

Untuk memastikan data valid, pengirim harus terlebih dahulu menandatangani dokumen yang akan dikirim. Penerima kemudian dapat memverifikasi bahwa dokumen tersebut asli dengan memverifikasi tanda tangan dokumen tersebut. Tanda tangan digital yang menggunakan algoritma *hashing* untuk membentuk kombinasi karakter unik yang disebut *message digest*. Dengan cara ini, pengirim bertanggung jawab atas isi dokumen dan penerima dapat memverivikasi keaslian dokumen (Cahyo Prabowo & Afrianto, 2017).

Dalam hal keamanan kriptografi, fungsi utama dari tanda tangan digital adalah *non-repudiation* atau anti penyangkalan, jika dokumen tersebut valid, pengirim tidak dapat menyangkal bahwa pengirim telah mengkonfirmasi keberadaan dokumen tersebut.

Jika pada saat mengirim data, terdapat pesan yang diubah oleh penyadap adalah satu karakter, jika isi pesan diubah dengan menghapus atau menambahkannya, *Message digest* penerima mungkin berbeda dari informasi yang diterima pengirim dalam hal ini. terkirim . Karena *Message digest* tidak didekodekan lagi, itu disebut *one-way hash*.

Penendatangan pesan dapat dilakuakan dengan salah satu dari dua cara berikut: (Munir, 2019)

1. Enkripsi pesan

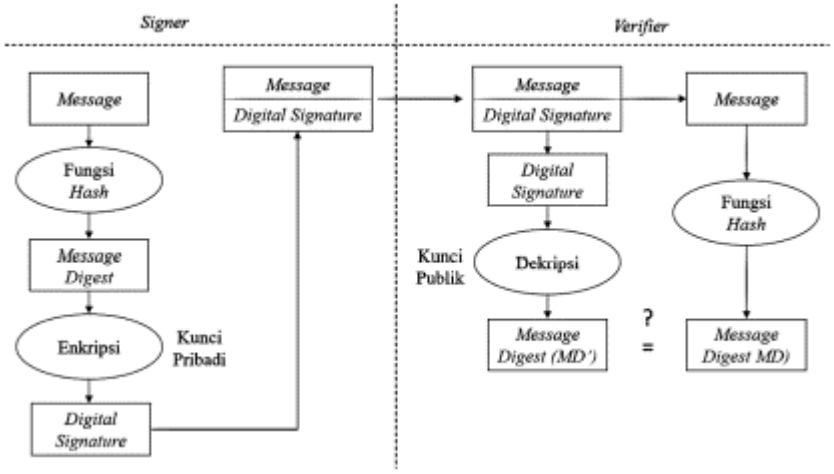
   Penandatangan pesan dapat dilakukan dengan mengenkripsi pesan. Enkripsi pesan dapat menggunakan kriptografi kunci simetri atau kriptografi kunci publik.

2. Tanda tangan digital dengan fungsi *hash* dan algotritma kriptografi kunci publik.

   Tanda tangan digital dilakukan dengan proses *hashing* dan enkripsi kriptografi kunci publik terhadap isi pesan. Proses *hashing* menghasilkan *message digest*. Selanjutnya *message digest* dienkripsikan menggunakan kriptografi kunci publik dengan syarat algoritma kunci publik yang digunakan memenuhi sifat $D_d\big(Ee\ (M)\big) = M$ dan $D_e(E_d(M)) = M$, dengan e merupakan kunci publik dan d kunci pribadi.

Mengenkripsi *message digest* dengan kriptografi kunci publik menghasilkan tanda tangan digital. Pesan (tidak dienkripsi) dikirim dengan tanda tangan digital. Penerima pesan memverifikasi tanda tangan digital dan membandingkannya dengan *message digest* dari pesan. Berikut ini adalah skema

tanda tangan digital menggunakan kombinasi fungsi *hash* dan kriptografi kunci publik.



Gambar 2.2 Skema Tanda-tangan Digital

Berdasarkan gambar di atas, proses tanda tangan yang dilakukan oleh pengirim (*signer*) adalah sebagai berikut:

1. Pengirim pesan menggunakan fungsi hash untuk menghitung *message digest* dari pesan asli.
2. *Message digest* dienkripsi dengan kunci pribadi pengirim. Hasil enkripsi ini adalah tanda tangan digital.
3. Tanda tangan digital yang dihasilkan dilampirkan ke pesan asli dan kemudian keduanya dikirim ke penerima.

Proses verifikasi tanda tangan yang dilakukan oleh penerima (*verifier*) adalah sebagai berikut:

1. Penerima menggunakan fungsi *hash* untuk menghitung *message digest* dari pesan asli.
2. Tanda tangan digital didekripsi menggunakan kunci publik pengirim pesan untuk menghasilkan *message digest*.

3. Periksa apakah *message digest* dari pesan yang didekripsi dan pesan asli dari *message digest* memiliki nilai yang sama. Jika nilainya sama, tanda tangan yang diterima adalah asli dan isi pesan tidak berubah satu karakter.

2.1.10 Kriptografi Kurva Eliptik

Kriptografi yang menggunakan kurva eliptik yang dinamakan kriptografi kurva eliptik. Kurva eliptik adalah kurva matematik yang memiliki salah satu sifat yaitu ketertutupan, yaitu operasi penjumlahan dua buah titik di dalam kurva eliptik yang selalu menghasilkan titik yang terletak di kurva eliptik. Secara umum, persamaan kubik untuk kurva eliptik dapat dituliskan dalam bentuk:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (2.4)$$

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

$$y^2 = x^3 + ax + b \quad (2.5)$$

Persamaan tersebut adalah persamaan kubik atau berderajat 3, karena pangkat tertinggi yang termuat adalah 3. Persamaan tersebut termasuk juga dalam definisi kurva eliptik adalah elemen tunggal yang dilambangkan O dan disebut titik di tak terhingga atau titik nol (Stallings, 2017).

Untuk menggambarkan kurva, maka perlu dihitung:

$$y = \sqrt{x^3 + ax + b} \quad (2.6)$$

Untuk nilai a dan b yang diberikan, gambar plot terdiri dari nilai positif dan negatif pada y untuk setiap nilai x. Jadi, setiap kurva simetris terhadap sumbu x atau $y = 0$. Kurva eliptik dapat juga dilihat sebagai suatu himpunan yang terdiri dari titik-

titik (x, y) yang memenuhi persamaan $y^2 = x^3 + ax + b$. Himpunan tersebut dinotasikan dengan $E(a, b)$. Menggunakan nilai yang berbeda dari pasangan (a, b) menghasilkan himpunan $E(a, b)$ yang berbeda (Stallings, 2017).

Kriptografi kurva eliptik menggunakan kurva eliptik di mana semua variabel dan koefisien terbatas pada elemen bidang hingga. Terdapat dua jenis kurva eliptik yang digunakan dalam aplikasi kriptografi, yaitu kurva prima yang didefinisikan F_p dan kurva biner di atas $F(2_m)$. Di dalam penelitian ini kurva eliptik prima yang didefinisikan F_p saja yang akan digunakan.

2.1.10.1 Kurva Eliptik Pada Bidang Terbatas F_p

Bentuk umum kurva eliptik pada F_p adalah

$$y^2 = x^3 + ax + b \ (mod\ p) \qquad (2.7)$$

yang dalam hal ini p adalah bilangan prima dan elemen-elemen di dalam medan galois adalah $\{0,1\ ,2\ ,3, \dots , p-1\}$. Semua operasi penjumlahan dan perkalian dilakukan di dalam modulus p.

Operasi yang berlaku pada F_p dapat adalah sebagai berikut (Triwinarko, 2005):

1. Penjumlahan (*Addition*), jika $a, b \in F_p$, maka $a + b = r$, dimana r adalah sisa pembagian $a + b$ dengan bilangan prima $p, 0 \leq r \leq p-1$. Penjumlahan seperti ini disebut penjumlahan modulo p atau dapat ditulis dengan $(mod\ p)$.
2. Perkalian (*Multiplication*), jika $a, b \in F_p$, maka $a \cdot b = s$, dimana s adalah sisa pembagian $a \cdot b$ dengan bilangan prima p, $0 \leq s \leq p-1$. perkalian seperti ini disebut perkalian modulo p.

Untuk mendefinisikan persamaan kurva eliptik pada bidang terbatas Fp. Persamaan *Weierstrass* yang digunakan untuk kedua bidang terbatas tersebut berbeda.

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 $E(F_p)$ pada F_p merupakan himpunan titik-titik $P(x, y)$, dimana $x, y \in F_p$, yang memenuhi persamaan (*2.7*) dan sebuah titik khusus $\varphi(\infty, \infty)$ yang merupakan titik tak hingga. Operasi penjumlahan pada $E(F_p)$ didefinisikan sebagai berikut:

a. $P + \varphi = \varphi + P = P$ untuk setiap $P \in E(F_p)$, Jika $P(x, y) \in E(F_p)$, maka $(x, y) + (x, -y) = \varphi$ dan φ merupakan titik tak hingga atau titik nol. 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.

b. Penjumlahan kedua titik. 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 $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

   Bukti:

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

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

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

$$y_1^2 = x_1^3 - ax_1 - b \qquad (2.8)$$

$$y_2^2 = x_2^3 - ax_2 - b \qquad (2.9)$$

$$y_3^2 = x_3^3 - ax_3 - b \qquad (2.10)$$

Persamaan (2.10) dikurangkan dengan persamaan (2.8) kemudian kedua ruas dibagi dengan $(x_3 - x_1)$, sehingga diperoleh:

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

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

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

$$(-y_3 + y_1)\lambda = (x_3^2 + x_1x_3 + x_1^2) + a \qquad (2.11)$$

Persamaan (2.10) dikurangkan dengan persamaan (2.9) kemudian kedua ruas dibagi dengan $(x_3 - x_2)$, sehingga diperoleh:

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

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

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

$$(-y_3 + y_2)\lambda = (x_3^2 + x_2x_3 + x_2^2) + a \qquad (2.12)$$

Jika persamaan (2.11) dan dikurangkan dengan persamaan (2.12) kemudian kedua ruas dibagi dengan $(x_1 - x_2)$, sehingga diperoleh:

$$[(-y_3 + y_1) - (-y_3 + y_2)]\lambda$$

$$= [(x_3^2 + x_1x_3 + x_1^2) + a] - [(x_3^2 + x_2x_3 + x_2^2) + a]$$

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

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

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

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

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

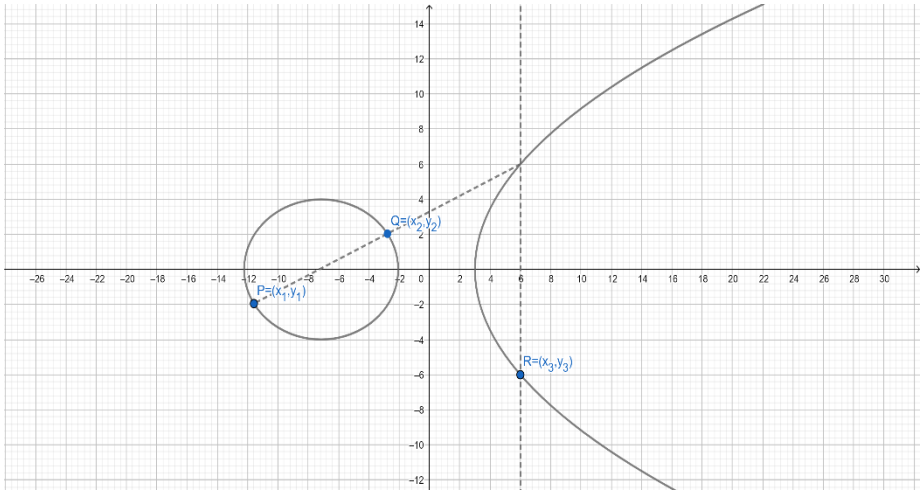
$$x_3 = \lambda^2 - x_1 - x_2 \qquad (2.13)$$

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

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

$$y_3 = \lambda(x_3 - x_1) - y_1 \qquad (2.14)$$

Aturan penjumlahan akan sangat baik jika dijelaskan secara geometri. Misalkan $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$ menjadi sebuah titik yang nyata pada kurva eliptik. Kemudian hasil penjumlahan dari P dan Q didenotasikan sebagai $R = (x_3, y_3)$, yang didefinisikan sebagai berikut. Perata 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 yaitu, bagian elips dan kurva tak hingga.



Gambar 2.3 Operasi Penjumlahan Titik Kurva Eliptik

c. Penggandaan titik (*doubling a point*). Misalkna $P = (x_1, y_1) \in E(F_p)$, 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 $\lambda = \frac{3x_{1+a}^2}{2y_1}$.

Bukti:

Misal

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1} \qquad (2.15)$$

dari ( ) diperoleh :

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

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

$$y_3 = \lambda(x_3 - x_1) - y_1 \qquad (2.16)$$

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

$$2y\frac{dy}{dx} = 3x^2 + a \leftrightarrow \frac{dy}{dx} = \frac{3x^2 + a}{2y} \leftrightarrow \lambda = \frac{3x^2 + a}{2y} \qquad (2.17)$$

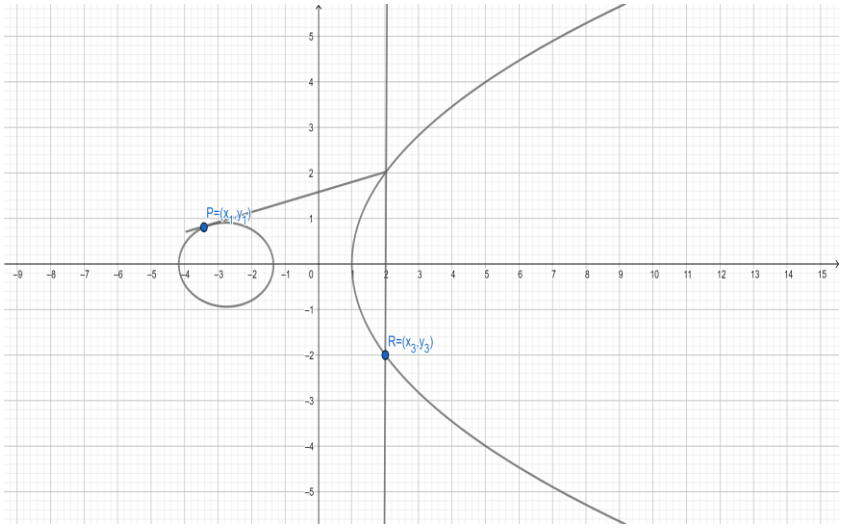
Dari persamaan (2.10) karena penjumlahan dilakukan pada titik yang sama maka $x_1 = x_2$ sehingga :

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

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

$$x_3 = \lambda^2 - 2x_1 \qquad (2.18)$$

Secara geometris, aturan penggandaan titik dapat dijabarkan yaitu, jika $P = (x_1, y_1)$, kemudian penggandaan dari P, dapat didenotasikan $R = (x_3, y_3)$ yang didefinisikan sebagai berikut. Pertama akan digambarkan 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 2.4 Operasi Penggandaan Titik Kurva Eliptik

2.1.10.2 Struktur Grup Kurva Eliptik

Akan dibuktikan bahwa kurva eliptik atas $F(p)$ atau $GF(p)$ membentuk suatu grup, yatitu sebagi berikut:

a. Akan dibuktikan bahwa kurva eliptik atas $F(p)$ atau $GF(p)$ tertutup terhadap operasi penjumlahan. Ambil sebarang titik $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$ dengan $P \neq \pm Q$, maka $P + Q = R$, merupakan garis yang memotong kurva eliptik tepat di suatu titik, misalkan titik $-R$. Pembuktian

secara perhitungan yaitu $R = (x_3, y_3)$ dengan $x_3 = (\lambda^2) - x_1 - x_2$ dan $y_3 = (\lambda)(x_1 - x_3) - y_1$ dengan $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, nilai x_3 dan y_3 dapat dihitung dengan menggunakan prinsip penjumlahan pada $G(F_p)$ dan didapatkan $R = (x_3, y_3) \in G(F_p)$. Untuk nilai $Q = -P$, maka λ tidak akan terdefinisi karena nilai $x_1 = x_2$, jadi titik R akan berada pada titik *infinity*. Untuk titik $Q = P$, titik $R = (x_3, y_3)$ didefinisikan $x_3 = (\lambda)^2 - 2x_1$ dan $y_3 = (\lambda)(x_1 - x_3) - y_1$ dengan $\lambda = \frac{3x_1^2 + a}{2y_1}$, sehingga $R = (x_3, y_3) \in G(F_p)$. Maka jelas bahwa $P + Q = R$ terpenuhi, jadi terbukti bahwa $G(F_p)$ tertutup pada operasi penjumlahan.

b. Akan dibuktikan bahwa penjumlahan titik di $GF(p)$ memenuhi sifat asosiatif yaitu sebarang $P, Q, R \in G(F_p)$ berlaku $(P + Q) + R = P + (Q + R)$.

c. Akan dibuktikan bahwa $GF(p)$ mempunyai unsur identitas. Misalkan ambil sebarang titik $P \in G(F_p)$ maka aka nada titik $-P$ yang merupakan garis vertical yang tidak memotong kurva eliptik di titik ketiga, jika titik P dan $-P$ dijumlahkan akan menyebabkan kurva eliptik meliputi titik *invinity* dengan definisi penjumlahannya $P + (-P) = \infty$.

d. Akan dibuktikan bahwa $GF(p)$ mempunyai unsur balikan (*Invers*). Dari pembuktian ke (3) dari grup diatas secara jelas terlihat bahwa elemen dari kurva eliptik mempunyai invers. Titik P mempunyai invers $-P$.

2.1.11 Algoritma Kriptografi Kurva Eliptik Tanda-tangan Digital

Elliptic Curves Digital Signature Algorithm (ECDSA) merupakan sistem kriptografi kurva eliptik yang analog dengan Algoritma ElGamal *Signature*. Algoritma tanda tangan digital kurva eliptik didasarkan pada Algoritma ElGamal Signature. ECDSA diusulkan oleh Abdalla, Bellare, dan Rogaway pada tahun 1999 (Munir, 2019).

Dalam proses ECDSA, pihak yang akan melakukan tanda tangan menyepakati parameter bilangan bulat a dan b dan bilangan prima p pada persamaan kurva eliptik, grup eliptik, dan sebuah titik basis $B(x, y)$ yang dipilih dari grub eliptik. Proses-proses yang terjadi adalah sebagai berikut :

Pembangkitan Kunci Publik dan Kunci Privat *Elliptic Curves Cryptography Digital Signature*

Pengirim membangkitkan kunci privat dan kunci publiknya sebagai berikut:

1. Pengirim memilih sebuah bilangan bulat x
2. Pengirim menghitung $P_B = x \cdot B$

Penerima membangkitkan kunci privat dan kunci publik nya sebagai berikut:

1. Pengirim memilih sebuah bilangan bulat y
2. Pengirim menghitung $P_B = y \cdot B$

Prosedur Pembangkitan Tanda-tangan *Elliptic Curves Cryptography Digital Signature*

Pengirim membangkitkan tanda tangan digital untuk pesan M dengan langkah-langkah sebagai berikut:

1. Memilih sebuah bilangan bulat acak k, yang nilainya terletak di dalam selang $[1, p-1]$.

2. Menghitung $kB = (x_1, y_1)$ dan $r = x_1 \ mod \ p$. Jika $r = 0$, maka kembali ke langkah 1.
3. Menghitung $k^{-1} \ mod \ p$
4. Menghitung nilai *hash dari M, yaitu* $e = H(M)$
5. Menghitung $s = k^{-1}(e + xr) mod \ p$. Jika $s = 0$, maka ulangi kembali ke langkah 1. Tanda tangan pengirim untuk *message* m adalah (r, s)

Prosedur Verifikasi Keabsahan Tanda-tangan *Elliptic Curves Cryptography Digital Signature*

Memverifikasi tanda tangan digital (r, s) dari pengirim sebagai berikut:

1. Memverifikasi bahwa r dan s terletak di dalam selang [1, p-1]
2. Mengambil kunci publik Pengirim, yaitu $3P_A$
3. Menghitung nilai hash dari M, yaitu $e = H(M)$
4. Menghitung $w = s^{-1} \ mod \ p$.
5. Menghitung $u_1 = ew \ mod \ p$ dan $u_2 = rw \ mod \ p$
6. Menghitung $(x_1, y_1) = u_1 \cdot B + u_2 \cdot P_A$
7. Menghitung $v = x_1 mod \ p$
8. Menerima tanda tangan jika dan hanya jika $v = r$, maka tanda-tangan sah

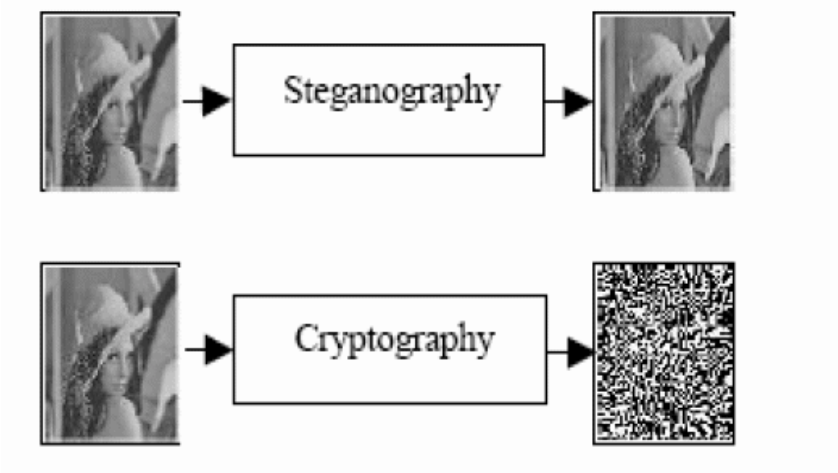
2.1.12 Steganografi

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Perbedaan Kriptografi dan Steganografi ialah jika Kriptografi untuk menyembunyikan isi (*content*) pesan dalam tujuan agar pesan tidak dapat dibaca oleh pihak ketiga. Sedangkan untuk Steganografi menyembunyikan keberadaan

(*existence*) pesan dalam tujuan untuk menghindari kecurigaan (*conspicuous*) dari pihak ketiga (lawan) (Munir, 2019).

Pada umumnya, pesan steganografi muncul dalam bentuk lain seperti gambar, artikel, daftar belanja, atau pesan lainnya. Pesan yang tertulis ini adalah teks yang mencakup semua atau menyeluruh. Teknik steganografi mencakup berbagai metode komunikasi untuk menyembunyikan pesan tersembunyi (teks atau gambar) dalam dokumen lain yang berisi teks, *image* dan bahkan audio tanpa menunjukkan perubahan nyata atau terlihat dalam struktur dan kualitas *file* asli. Metode ini termasuk tinta yang tidak tampak, *microdots*, pengaturan kata, tanda tangan digital, jalur tersembunyi, dan komunikasi spektrum luas.

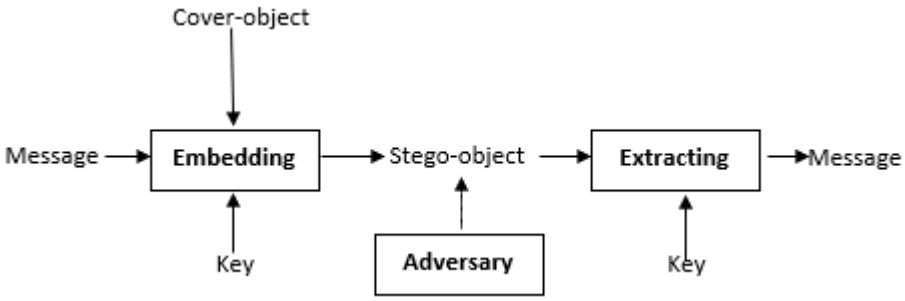
Tujuan dari steganografi adalah untuk merahasiakan atau menyembunyikan keberadaan dari sebuah pesan atau informasi yang tersembunyi. Dalam praktiknya, ini dilakukan terutama dengan membuat perubahan halus pada data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial (Aditya et al., 2010).



Gambar 2.5 Perbedaan Steganografi dengan Kriptografi

Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat

menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.



Gambar 2.6 Diagram penyisipan dan ekstrasi pesan

2.1.9.1 Noiseless Steganography

Saat ini berkembang sebuah peradigma baru steganografi yang bernama *Noiseless Steganography* atau *NoStega*. *NoStega* ditemukan oleh Desoky (2012). Jika penyembunyian pesan pada steganografi konvensional dapat menurunkan kualitas *cover*, maka penyembunyian pesan pada metode *NoStega* tidak menimbulkan kerusakan. *NoStega* melakukan kamuflase sedemikian rupa sehingga terlihat alami sehingga tidak menimbulkan kecurigaan. *NoStega* menggunakan berbagai materi untuk melakukan kamuflase seperti grafik, *email*, *game*, catatan, dan lain-lain. Ada beberapa teknik *NoStega* yang dapat digunakan, yaitu: *GraphStega*, *Chess Steganography*, *email header-based Steganography*, *education centric Steganography*, *list-based Steganography*, dan *Notes based Steganography*.

2.2 Sifat Amanah dalam Al-Quran dan Hadist

Menurut Kementerian Pendidikan dan Kebudayaan dalam Kamus Besar Bahasa Indonesia (2015), amanah adalah sesuatu yang dipercayakan (dititipkan) kepada orang lain, keamanan, ketenteraman, dan dapat dipercaya. Amanah secara

bahasa berasal dari bahasa arab أمن يأمن أمناً yang artinya aman, jujur, atau dapat dipercaya. Dengan demikian sikap amanah merupakan sesuatu yang dipercayakan untuk dijaga. Dari sinilah diambil kata amanah yang merupakan lawan dari kata khianat.

Secara istilah menurut Ibnu ‘Abbas, amanah mencakup ketaatan yang akan dibebankan kepada bumi, langit dan gunung-gunung sebelum dibebankan kepada Nabi Adam, namun bumi dan lainnya tidak mampu merimanya. Kemudian dikatakan kepada Nabi Adam: *“Sesungguhnya aku telah memberikan amanah kepada langit, bumi dan gunung akan tetapi mereka menolak, apakah kamu mau mengambilnya?”* Nabi Adam Berkata: *“ya Allah, apakah bagian di dalamnya?”* Allah berkata: *“apabila kamu melakukannya dengan baik maka akan diberikan pahala, dan apabila buruk maka akan dikenakan siksa”*. Maka Nabi Adam mengambilnya (Hakim & Susilo, 2020, hal. 124; Katsir, n.d.).

Menurut Asfahani dalam kitab *al-Mufradāt fi Gharīb al-Qur’ān* amanah merupakan ketenangan jiwa dan perasaan tak kenal takut. Di sisi lain, karena adanya unsur kebohongan maka dapat diartikan sebagai konsep ketidak percayaan manuasia terhadap sesuatu (seseorang). Misalnya, tidak berkata jujur dan menyembunyikan sesuatu (Al-Ashfahani, 2017; dalam Hakim & Susilo, 2020, hal. 123).

Dalam al-Qur’an (QS. al-Mā’idah [5]: 8), dinyatakan bahwa keadilan mendekati ketakwaan. Bahkan para mufassir seperti Abi Hayyan al-Andalusi menyatakan bahwa tahapan dalam berlaku amanah dan adil ialah, memulai dengan diri sendiri yang menjaga amanah, kemudian menyerukan kepada orang lain, setelah itu barulah menetapkan keputusan atau suatu perkara dengan adil. Meskipun

langkah-langkah ini tidak selama berjalan secara periodik, dapat pula berjalan secara komprehensif bersama-sama (Hakim & Susilo, 2020, hal. 120).

Amanah di dalam Al-Qu'ran salah satunya terdapat pada Surah An-Nisa' ayat 58, yang artinnya:

Sesungguhnya Allah menyuruh kamu menyampaikan amanah kepada pemiliknya. Apabila kamu menetapkan hukum di antara manusia, hendaklah kamu tetapkan secara adil. Sesungguhnya Allah memberi pengajaran yang paling baik kepadamu. Sesungguhnya Allah Maha Mendengar lagi Maha Melihat (QS. An-Nisā' [4]: 58).

Ayat ini memerintahkan agar menyampaikan amanat kepada yang berhak. Di dalam hadist al-Hasan dari Samurah, bahwa Rasullah bersabda, yang artinya:

"Tunaikanlah amanah kepada yang memberikan amanah dan jangan khianati orang yang berkhianat kepadamu."(HR. Ahmad dan Ahlus Sunan).

Hal itu mencakup seluruh amanah yang wajib bagi manusia, berupa hak-hak Allah terhadap para hamba-Nya, seperti shalat, zakat, puasa, kafarat, nadzar dan selain dari itu, yang kesemuannya adalah amanah yang diberikan tanpa pengawasan hamba-Nya yang lain. serta amanah yang berupa hak-hak sebagian hamba dengan hamba yang lain, seperti titipan dan selanjutnya, yang kesemuanya adalah amanah yang dilakukan tanpa pengawasan saksi. Itulah yang diperintahkan oleh Allah untuk ditunaikan. Barang siapa yang tidak melakukan di dunia ini, maka akan dimintai pertanggungjawabannya di hari kiamat (Al-Sheikh, 2003, hal. 336).

Amanah terhadap sesama manusia yaitu apabila seseorang menitipkan amanah kepada dirinya, maka dia akan menjaga serta menyampaikan amanah tersebut tanpa mengurangi hak-hak di dalamnya. Orang yang menjaga amanah adalah orang yang bertanggung jawab dan jujur terhadap amanah yang dibawanya. Ibnu Mas'ud ra. mengatakan, Nabi Muhammad Rasullullah Saw bersabda, *"Sholat adalah amanah, wudhu adalah amanah, menimbang barang adalah amanah,*

menakar adalah amanah. Segala sesuatu akan diperhitungkan. Dan yang paling berat adalah barang titipan (amanah).” (Ahmad bin Hanbal). Maksud dari hadist diatas menegaskan bahwa semua perintah Allah SWT seperti wudhu, sholat, dan lain sebagainya adalah amanah yang harus kita kerjakan sesuai dengan syarat rukunnya. Demikian pula, pekerjaan yang kita geluti sehari-hari adalah amanah yang harus kita emban dengan sebaik-baiknya. Karena itu: Bagi pedagang janganlah mengurangi timbangan atau takaran. Bagi sopir taksi janganlah memasang “argo kuda” (kecepatannya di atas normal). Bagi karyawan atau pegawai janganlah mengurangi jam kerja. Sebab, banyak karyawan yang tidak menyadari bahwa masuk kantor terlambat dan pulang cepat (sebelum waktunya) berarti korupsi waktu. Bagi orang yang bersedia menerima barang titipan, hendaklah menjaganya baik-baik. Lalu, menyampaikannya kepada yang berhak dalam keadaan sebagaimana waktu kita menerima-nya (Hamid, 2013).

2.3 Kajian Topik dengan Teori Pendukung

Penelitian ini disusun menggunakan beberapa teori pendukung, seperti kongruensi linier yang linier akan ditentukan bilangan bulat x sehingga memenuhi kongruensi $f(x) \equiv 0\ (mod\ m)$, dimana $f(x)$ adalah polynomial dengan koefisien bilangan bulat. Misalkan $s_1, s_2, s_3, \dots, s_m$ adalah suatu sistem residu lengkap modulo m. Banyaknya selesaian dari $f(x) \equiv 0(mod\ m)$ adalah banyaknya s_i yang memenuhi $f(s_i) \equiv 0(mod\ m)$ (Irawan et al., 2014). Kongruensi linier digunakan untuk menentukan semua titik di dalam kurva eliptik pada $GF(p)$ (atau F_p), sehingga titik-titik yang terdapat pada kurva eliptik jika di tambah dengan titik O di infinity, maka titik-titik pada kurva eliptik membentuk grup dengan n elemen.

Selanjutnya terdapat fungsi hash satu arah yaitu sebuah fungsi dengan masukan *string biner* yang panjangnya sembarang dan menghasilkan *string biner* dengan panjang yang tetap. Fungsi *hash* yang paling banyak digunakan dalam kriptografi adalah untuk integritas data dan tanda tangan digital (Hayati et al., 2017). Fungsi *hash* dapat menerima masukan string apa saja. Jika *string M* menyatakan pesan maka sembarang pesan M berukuran bebas dikompresi oleh fungsi *hash* H dapat ditulis sebagai:

$$h = H(M)$$

Fungsi utama fungsi *hash* adalah untuk memeriksa keaslian pesan dengan cara membandingkan pesan asli dengan pesan yang diduga sudah diubah. Selanjutnya terdapat *MD5* merupakan pengembangan dari *MD*4 dimana ada penambahan satu putaran. *MD*5 umumnya digunakan sebagai *checksum* untuk verifikasi integritas file yang didownload dari internet.

Selanjutnya terdapat tanda tangan digital yaitu suatu nilai kriptografi yang memiliki ketergantungan pada isi pesan dan pengirim pesan, maksudnya adalah tanda tangan digital dari pesan yang berbeda, walaupun dengan pengirim yang sama, akan memiliki tanda tangan yang berbeda. Fungsi utama dari tanda tangan digital pada aspek keamanan kriptografi adalah *non-repudiation* atau anti penyangkalan dimana apabila dokumen valid maka pengirim tidak bisa menyangkal bahwa keberadaan dokumen benar dikirim oleh pengirim yang bersangkutan. Selanjutnya terdapat kurva eliptik yaitu kurva matematik yang memiliki salah satu sifat yaitu ketertutupan, yaitu operasi penjumlahan dua buah titik di dalam kurva eliptik yang selalu menghasilkan titik yang terletak di kurva eliptik. Secara sederhana, bentuk umum persamaan kurva eliptik dapat ditulis sebagai berikut:

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

Selanjutnya terdapat steganografi yaitu seni dan ilmu menulis atau menyembunyikan keberadaan (*existence*) pesan dalam tujuan untuk menghindari kecurigaan (*conspicuous*) dari pihak ketiga (lawan). Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Sehingga informasi berupa teks yang dikirim oleh pengirim tidak bisa diubah keaslian teksnya dan informasi tersebut telah disembunyikan pada media lain.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan jenis penelitian kualitatif, karena dalam penelitian ini akan menganalisis pada hasil dalam bentuk data deskriptif yang diperoleh dari subjek penelitian. Metode yang digunakan dalam skripsi ini adalah metode kajian pustaka (*library research*) meliputi mengumpulkan data dan informasi dari berbagai sumber seperti buku, jurnal penelitian, skripsi, tesis, disertasi, laporan penelitian, dan karya ilmiah.

3.2 Pra Penelitian

Proses penelitian diawali dengan memahami landasan teori dan konsep dasar yang berkaitan dengan topik penelitian sebagai acuan dasar dalam penelitian ini. langkah awal yang dilakukan adalah memahami tentang definisi grup bahwasannya penjumlahan titik pada kurva eliptik membentuk sebuah grup G dengan operasi penjumlahan yang dapat ditulis $(G, +)$. Selanjutnya memahami tentang *Ring* yang merupakan sebuah *ring* komutatif, yang setiap elemen tak nol mempunyai balikan perkalian. Medan (*field*) untuk p bilangan prima dengan anggota $Zp = \{0,1,2, p-1\}$ yang akan dilakukan operasi penjumlahan dan perkalian dalam modulo p. Selanjutya terdapat fungsi *hash* satu arah digunakan untuk pengkompresi sebuah pesan menjadi *message digest*. Algoritma MD5 digunakan untuk menerima input berupa pesan berukuran sebarang dan menghasilkan MD (message digest) berukuran 128 bit. Tanda-tangan digital merupakan tanda tangan pada data digital. ECC (Elliptic Curves Cryptography) merupakan penggunaan suatu persamaan kurva eliptik yang memfokuskan pada

suatu algoritma. Selanjutnya terdapat metode Steganografi serta memilih kajian integrasi agama dengan Al-Quran atau Hadist yang dapat di integrasikan dengan topik penelitian ini.

3.3 Tahapan Penelitian

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

1. Merepresentasikan pesan M ke dalam kode ASCII 8-bit.
2. Melakukan penyembunyian pesan menggunakan metode Steganografi.
3. Menentukan persamaan kurva eliptik pada medan berhingga prima F_p.
4. Menentukan elemen-elemen grup eliptik
    a. Menghitung nilai residu kuadrat modulo p.
    b. Membandingkannya dengan nilai dari $y^2 = x^3 + ax + b(mod\ p)$.
    c. Menentukan nilai $P(x, y)$ pada kurva eliptik sebagai generator dari grup eliptik.
    d. Menentukan sebuah titik basis $B(x, y)$ yang dipilih dari grup eliptik.
5. Menentukan algoritma kurva eliptik menggunakan *Elliptic Curves Cryptography Digital Signature Algorithm*
    a. Melakukan proses pembangkitan kunci publik dan kunci privat *Elliptic Curves Cryptography Digital Signature Algorithm*.
    b. Melakukan proses pembangkitan tanda tangan *Elliptic Curves Cryptography Digital Signature Algorithm*.
    c. Melakukan proses verifikasi keabsahan tanda tangan *Elliptic Curves Cryptography Digital Signature Algorithm*.

BAB IV
PEMBAHASAN

Kriptografi kurva eliptik atau *Elliptic Curve Cryptography* (ECC) termasuk ke dalam sistem kriptografi kunci publik yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. *Elliptik Curves 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 penelitian ini akan dibahas mengenai penggunaan kriptografi kurva eliptik pada proses penyandian tanda tangan digital atau *Elliptic Curve Digital Signature Algorithm* (ECDSA) dan akan di kombinasikan dengan metode Steganografi untuk proses penyembunyian pesan.

4.1 *Penerapan Metode Steganography Pada Sebuah Pesan*

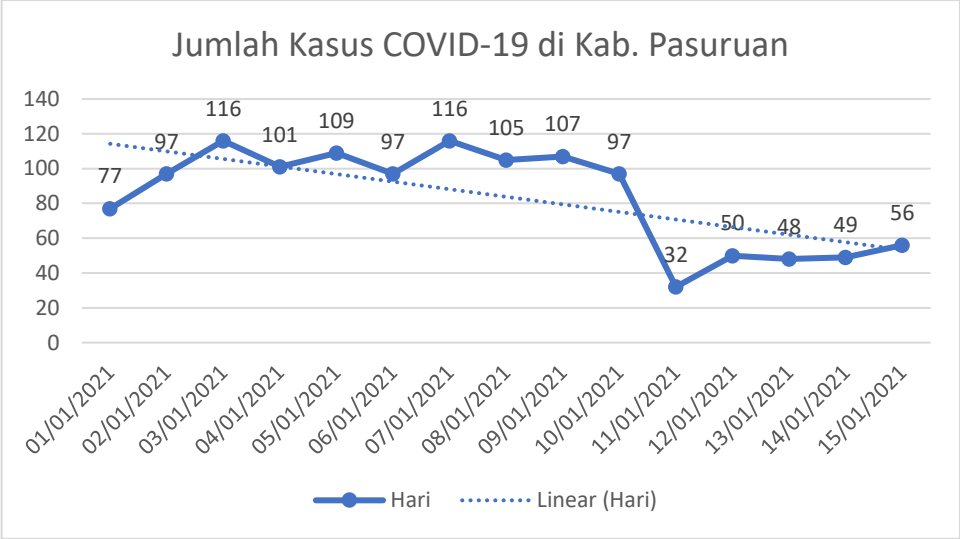
Sebelum melakukan prosedur algoritma *Elliptic Curves Cryptography Digital Signature* pengirim pesan akan menyembunyikan pesan tersebut di dalam media / *cover* metode *Noiseless Steganography*. Mula-mula akan di ubah pesan *M* = ”Matematika 2018” ke representasi biner (setiap karakter diubah ke dalam kode ASCII 8-bit) menjadi:

01001101 01100001 01110100 01100101 01101101 01100001 01110100 01101001 01101011 01100001 00100000 00110010 00110000 00110001 00111000

Selanjutnya, akan di konversi kembali kelompok-kelompok bit di atas menjadi nilai desimal

77 97 116 101 109 97 116 105 107 97 32 50 48 49 56

Kemudian akan dibuat grafik menggunakan nilai desimal diatas, misalnya nilai tersebut menyatakan jumlah kasus COVID-19 di Kab. Pasuruan.



Gambar 4.2 Grafik Garis yang Menyembunyikan Pesan “Matematika 2018”

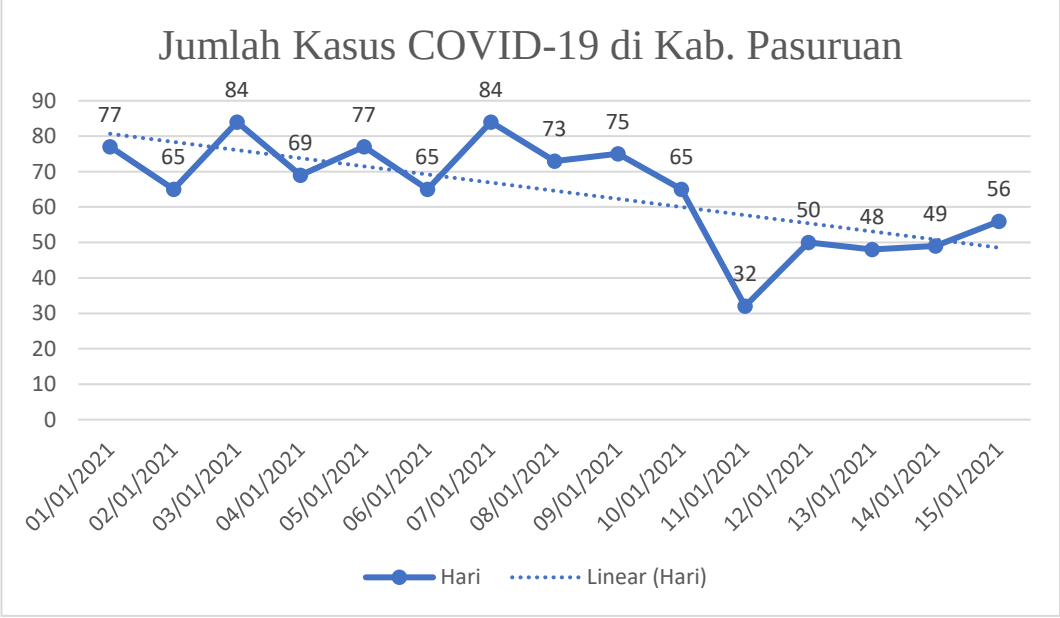
Dengan demikian pesan yang akan dikirimkan telah tersembunyi pada media berupa grafik garis seperti pada gambar 4.2. Sehingga dengan menggunakan metode steganografi tersebut tidak akan menimbulkan kecurigaan bahwasannya media tersebut menyimpan sebuah informasi pesan rahasia.

Hasil pengujian metode steganografi dari dua pesan berbeda dapat dilihat pada tabel 4.1.

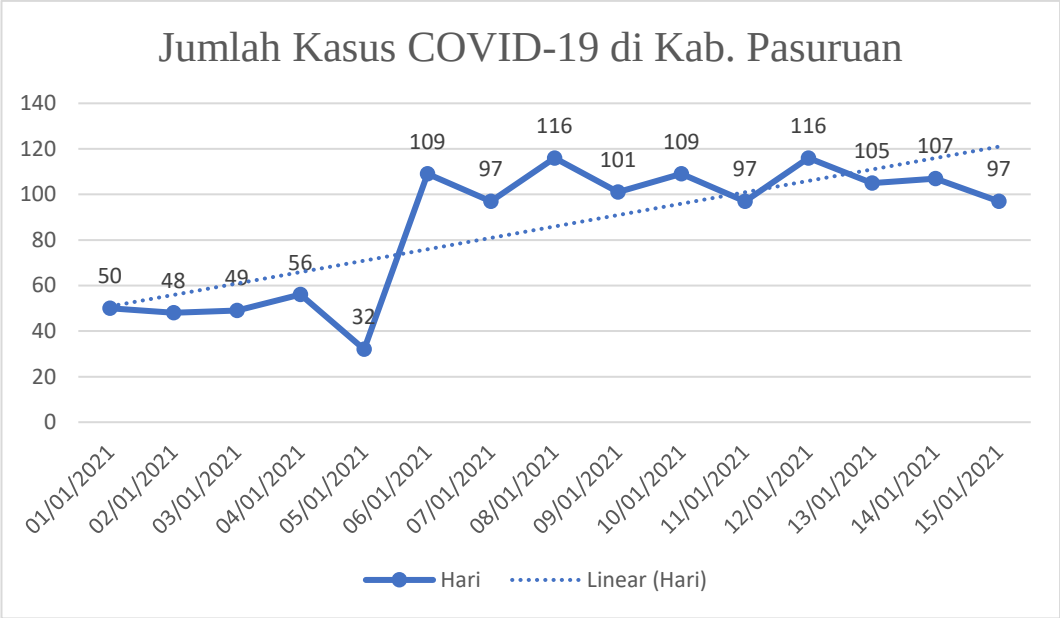
Tabel 4.1 Hasil Pengujian Metode Steganografi dari dua pesan Berbeda

No	Pesan	Biner Kode ASCII	Desimal
1	MATEMATIKA 2018	01001101 01000001 01010100 01000101 01001101 01000001 01010100 01001001 01001011 01000001 00100000 00110010 00110000 00110001 00111000	77 65 84 69 77 65 84 73 75 65 32 50 48 49 56
2	2018 matematika	00110010 00110000 00110001 00111000 00100000 01101101 01100001 01110100 01100101 01101101 01100001 01110100 01101001 01101011 01100001	50 48 49 56 32 109 97 116 101 109 97 116 105 107 97

Berikut akan dibuat grafik menggunakan nilai desimal diatas sebagai pembeda.



Gambar 4.3 Grafik Garis yang Menyembunyikan Pesan “MATEMATIKA 2018”



Gambar 4.4 Grafik Garis yang Menyembunyikan Pesan "2018 matematika"

4.2 *Persamaan Kurva Eliptik pada Medan Berhingga Prima F_p*

Sebelum melakukan perhitungan pada setiap elemen-elemen grup eliptik modulo prima $GF(97)$ akan ditentukan terlebih dahulu kurva eliptik pada medan berhingga prima. Misalkan $p > 3$ adalah bilangan prima ganjil, dan $a, b \in F_p$ memenuhi $4a^3 + 27b^2 \neq 0(mod\ p)$ maka kurva eliptik didefinisikan pada medan berhingga prima (F_p) yaitu dapat dinotasikan dengan $GF(p)$ atau $E(F_p)$ merupakan himpunan titik-titik $P(x, y)$ dan sebuah titik $O(x, \infty)$, yaitu titik pada *infinity*. Titik-titik pada $GF(p)$ membentuk suatu grup eliptik modulo prima dimana titik-titik tersebut yang akan digunakan untuk proses penyandian.

Misal diberikan $GF(97)$ dan dipilih $a = 1$ dan $b = 3$ dengan a dan b memenuhi $4(1)^3 + 27(3)^2 = 247 \not\equiv 0\ (mod\ 97)$, sehingga didapatkan persamaan kurva eliptik:

$$GF(97): y^2 = x^3 + x + 3$$

Untuk menentukan titik-titik dalam kurva eliptik $GF(97)$, digunakan metode pencarian himpunan residu kuadratik modulo. Yaitu dengan mencari semua elemen dari himpunan residu kuadratik modulo 97 yang dinotasikan dengan QR_{97}, dengan cara menggunakan semua elemen dari himpunan $GF(97)$ sebagai titik y yang kemudian dikuadratkan dan hasil kuadrat dari titik y tersebut di modulo dengan 97, lalu didapatlah himpunan $QR(97)$.

4.3 *Elemen Grup Eliptik Modulo Prima* $GF(97)$

Akan ditentukan semua titik $P(x, y)$ pada kurva eliptik $y^2 \equiv x^3 + x + 3 \ (mod\ 97)$ dengan x dan y di definisikan di dalam $GF(97)$. Maka diketahui elemen di dalam $GF(97)$ adalah $\{0, 1, 2, \dots, 96\}$. Dilakukan perhitungan untuk semua titik pada kurva y^2 dengan mensubsitusi elemen $GF(97)$ ke persamaan kurva eliptik sebagai berikut:

1. Mencari residu kuadratis modulo $97 (QR_{97})$

Tabel 4.2 Residu Kuadraris Modulo 97

$y \in GF_{97}$	$y^2 (mod\ 97)$	QR_{97}	$y \in GF_{97}$	$y^2 (mod\ 97)$	QR_{97}
0	$y^2 (\text{mod } 97)$	0	49	$y^2 (\text{mod } 97)$	73
1	$y^2 (\text{mod } 97)$	1	50	$y^2 (\text{mod } 97)$	75
2	$y^2 (\text{mod } 97)$	4	51	$y^2 (\text{mod } 97)$	79
3	$y^2 (\text{mod } 97)$	9	52	$y^2 (\text{mod } 97)$	85
4	$y^2 (\text{mod } 97)$	16	53	$y^2 (\text{mod } 97)$	93
5	$y^2 (\text{mod } 97)$	25	54	$y^2 (\text{mod } 97)$	6
6	$y^2 (\text{mod } 97)$	36	55	$y^2 (\text{mod } 97)$	18
7	$y^2 (\text{mod } 97)$	49	56	$y^2 (\text{mod } 97)$	32
8	$y^2 (\text{mod } 97)$	64	57	$y^2 (\text{mod } 97)$	48
9	$y^2 (\text{mod } 97)$	81	58	$y^2 (\text{mod } 97)$	66
10	$y^2 (\text{mod } 97)$	3	59	$y^2 (\text{mod } 97)$	86

Tabel 4.2 Residu Kuadraris Modulo 97 (Lanjutan)

$y \in GF_{97}$	$y^2 (mod\ 97)$	QR_{97}	$y \in GF_{97}$	$y^2 (mod\ 97)$	QR_{97}
11	$y^2 (\text{mod } 97)$	24	60	$y^2 (\text{mod } 97)$	11
12	$y^2 (\text{mod } 97)$	47	61	$y^2 (\text{mod } 97)$	35
13	$y^2 (\text{mod } 97)$	72	62	$y^2 (\text{mod } 97)$	61
14	$y^2 (\text{mod } 97)$	2	63	$y^2 (\text{mod } 97)$	89
15	$y^2 (\text{mod } 97)$	31	64	$y^2 (\text{mod } 97)$	22
16	$y^2 (\text{mod } 97)$	62	65	$y^2 (\text{mod } 97)$	54
17	$y^2 (\text{mod } 97)$	95	66	$y^2 (\text{mod } 97)$	88
18	$y^2 (\text{mod } 97)$	33	67	$y^2 (\text{mod } 97)$	27
19	$y^2 (\text{mod } 97)$	70	68	$y^2 (\text{mod } 97)$	65
20	$y^2 (\text{mod } 97)$	12	69	$y^2 (\text{mod } 97)$	8
21	$y^2 (\text{mod } 97)$	53	70	$y^2 (\text{mod } 97)$	50
22	$y^2 (\text{mod } 97)$	96	71	$y^2 (\text{mod } 97)$	94
23	$y^2 (\text{mod } 97)$	44	72	$y^2 (\text{mod } 97)$	43
24	$y^2 (\text{mod } 97)$	91	73	$y^2 (\text{mod } 97)$	91
25	$y^2 (\text{mod } 97)$	43	74	$y^2 (\text{mod } 97)$	44
26	$y^2 (\text{mod } 97)$	94	75	$y^2 (\text{mod } 97)$	96
27	$y^2 (\text{mod } 97)$	50	76	$y^2 (\text{mod } 97)$	53
28	$y^2 (\text{mod } 97)$	8	77	$y^2 (\text{mod } 97)$	12
29	$y^2 (\text{mod } 97)$	65	78	$y^2 (\text{mod } 97)$	70
30	$y^2 (\text{mod } 97)$	27	79	$y^2 (\text{mod } 97)$	33
31	$y^2 (\text{mod } 97)$	88	80	$y^2 (\text{mod } 97)$	95
32	$y^2 (\text{mod } 97)$	54	81	$y^2 (\text{mod } 97)$	62
33	$y^2 (\text{mod } 97)$	22	82	$y^2 (\text{mod } 97)$	31
34	$y^2 (\text{mod } 97)$	89	83	$y^2 (\text{mod } 97)$	2
35	$y^2 (\text{mod } 97)$	61	84	$y^2 (\text{mod } 97)$	72
36	$y^2 (\text{mod } 97)$	35	85	$y^2 (\text{mod } 97)$	47

Tabel 4.2 Residu Kuadraris Modulo 97 (Lanjutan)

$y \in GF_{97}$	$y^2 (mod\ 97)$	QR_{97}	$y \in GF_{97}$	$y^2 (mod\ 97)$	QR_{97}
37	$y^2 (\text{mod } 97)$	11	86	$y^2 (\text{mod } 97)$	24
38	$y^2 (\text{mod } 97)$	86	87	$y^2 (\text{mod } 97)$	3
39	$y^2 (\text{mod } 97)$	66	88	$y^2 (\text{mod } 97)$	81
40	$y^2 (\text{mod } 97)$	48	89	$y^2 (\text{mod } 97)$	64
41	$y^2 (\text{mod } 97)$	32	90	$y^2 (\text{mod } 97)$	49
42	$y^2 (\text{mod } 97)$	18	91	$y^2 (\text{mod } 97)$	36
43	$y^2 (\text{mod } 97)$	6	92	$y^2 (\text{mod } 97)$	25
44	$y^2 (\text{mod } 97)$	93	93	$y^2 (\text{mod } 97)$	16
45	$y^2 (\text{mod } 97)$	85	94	$y^2 (\text{mod } 97)$	9
46	$y^2 (\text{mod } 97)$	79	95	$y^2 (\text{mod } 97)$	4
47	$y^2 (\text{mod } 97)$	75	96	$y^2 (\text{mod } 97)$	1

2. Menentukan nilai dari $y^2 \equiv x^3 + x + 3\ (mod\ 97)$

Pada pembahasan ini nilai y^2 adalah nilai dari persamaan kurva eliptik yang telah ditentukan sebelumya pada tabel 4.1. Dengan mensubsitusi setiap nilai $x \in GF_{97}$ ke persamaan $y^2 \equiv x^3 + x + 3\ (mod\ 97)$ maka diperoleh hasil sebagai berikut:

Tabel 4.3 Nilai $y^2 \equiv x^3 + x + 3\ (mod\ 97)$

$x \in GF_{97}$	y^2	$x \in GF_{97}$	y^2	$x \in GF_{97}$	y^2
0	3	33	83	66	57
1	5	34	56	67	36
2	13	35	39	68	29
3	33	36	38	69	42
4	71	37	59	70	81
5	36	38	11	71	55
6	31	39	94	72	67
7	62	40	23	73	26

Tabel 4.3 Nilai $y^2 \equiv x^3 + x + 3 \pmod{97}$ (Lanjutan)

$x \in GF_{97}$	y^2	$x \in GF_{97}$	y^2	$x \in GF_{97}$	y^2
8	38	41	95	74	35
9	62	42	25	75	3
10	43	43	13	76	33
11	84	44	65	77	34
12	94	45	90	78	12
13	79	46	94	79	70
14	45	47	83	80	20
15	95	48	63	81	62
16	41	49	40	82	8
17	83	50	20	83	58
18	33	51	9	84	24
19	91	52	13	85	9
20	69	53	38	86	19
21	70	54	90	87	60
22	3	55	78	88	41
23	68	56	8	89	65
24	77	57	80	90	41
25	36	58	9	91	72
26	48	59	92	92	67
27	22	60	44	93	32
28	61	61	65	94	70
29	74	62	64	95	90
30	67	63	47	96	1
31	46	64	20		
32	17	65	86		

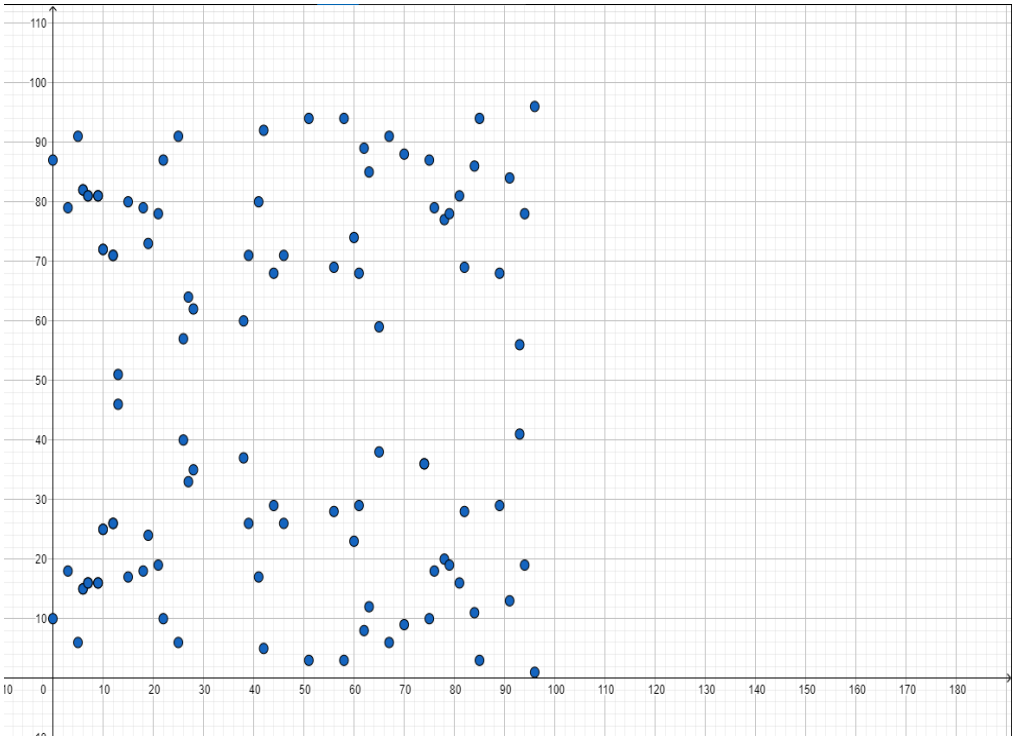
3. Menentukan pasangan berurutan $(x, y) \subset E_{97}$

Berdasarkan tabel 4.3, untuk $x = 1$ diperoleh nilai $y^2 = 1^3 + 1 + 3 \ (mod\ 97) = 5$. Setelah disamakan terhadap nilai residu kuadratis modulo 97 pada tabel 4.1, ternyata $y^2 = 5$ juga terdapat pada QR_{97} yaitu untuk nilai $y_1 = 11$ dan $y_2 = 18$. Maka didapatkan pasangan titik $(x, y) = (1,11)$ dan $(x, y) = (1,18)$ yang merupakan elemen-elemen dari grup eliptik $E_{97}(1,3)$.

Tidak semua $x \in GF_{97}$ akan menghasilkan nilai y^2 dari elemen QR_{97}. Misalnya, untuk $x = 0$ diperoleh nilai $y^2 = 0^3 + 0 + 3 \ (mod\ 97) = 3$, sedangkan y^2 tidak termuat pada QR_{97}. Sehingga untuk $x = 0$ tidak terdapat nilai y yang memenuhi.

Oleh karena itu perlu dilakukannya pengecekan pada setiap $x \in F_{97}$ yang dapat menghasilkan nilai $y^2 \in QR_{97}$. Sehingga dengan menggunakan cara yang sama, diperoleh hasil perhitungan yang dapat disajikan dalam tabel lampiran 3.

Jadi, titik-titik yang terdapat pada kurva eliptik adalah 96 titik, jika ditambah dengan titik O di infinity, maka titik-titik pada kurva eliptik membentuk grup dengan $n = 97$ elemen.



Gambar 4.1 Titik Kurva Eliptik $GF(97)$

Di dalam ECC, dua belah pihak yang berkomunikasi menyepakati parameter bilangan bulat (a, b) dan bilangan prima p pada persamaan kurva eliptik $y^2 = x^3 + ax + b\ (mod\ p)$, grup eliptik, dan sebuah titik basis $B(x, y)$ yang dipilih dari grup eliptik.

4.4 *Generator Grup Eliptik* $GF(97)$

Misalkan $P \in GF(97)$, maka P disebut generator atau pembangkit dari $GF(97)$ jika setiap elemen $GF(97)$ dapat dituliskan sebagai perpangkatan dari P atau $GF(97) = \{P^n | n \in GF(97)\}$ diaman $GF(97)$ merupakan bilangan prima dengan elemen di dalam medan galois $\{0,1,2,\ldots,36\}$. Pada pembahasan sebelumnya, telah didapatkan 96 titik $P(x, y)$ sehingga pembangkit dari grup eliptik $GF(97)$ 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 96 titik kurva yang ada ternyata semua titik tersebut merupakan generator dari grup eliptik $GF(97)$. Hasil perhitungan generator dari grup eliptik $GF(97)$ akan disajikan dalam lampiran 4.

4.5 *Elliptic Curves Cryptography Digital Signature Algorithm*

Akan ditinjau *Elliptic Curves Cryptography Digital Signature Algorithm*. Dalam hal ini yang harus diperhatikan yaitu kedua belah pihak menyepakati parameter bilangan bulat a dan b dan bilangan prima p pada persamaan kurva eliptik $y^2 \equiv x^3 + ax + b \ (mod\ p)$, grup eliptik, dan sebuah titik basis $B(x, y)$ yang dipilih dari elemen grup eliptik. Setelah mengetahui segala sesuatu yang dibutuhkan dalam penggunaan kriptografi kurva eliptik yan akan diaplikasikan pada tanda tagan digital, berikut akan dibahas mengenai *Elliptic Curves Cryptography Digital Signature Algorithm* dengan menggunakan contoh agar mudah dipahami. Misalkan, Alpha ingin membagi sebuah informasi pesan rahasia yang berbunyi “Matematika 2018” kepada Betha pesan ini merupakan pesan rahasia yang tidak boleh diketahui oleh sembarang orang. Jika pesan tersebut terungkap maka keamanan perusahaan bisa terganggu. Ada tiga algoritma kurva eliptik tanda tangan digital yang digunakan, yaitu:

1. Pembangkitan Kunci Publik dan Kunci Privat *Elliptic Curves Cryptography Digital Signature*

   Diketahui persamaan kurva eliptik atas medan berhingga $GF(p)$ yaitu $y^2 = x^3 + x + 3\ (mod\ 97)$. Dari persamaan tersebut diperoleh pasangan titik-titik kurva eliptik sebanyak 96 titik dan satu titik tak hingga yang dapat dilihat pada lampiran dalam tabel. Untuk pembangkitan kunci publik dan privat diperlukan nilai P_A dan P_B untuk masing-masing kedua belah pihak.

   Alpha membangkitkan kunci publik dan privatnya sebagai berikut:

   a. Pilih sebuah bilangan bulat $x = 3$

   b. Hitung $P_A = x \cdot B$

   $P_A = 3 \cdot (0{,}10)$

   $P_A = 2(0{,}10) + (0{,}10)$

   Dengan menggunakan rumus penggandaan titik kurva eliptik yang sudah dijelaskan pada sub bab 4.3. Berikut ini akan ditunjukan proses perhitungan untuk nilai 2P dan 3P:

   a. Misalkan $P(x_1 = 0, y_1 = 10) \in GF(97)$, maka $P + P = 2P = (x_3, y_3)$ dimana:

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

   $$= \left(\frac{3 \cdot 0^2 + 1}{2 \cdot 10}\right)^2 - 2 \cdot 0 = \left(\frac{1}{20}\right)^2 - 0 = (1 \cdot 20^{-1})^2 - 0$$

   $$= (1 \cdot 34)^2 - 0 = 34^2 (mod 97) = 89$$

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

$= \left(\frac{1}{20}\right)(0 - 89) - 10 = 34 \cdot (-89) - 10$

$= 34 \cdot 8 - 10 = 78 - 10 = 68\ (mod 97) = 68$

Jadi $2P = (89,68)$

b. Misalkan

$P(x_1 = 0, y_1 = 10) \in GF(97), Q(x_2 = 89, y_2 = 68) \in GF(97),$ dan $P \neq Q$, maka $P + Q = (x_3, y_3)$ dimana:

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

$= \left(\frac{68-10}{89-0}\right)^2 - 0 - 89 = \left(\frac{58}{89}\right)^2 - 89$

$= (58 \cdot 89^{-1})^2 - 89 = (58 \cdot 12)^2 - 89$

$= 17^2 - 89 = 6(mod\ 97) = 6$

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

$= 17 \cdot (0 - 6) - 10 = 17 \cdot (-6) - 10$

$= (17 \cdot 91) - 10 = 82\ mod\ 97 = 82$

Jadi $3P = (6,82)$

Maka diperoleh nilai $P_A = (6,82)$.

Jadi, $P_A = (6,82)$ adalah kunci publik Alpha dan $x = 3$ kunci privatnya.

Betha membangkitkan kunci privat dan kunci publiknya sebagai berikut:

a. Pilih sebarang bilangan bulat $y = 2$

b. Hitung $P_B = y \cdot B$

$P_B = 2 \cdot (0,10)$

Dengan menggunakan rumus penggandaan titik kurva eliptik yang sudah dijelaskan pada sub bab 4.3. Misalkan $P(x_1 = 0, y_1 = 10) \in GF(97)$,

maka $P + P = 2P = (x_3, y_3)$ dimana:

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

$= \left(\frac{3 \cdot 0^2 + 1}{2 \cdot 10}\right)^2 - 2 \cdot 0 = \left(\frac{1}{20}\right)^2 - 0 = (1 \cdot 20^{-1})^2 - 0$

$= (1 \cdot 34)^2 - 0 = 34^2 (mod 97) = 89$

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

$= \left(\frac{1}{20}\right)(0 - 89) - 10 = 34 \cdot (-89) - 10$

$= 34 \cdot 8 - 10 = 78 - 10 = 68\ (mod 97) = 68$

Maka diperoleh nilai $P_B = (89{,}68)$.

Jadi, $P_B = (89{,}68)$ adalah kunci publik Betha dan $y = 2$ kunci privatnya.

2. Prosedur Pembangkitan *Elliptic Curves Cryptography Digital Signature*

   Alpha membangkitkan tanda tangan digital untuk suatu pesan M = "Matematika 2018" sebagai berikut:

   a. Pilih sebuah bilangan bulat acak k, yang nilainya terletak pada selang $[1, p-1]$, akan dipilih $k = 10$

   b. Hitung $k \cdot B = (x_1, y_1)$ dan $r = x_1\ mod\ p$. Jika $r = 0$ maka kembali ketahap 1.

      $k \cdot B = 10 \cdot (0{,}10)$

      $= 5 \cdot (0{,}10) + 5 \cdot (0{,}10)$

      $= (3{,}18) + (3{,}18)$

      $= (94{,}19)$

      Jadi, $r = x_1 = 94\ mod\ 97 = 94$

   c. Hitung $k^{-1} mod\ p$

$k^{-1}\ mod\ p = 10^{-1}\ mod\ 97 = 68$

d. Hitung nilai hash dari M, yaitu $e = H(M)$.

Dengan pesan yang disampaikan "Matematika 2018" maka diperoleh

$e = a6bd3d71ecfd38391462dbedee65ba02$ (Heksadesimal)

$e = 221634437659671890243246613210809612 80$ (Desimal)

e. Hitung $s = k^{-1}(e + x \cdot r) mod\ p$. Jika $s = 0$, maka ulangi ke tahap 1.

$s = 10^{-1}(221634437659671890243246613210809612802 + 3 \cdot 94)\ mod\ 97$

$s = 67$

Maka diperoleh pesan M adalah (94,67) dari pembangkitan tanda tangan digital.

3. Prosedur Verifikasi Keabsahan *Elliptic Curves Cryptography Digital Signature*

Betha akan memverifikasi tanda tangan digital (r, s) dari Alpha sebagai berikut:

a. Verifikasi bahwa r dan s terletak di dalam selang $[1, p-1]$.

b. Ambil kunci publik Alpha, yaitu $3P_A$.

c. Betha menghitung nilai *Hash* dari M, yaitu $e = H(M)$.

$e = a6bd3d71ecfd38391462dbedee65ba02$ (Heksadesimal)

$e = 221634437659671890243246613210809612802$(Desimal)

d. Hitung $w = s^{-1}\ mod\ p$

$w = 67^{-1}\ mod\ 97 = 42$

e. Hitung $u_1 = e \cdot w\ mod\ p$ dan $u_2 = r \cdot w\ mod\ p$

$u_1 = e \cdot w\ mod\ p$

$u_1 = (22163443765967189024324661321080961280 2 \cdot$

$42) mod\ 97$

$u_1 = 0$

Maka, diperoleh nilai $u_1 = 0$

$u_2 = r \cdot w\ mod\ p$

$u_2 = 94 \cdot 42\ mod\ 97 = 68$

Maka, diperoleh nilai $u_2 = 68$

f. Hitung $(x_1, y_1) = u_1 \cdot B + u_2 \cdot P_A$

$(x_1, y_1) = u_1 \cdot B + u_2 \cdot P_A$

$(x_1, y_1) = 0 \cdot (0,10) + 68 \cdot (6,82)$

$(x_1, y_1) = 0 + (30(6,82) + 30(6,82) + 8(6,82))$

$(x_1, y_1) = 0 + \big((93,41) + (93,41) + (39,71)\big)$

$(x_1, y_1) = 0 + (26,57) + (39,71)$

$(x_1, y_1) = 0 + (94,19)$

$(x_1, y_1) = (94,19)$

g. Hitung $v = x_1\ mod\ p$

$v = x_1\ mod\ p$

$v = 94\ mod\ 97 = 94$

h. Maka, $v = r = 94$, tanda tangan sah

Hasil pengujian verifikasi *Elliptic Curves Cryptography Digital Signature* dari dua pesan dapat dilihat pada tabel 4.4

Tabel 4.4 Hasil Pengujian Verifikasi Elliptic Curves Cryptography Digital Signature dari Dua Pesan Berbeda

No.	Pesan	Fungsi Hash MD5	$M(r,s)$
1	MATEMATIKA 2018	4c1c51084eb518b13ac452a0bf4cf8c4	(15,17)
2	2018 matematika	3b4440218396357734f50ddf0d97d337	(9,16)

4.6 *Kajian Agama dengan Pembahasan*

Amanah merupakan salah satu sifat mulia yang dimiliki oleh Nabi Muhammad shallallahu ‘alaihi wa sallam. Ajaran untuk bersifat amanah ini sejalan dengan perintah Allah di surat An Nisa ayat 58. Selain itu, Nabi Muhammad juga pernah bersabda tentang amanah, yang diriwayatkan oleh Ahmad, “Tidak ada iman yang sempurna bagi orang yang tidak memiliki sifat amanah, dan tidak ada agama yang sempurna bagi orang yang tidak menepati janji”. (H.R. Ahmad, Muttafaq ‘alaih, Abu Daud dan Tirmidzi dari Ibnu Umar).

Dalam hal ini sebagai manusia kita mengemban amanah sebagai pemimpin di muka bumi, minimal memimpin diri kita sendiri. Kita juga berinteraksi dengan manusia lainnya yang juga akan membawa kita memikul amanah lainnya, seperti kepercayaan, kejujuran, janji, ataupun tanggung jawab lainnya. Bedasarkan pada penjelasan pada sub bab sebelumnya, maka untuk setiap keaslian sebuah pesan akan di nilai dari segi perjanjian atau tanggung jawab yang diberikan terhadap penerima dari pengirim yang bersangkutan.

BAB V
PENUTUP

5.1 Kesimpulan

Kriptografi kurva eliptik tanda tangan digital menggunakan konsep kurva eliptik untuk memverifikasi keabsahan sebuah pesan atau informasi berupa teks agar mengetahui keaslian teks tersebut dari pengirim. Kesimpulan yang dapat diambil penulis setelah menyelesaikan pembuatan skripsi ini adalah:

1. Proses penyembunyian pesan terenkripsi dengan menggunakan metode steganografi. Pada proses ini sebuah pesan M akan diubah ke representasi biner dan desimal menggunkana kode ASCII 8-bit. Setelah menghasilkan nilai desimal pesan terenkripsi tersebut akan di implementasikan menggunakan grafik kurva.
2. Proses pembangkitan kunci dan algoritma kurva eliptik tanda tangan digital pada proses pembangkitan kunci publik dan kunci privat akan menghasilkan niali P_A dan P_B sebagai kunci publik. serta kunci privat x dan y. Dalam hal ini diberikan sebuah contoh berupa pesan M yang berisi "Matematika 2018" yang akan diubah menjadi nilai hexadesimal dan nilai desimal.
3. Proses verifikasi keabsahan algoritma kurva eliptik tanda tangan digital pada proses verifikasi keabsahan pesan akan menghasilkan nilai $v = r$. Jika nilai $v \neq r$ maka sebuah pesan M tersebut tidak asli dan diragukan keasliannya.

5.2 Saran

Dalam skripsi ini hanya dibahas mengenai kriptografi kurva eliptik pada algoritma kurva eliptik tanda tangan digital dan hanya terbatas pada medan berhingga F_p serta dikombinasikan dengan metode steganografi. Sehingga untuk

skirpsi selanjutnya dapat dibahas penggunaan metode steganogarfi LSB atau yang lainnya. Serta penggunaan kriptografi kurva eliptik yang lain, maupun pertukaran kunci atau dapat pula membahas mengenai kriptografi kurva eliptik pada medan berhingga F_{2^m}.

DAFTAR PUSTAKA

Aditya, Y., Pratama, A., & Nurlifa, A. (2010). *Studi pustaka untuk steganografi dengan beberapa metode*. *2010*(Snati), 32–35.

Al-Ashfahani, A.-R. (2017). Al-Mufradat fi Gharibil Qur'an. In M. P. . Ruslan Nurhadi, Lc (Ed.), *Jilid 1* (1 ed., hal. 826). Pustaka Khazanah Fawa' id.

Al-Hasyīmī, S. A. (n.d.). *Mukhtar al-Ahadīst an-Nabawīyah wa al-Hikām al-Muhammadiyah Dar al-Alam*.

Al-Sheikh, A. B. M. bin A. bin I. (2003). Tafsir Ibnu Katsir. In *Jilid 2* (Edisi 2). Pustaka Imam asy-Syafi'i.

Andari, A. (2015). *Teori Grup*. Universitas Brawijaya Press.

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

Benvenuto, C. J. (2012). *Galois Field in Cryptography*. 1–11.

Cahyo Prabowo, E., & Afrianto, I. (2017). Ilmiah Komputer dan Penerapan Digital Signature dan Kriptografi Pada Teknik Informatika – Universitas Komputer Indonesia Ilmiah Komputer dan. *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*, *6*(2), 83–90.

Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2018). *Encryption and Decryption using Password Based Encryption, MD5, and DES*. *141*(ICOPOSDev 2017), 278–283. https://doi.org/10.2991/icoposdev-17.2018.57

Gilbert, L., & Gilbert, J. (2015). *Elements of Modern Algebra*.

Hakim, R., & Susilo, A. (2020). Makna dan Klasifikasi Amanah Qur'ani Serta Relevansinya dengan Pengembangan Budaya Organisasi. *AL QUDS : Jurnal Studi Alquran dan Hadis*, *4*(1), 119. https://doi.org/10.29240/alquds.v4i1.1400

Hamid, S. R. (2013). *Buku Pintar Hadist* (Ed. Revisi). Penerbit Qibla.

Hardiningsih, A. (2021). *Implementasi Fungsi Hash MD5 dan Kriptografi Algoritma RSA Pada Pembuatan Tanda Tangan Digital*.

Hayati, N., Andri Budiman, M., & Sharif, A. (2017). *Implementasi Algoritma RC4A dan MD5 untuk Menjamin Confidentiality dan Integrity pada File Teks*. *1*, 7.

Irawan, W. H., Hijriyah, N., & Habibi, A. R. (2014). *Pengantar Teori Bilangan* (A. H. Fathani (ed.); 1 ed.). UIN-MALIKI PRESS.

Katsir, I. A. al-F. (Ibnu). (n.d.). *Tafsir al-Qur'an al-Adzim*.

Munir, R. (2019). *Kriptografi* (Kedua). Informatika Bandung.

Schneier, B. (1994). *Applied Crypthography*. 784.

Setyobudi, F. M. (2013). *Penggunaan Kritptografi Kurva Eliptik Pada Proses Penyandian Elgamal*. Universitas Islam Negeri Maulana Malik Ibrahim.

Stallings, W. (2017). *Criptography and Net Securitywork Principles and Practice* (7 ed.). Pearson Education Limited.

Triwinarko, A. (2005). *Elliptic Curve Digital Signature Algorithm (ECDSA)*. 1–6.

LAMPIRAN

Lampiran 1 Program Python Untuk Menentukan Titik Kurva Eliptik

```
INF_POINT = None
class EllipticCurve:
	def __init__(self, a, b, p):
		self.a = a
		self.b = b
		self.p = p
		self.points = []
		self.definePoints()

	def definePoints(self):
		self.points.append(INF_POINT)
		for x in range(self.p):
			for y in range(self.p):
				if self.equalModp(y * y, x * x * x + self.a * x + 
self.b):
					self.points.append((x,y))

	def addition(self, P1, P2):
		if P1 == INF_POINT:
			return P2
		if P2 == INF_POINT:
			return P1

		x1 = P1[0]
		y1 = P1[1]
		x2 = P2[0]
		y2 = P2[1]

		if self.equalModp(x1, x2) and self.equalModp(y1, -y2):
			return INF_POINT

		if self.equalModp(x1, x2) and self.equalModp(y1, y2):
			u = self.reduceModp((3 * x1 * x1 + self.a) * 
self.inverseModp(2 * y1))
		else:
			u = self.reduceModp((y1 - y2) * self.inverseModp(x1 - x2))

		v = self.reduceModp(y1 - u * x1)
		x3 = self.reduceModp(u * u - x1 - x2)
		y3 = self.reduceModp(-u * x3 - v)

		return (x3, y3)
```

```
        def testAssociativity(self):
                n = len(self.points)
                for i in range (n):
                        for j in range(n):
                                for k in range(n):
                                        P = self.addition(self.points[i],
self.addition(self.points[j], self.points[k]))
                                        Q = self.addition(self.addition(self.points[i],
self.points[j]), self.points[k])
                                        if P != Q:
                                                return False
                return True



        def numberPoints(self):
                return len(self.points)

        def discriminant(self):
                D = -16 *(4 * self.a * self.a * self.a + 27 * self.b * self.b)
                return self.reduceModp(D)

        def printPoints(self):
                print(self.points)

        # helper functions

        def reduceModp(self, x):
                return x % self.p

        def equalModp(self, x, y):
                return self.reduceModp(x - y) == 0

        def inverseModp(self, x):
                for y in range(self.p):
                        if self.equalModp(x * y, 1):
                                return y
                return None

ec = EllipticCurve(1,3,97)
ec.printPoints()
print(ec.numberPoints())

P = ec.addition(ec.points[1], ec.points[1])
print(P)
```

Lampiran 2 Program Python untuk Menentukan Nilai Fungsi Hash MD5

```
import hashlib

str="Matematika 2018”
hasil=hashlib.md5(str.encode())

print("Hasil dalam bentuk MD5 adalah ", end="")
print(hasil.hexdigest())
```

Lampiran 3 Program Python Untuk Convert Nilai Hexadesimal ke Nilai Desimal

```
hexas=int(input(),16)
print("Your number in decimal is "+ str(hexas))
```

Lampiran 4 Program Python untuk Menghitung Nilai Penjumlahan dan Penggandaan Titik Kurva Eliptik

```
P = [0, 10]
prime = 97
a = 1
b = 3

def gcdExtended(a, b):
    if a == 0:
        return b, 0, 1
    gcd, x1, y1 = gcdExtended(b % a, a)
    x = y1 - (b // a) * x1
    y = x1
    return gcd, x, y

def double_point(point: list):
    x = point[0]
    y = point[1]

    s = ((3*(x**2)+a) * (gcdExtended(2*y, prime)[1])) % prime

    newx = (s**2 - x - x) % prime
    newy = (s * (x - newx) - y) % prime

    return [newx, newy]

def add_points(P: list, Q: list):
   x1 = P[0]
   y1 = P[1]
   x2 = Q[0]
   y2 = Q[1]
```

```
    s = (y2-y1) * (gcdExtended(x2-x1, prime)[1] % prime)

    newx = (s**2 - x1 - x2) % prime
    newy = (s * (x1 - newx) - y1) % prime

    return [newx, newy]

Q = P
index = 2
while True:
    if Q[0] == P[0] and Q[1] == P[1]:
        print("doubling")
        Q = double_point(P)
    else:
        print("adding")
        Q = add_points(P, Q)

    if index == 97 :
        break

    print(f"{index}P = {Q}")
    index += 1
```

Lampiran 5 Tabel Elemen $GF(97)(1,3)$

$x \in F_{97}$	$y^2 \equiv x^3 + x + 3 \ (mod\ 97)$	$y^2 \in QR_{97}$	$(x,y) \in E_{97}(1,3)$
0	3	Ya	(0,10) dan (0,87)
1	5	Tidak	-
2	13	Tidak	-
3	33	Ya	(3,18) dan (3,79)
4	71	Tidak	-
5	36	Ya	(5,6) dan (5, 91)
6	31	Ya	(6,15) dan (6,82)
7	62	Ya	(7,16) dan (7,81)
8	38	Tidak	-
9	62	Ya	(9,16) dan (9,81)
10	43	Ya	(10,25) dan (10,72)
11	84	Tidak	-
12	94	Ya	(12,26) dan (12,71)
13	79	Ya	(13,46) dan (13,51)

Lampiran 3: Tabel Elemen $GF(97)(1,3)$ (Lanjutan)

$x \in F_{97}$	$y^2 \equiv x^3 + x + 3 \ (mod\ 97)$	$y^2 \in QR_{97}$	$(x, y) \in E_{97}(1, 3)$
14	45	Tidak	-
15	95	Ya	(15,17) dan (15,80)
16	41	Tidak	-
17	83	Tidak	-
18	33	Ya	(18,18) dan (18,79)
19	91	Ya	(19,24) dan (19,73)
20	69	Tidak	-
21	70	Ya	(21,19) dan (21,78)
22	3	Ya	(22,10) dan (22,87)
23	68	Tidak	-
24	77	Tidak	-
25	36	Ya	(25,6) dan (25,91)
26	48	Ya	(26,40) dan (26,57)
27	22	Ya	(27,33) dan (27,64)
28	61	Ya	(28,35) dan (28,62)
29	74	Tidak	-
30	67	Tidak	-
31	46	Tidak	-
32	17	Tidak	-
33	83	Tidak	-
34	56	Tidak	-
35	39	Tidak	-
36	38	Tidak	-
37	59	Tidak	-
38	11	Ya	(38,37) dan (38,60)
39	94	Ya	(39,26) dan (39,71)
40	23	Tidak	-
41	95	Ya	(41,17) dan (41,80)
42	25	Ya	(42,5) dan (42,92)
43	13	Tidak	-
44	65	Ya	(44,29) dan (44,68)
45	90	Tidak	-
46	94	Ya	(46,26) dan (46,71)
47	83	Tidak	-
48	63	Tidak	-
49	40	Tidak	-
50	20	Tidak	-
51	9	Ya	(51,3) dan (51,94)
52	13	Tidak	-
53	38	Tidak	-
54	90	Tidak	-
55	78	Tidak	-
56	8	Ya	(56,28) dan (56,69)
57	80	Tidak	-

Lampiran 3: Tabel Eleme $GF(97)(1,3)$ (Lanjutan)

$x \in F_{97}$	$y^2 \equiv x^3 + x + 3 \ (mod\ 97)$	$y^2 \in QR_{97}$	$(x, y) \in E_{97}(1, 3)$
58	9	Ya	(58,3) dan (58,94)
59	92	Tidak	-
60	44	Ya	(60,23) dan (60,74)
61	65	Ya	(61,29) dan (61,68)
62	64	Ya	(62,8) dan (62,89)
63	47	Ya	(63,12) dan (63,85)
64	20	Tidak	-
65	86	Ya	(65,38) dan (65,59)
66	57	Tidak	-
67	36	Ya	(67,6) dan (67,91)
68	29	Tidak	-
69	42	Tidak	-
70	81	Ya	(70,9) dan (70,88)
71	55	Tidak	-
72	67	Tidak	-
73	26	Tidak	-
74	35	Ya	(74,36) dan (74,61)
75	3	Ya	(75,10) dan (75,87)
76	33	Ya	(76,18) dan (76,79)
77	34	Tidak	-
78	12	Ya	(78,20) dan (78,77)
79	70	Ya	(79,19) dan (79,78)
80	20	Tidak	-
81	62	Ya	(81,16) dan (81,81)
82	8	Ya	(82,28) dan (82,69)
83	58	Tidak	-
84	24	Ya	(84,11) dan (84,86)
85	9	Ya	(85,3) dan (85,94)
86	19	Tidak	-
87	60	Tidak	-
88	41	Tidak	-
89	65	Ya	(89,29) dan (89,68)
90	41	Tidak	-
91	72	Ya	(91,13) dan (91,84)
92	67	Tidak	-
93	32	Ya	(93,41) dan (93,56)
94	70	Ya	(94,19) dan (94,78)
95	90	Tidak	-
96	1	Ya	(96,1) dan (96,96)

Lampiran 6 Tabel Generator Grup Eliptik GF(97) Pada Titik (0,10) dan (6,82)

P	(0,10)	(6,82)	43P	(75,10)	(70,9)	86P	(12,71)	(61,68)
2P	(89,68)	(58,94)	44P	(22,87)	(56,69)	87P	(94,78)	(84,86)
3P	(6,82)	(21,19)	45P	(63,12)	(67,91)	88P	(21,78)	(10,72)
4P	(41,80)	(76,18)	46P	(82,69)	(18,18)	89P	(15,80)	(63,12)
5P	(3,18)	(61,8)	47P	(96,96)	(26,57)	90P	(93,41)	(25,6)
6P	(58,94)	(91,13)	48P	(25,6)	(12,71)	91P	(58,3)	(82,28)
7P	(93,56)	(27,64)	49P	(25,91)	(15,80)	92P	(3,79)	(75,87)
8P	(15,17)	(39,71)	50P	(96,1)	(3,79)	93P	(41,17)	(7,81)
9P	(21,19)	(9,16)	51P	(82,28)	(89,29)	94P	(6,15)	(85,94)
10P	(94,19)	(81,16)	52P	(63,85)	(0,10)	95P	(89,29)	(28,62)
11P	(12,26)	(19,73)	53P	(22,10)	(41,80)	96P	(0,87)	(51,3)
12P	(76,18)	(61,68)	54P	(75,87)	(93,56)			
13P	(46,26)	(84,86)	55P	(10,25)	(94,19)			
14P	(26,40)	(10,72)	56P	(65,38)	(46,26)			
15P	(62,8)	(63,12)	57P	(7,81)	(78,77)			
16P	(78,77)	(25,6)	58P	(84,11)	(79,78)			
17P	(18,79)	(82,28)	59P	(44,68)	(74,36)			
18P	(91,13)	(75,87)	60P	(85,94)	(60,23)			
19P	(79,78)	(7,81)	61P	(61,29)	(13,46)			
20P	(67,6)	(85,94)	62P	(38,37)	(51,94)			
21P	(27,64)	(28,62)	63P	(28,62)	(28,35)			
22P	(74,36)	(51,3)	64P	(19,24)	(85,3)			
23P	(56,28)	(13,52)	65P	(42,5)	(7,16)			
24P	(39,71)	(60,74)	66P	(51,3)	(75,10)			
25P	(60,23)	(74,61)	67P	(81,81)	(82,69)			
26P	(70,88)	(79,19)	68P	(5,91)	(25,91)			
27P	(9,16)	(78,20)	69P	(13,51)	(63,85)			
28P	(13,46)	(46,71)	70P	(9,81)	(10,25)			
29P	(5,6)	(94,78)	71P	(70,9)	(84,11)			
30P	(81,16)	(93,41)	72P	(60,74)	(61,29)			
31P	(51,94)	(41,17)	73P	(39,26)	(19,24)			
32P	(42,92)	(0,87)	74P	(56,69)	(81,81)			
33P	(19,73)	(89,68)	75P	(74,61)	(9,81)			
34P	(28,35)	(3,18)	76P	(27,33)	(39,26)			
35P	(38,60)	(15,17)	77P	(67,91)	(27,33)			
36P	(61,68)	(12,26)	78P	(79,19)	(91,84)			
37P	(85,3)	(26,40)	79P	(91,84)	(62,89)			
38P	(44,29)	(18,79)	80P	(18,18)	(91,13)			
39P	(84,86)	(67,6)	81P	(78,20)	(27,64)			
40P	(7,16)	(56,28)	82P	(62,89)	(39,71)			
41P	(65,59)	(70,88)	83P	(26,57)	(9,16)			
42P	(10,72)	(5,6)	84P	(46,71)	(81,16)			
43P	(75,10)	(70,9)	85P	(76,79)	(19,73)			

Lampiran 7 Tabel Kode ASCII (Kode Karakter 32 – 128)

Desimal	Biner	Hexadesimal	Karakter
32	00100000	20	*(Space)*
33	00100001	21	!
34	00100010	22	"
35	00100011	23	#
36	00100100	24	$
37	00100101	25	%
38	00100110	26	&
39	00100111	27	'
40	00101000	28	(
41	00101001	29	)
42	00101010	2A	*
43	00101011	2B	+
44	00101100	2C	,
45	00101101	2D	-
46	00101110	2E	.
47	00101111	2F	/
48	00110000	30	0
49	00110001	31	1
50	00110010	32	2
51	00110011	33	3
52	00110100	34	4
53	00110101	35	5
54	00110110	36	6
55	00110111	37	7
56	00111000	38	8
57	00111001	39	9

58	00111010	3A	:
59	00111011	3B	;
60	00111100	3C	<
61	00111101	3D	=
62	00111110	3E	>
63	00111111	3F	?
64	01000000	40	@
65	01000001	41	A
66	01000010	42	B
67	01000011	43	C
68	01000100	44	D
69	01000101	45	E
70	01000110	46	F
71	01000111	47	G
72	01001000	48	H
73	01001001	49	I
74	01001010	4A	J
75	01001011	4B	K
76	01001100	4C	L
77	01001101	4D	M
78	01001110	4E	N
79	01001111	4F	O
80	01010000	50	P
81	01010001	51	Q
82	01010010	52	R
83	01010011	53	S
84	01010100	54	T
85	01010101	55	U

86	01010110	56	V
87	01010111	57	W
88	01011000	58	X
89	01011001	59	Y
90	01011010	5A	Z
91	01011011	5B	[
92	01011100	5C	\
93	01011101	5D	]
94	01011110	5E	^
95	01011111	5F	_
96	01100000	60	`
97	01100001	61	a
98	01100010	62	b
99	01100011	63	c
100	01100100	64	d
101	01100101	65	e
102	01100110	66	f
103	01100111	67	g
104	01101000	68	h
105	01101001	69	i
106	01101010	6A	j
107	01101011	6B	k
108	01101100	6C	l
109	01101101	6D	m
110	01101110	6E	n
111	01101111	6F	o
112	01110000	70	p
113	01110001	71	q

114	01110010	72	r
115	01110011	73	s
116	01110100	74	t
117	01110101	75	u
118	01110110	76	v
119	01110111	77	w
120	01111000	78	x
121	01111001	79	y
122	01111010	7A	z
123	01111011	7B	{
124	01111100	7C	|
125	01111101	7D	}
126	01111110	7E	~
127	01111111	7F	*(Delete)*
128	10000000	80	€

RIWAYAT HIDUP

Muhammad Febry Andrean , dilahirkan di Malang pada tanggal 27 Mei 2001. Memiliki nama panggilan Andre. Bertempat tinggal di Ds. Gambiran Dsn. Bogem RT/RT 002/006 Kec. Prigen Kab. Pasuruan. Berasal dari Ds. Jambesari Dsn. Sumberjambe RT/RW 014/003 Kec. Poncokusumo Kab. Malang. Merupakan putra pertama dari pasangan Bapak Jazuli dan Ibu Supi'ani serta memiliki adik perempuan yang bernama Ayunda yuniastanti.

Jenjang pendidikannya dimulai sejak bersekolah di TK Negeri Pembina Kec. Prigen yang lulus pada tahun 2007. Setelah itu melanjutkan Pendidikan di SD Negeri Gambiran 1 Prigen yang lulus pada tahun 2013. Pendidikan selanjutnya ditempuh di Mts. Unggulan Amanatul Ummah yang lulus pada tahun 2016. Kemudian melanjutkan Pendidikan di MA Unggulan Amanatul Ummah yang lulus pada tahun 2018. Pada jenjang perguruan tinggi ia melanjutkan pendidikannya dengan berkuliah di UIN Maulana Malik Ibrahim Malang dengan memilih menekuni bidang Matematika murni di Fakultas Sains dan Teknologi.

Selama menempuh Pendidikan di Kampus UIN Maulana Malik Ibrahim Malang, selain menyelesaikan tugasnya sebagai mahasiswa, Ia juga memiliki aktivitas yakni pemilik toko bahan bangunan di Kec. Prigen Kab. Pasuruan. Menurutnya dengan kegiatan tersebut, dapat semakin mengasah ilmu yang didapatkan di bangku perkuliahan sepertihalnya analisis khususnya pada perekonomian dan perdagangan sembari menambah pengalaman. Baginya, Matematika adalah salah satu ilmu yang istimewa.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Mohamad Febry Andrean
NIM : 18610103
Fakultas / Jurusan : Sains dan Teknologi / Prodi Matematika
Judul Skripsi : Penerapan Metode *Noiseless Steganography* dan *Elliptic Curves Cryptography Digital Signature Algorithm* Pada Pengamanan Pesan Teks
Pembimbing I : Juhari, M.Si,
Pembimbing II : Ach. Nasichuddin, M.A.

No	Tanggal	Hal	Tanda Tangan
1.	12 Februari 2022	Konsultasi Bab 4	1.
2.	16 Februari 2022	Konsultasi Bab 1,2	2.
3.	24 Februari 2022	Konsultasi Bab 1,2,3	3.
4.	17 Maret 2022	Konsultasi Bab 1,2,3	4.
5.	24 Maret 2022	ACC Bab 1,2,3	5.
6.	12 April 2022	Konsultasi ½ Bab 4	6.
7.	20 April 2022	Konsultasi ½ Bab 4	7.
8.	27 Mei 2022	Konsultasi ½ Bab 4	8.
9.	26 Mei 2022	Konsultasi ½ Bab 4	9.
10.	30 Mei 2022	Revisi Bab 4	10.
11.	6 Juni 2022	Revisi Bab 4	11.
12.	8 Juni 2022	Konsultasi ½ Bab 4,5	12.
13.	10 Juni 2022	ACC Bab 4,5	13.
14.	15 Juni 2022	Revisi Bab 5	14.
15	20 Juni 2022	Konsultasi Bab 5	15.

Malang, 21 Juni 2022
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, S.Pd., M.Sc.
NIP. 19741129200012200 5