PENERAPAN *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM* (ECDSA) PADA *DIGITAL SIGNATURE* UNTUK PENGAMANAN DOKUMEN

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik
Pada Jurusan Teknik Informatika

Oleh:

JONI SAPUTRA
11351104894

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2021

LEMBAR PERSETUJUAN

PENERAPAN *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM* (ECDSA) PADA *DIGITAL SIGNATURE* UNTUK PENGAMANAN DOKUMEN

TUGAS AKHIR

Oleh

JONI SAPUTRA

11351104894

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir

di Pekanbaru, pada tanggal 25 Januari 2021

Pembimbing,

Febi Yanto, S.T., M.Kom.

NIK 198102062009121003

LEMBAR PENGESAHAN

PENERAPAN *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM* (ECDSA) PADA *DIGITAL SIGNATURE* UNTUK PENGAMANAN DOKUMEN

TUGAS AKHIR

Oleh

JONI SAPUTRA

11351104894

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar sarjana Teknik Informatika
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 25 Januari 2021

Pekanbaru, 25 Januari 2021
Mengesahkan,

Dekan,	Ketua Jurusan,
Dr. Drs. Ahmad Darmawi., M.Ag.	**Dr. Elin Haerani, S.T., M.Kom.**
NIP. 19660604 199203 1 004	**NIP. 19810523 200710 2 003**

DEWAN PENGUJI

Ketua	: Muhammad Fikry, S.T.,M.Sc.
Sekretaris	: Febi Yanto, M.Kom.
Anggota I	: Benny Sukma Negara, S.T.,M.T.
Anggota II	: Pizaini, M.Kom.

LEMBAR HAK KEKAYAAN INTELEKTUAL

Tugas akhir yang tidak diterbitkan ini telah terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankkan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan seizin penulis dan harus disertai dengan kebiasaan ilmiah untuk menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh tugas akhir ini harus memperoleh izin dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan yang meminjamkan tugas akhir ini untuk anggotanya diharapkan untuk mengisi nama, tanda peminjaman dan tanggal peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana pada suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali secara tertulis yang terdapat dalam naskah ini dan disebutkan didalam daftar pustaka.

Pekanbaru, Januari 2021

Yang membuat pernyataan,

JONI SAPUTRA
11351104894

LEMBAR PERSEMBAHAN

Alhamdulillahi Rabbil'alamiiin

Tidak ada kata yang bisa diucapkan selain kata syukur kepada Allah

'Azza Wa Jalla

Sholawat serta salam untuk Rasulallah

Muhammad Shalallahu 'Alaihi Wa Sallam

Serta ucapan terimakasih pada ayah dan ibu tercinta, atas tetesan keringat, motivasi, saran dan nasihatnya. Sehingga laporan Tugas Akhir ini dapat terselesaikan. Kupersembahkan karya sederhana ini untuk

Ayah dan Ibu

Dan bagi para pembaca yang membaca. Terimakasih.

PENERAPAN *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM* (ECDSA) PADA *DIGITAL SIGNATURE* UNTUK PENGAMANAN DOKUMEN

JONI SAPUTRA

11351104894

Tanggal wisuda :

Periode wisuda :

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Pada penelitian ini akan membahas pengamanan pesan menggunakan metode digital signature yang di enkripsi dan dekripsi dengan menggunakan *Elliptic Curve Digital Signature Algorithm*. Dimana pesan atau dokumen yaitu surat wasiat atau surat kuasa dengan format pdf akan dibubuhi tanda tangan digital dengan cara di enkripsi menggunakan *Elliptic Curve Digital Signature Algorithm* sehingga menghasilkan kunci public dan kunci private. Setelah itu kunci public digunakan untuk mengenkripsi pesan sehingga menghasilkan *Chipertext*. Kemudian pesan yang sudah dienkripsi tersebut dikirim ke penerima kemudian penerima mendekripsi *chipertext* tersebut menggunakan kunci *private* sehingga pesan dapat di baca oleh penerima. Kunci *private* hanya boleh diketahui oleh si pengirim dan si penerima sedangkan kunci *public* boleh diketahui oleh orang lain. Pada penelitian ini hanya memfokuskan pada penandatanganan satu surat oleh satu orang dan diterima oleh satu orang saja. Diharapkan dengan penelitian ini dapat lebih membantu dalam penandatanganan surat penting seperti surat wasiat atau surat kuasa walaupun pengirim dan penerima tidak bertatap muka dan data yang dikirim tetap aman.

Kata kunci: *Digital Signature*, *Elliptic Curve Digital Signature Algorithm*, Kunci *private*, kunci *public*, *chipertext*, surat wasiat

PENERAPAN *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM* (ECDSA) PADA *DIGITAL SIGNATURE* UNTUK PENGAMANAN DOKUMEN

JONI SAPUTRA

11351104894

Date of Final Exam :

Graduation Ceremony Period:

Inforatics Engineering Departement

Faculty of Science and Technology

Islamic State University of Sultan Syarif Kasim Riau

ABSTRACT

Pada penelitian ini akan membahas pengamanan pesan menggunakan metode digital signature yang di enkripsi dan dekripsi dengan menggunakan *Elliptic Curve Digital Signature Algorithm*. Dimana pesan atau dokumen yaitu surat wasiat atau surat kuasa dengan format pdf akan dibubuhi tanda tangan digital dengan cara di enkripsi menggunakan *Elliptic Curve Digital Signature Algorithm* sehingga menghasilkan kunci public dan kunci private. Setelah itu kunci public digunakan untuk mengenkripsi pesan sehingga menghasilkan *Chipertext*. Kemudian pesan yang sudah dienkripsi tersebut dikirim ke penerima kemudian penerima mendekripsi *chipertext* tersebut menggunakan kunci *private* sehingga pesan dapat di baca oleh penerima. Kunci *private* hanya boleh diketahui oleh si pengirim dan si penerima sedangkan kunci *public* boleh diketahui oleh orang lain. Pada penelitian ini hanya memfokuskan pada penandatanganan satu surat oleh satu orang dan diterima oleh satu orang saja. Diharapkan dengan penelitian ini dapat lebih membantu dalam penandatanganan surat penting seperti surat wasiat atau surat kuasa walaupun pengirim dan penerima tidak bertatap muka dan data yang dikirim tetap aman.

Kata kunci: *Digital Signature*, *Elliptic Curve Digital Signature Algorithm*, Kunci *private*, kunci *public*, *chipertext*, surat wasiat

KATA PENGANTAR

بسم الله الرحمن الرحيم

Assalamu'alaikum wa rahmatullahi wa barakaatuh

Alhamdulillahi rabbil'alamin, ucapan syukur kepada Allah 'Azza Wa Jalla yang senantiasa memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penelitian dan penulisan laporan tugas akhir ini yang berjudul "Penerapan *Elliptic Curve Digital Signature Algorithm* (ECDSA) Pada *Digital Signature* Untuk Pengamanan Dokumen". Shalawat dan salam kepada Rasulallah Muhammad Shalallahu 'Alaihi Wa Sallam, yang telah membimbing kita ke jalan yang lurus dan penuh cahaya serta ridha dari Allah 'Azza Wa Jalla, sehingga kita dapat merasakan sains dan teknologi yang memudahkan aktivitas dan ibadah kita sehari-hari. Laporan tugas akhir ini disusun sebagai salah satu syarat untuk mendapatkan gelar Sarjana Teknik pada jurusan Teknik Informatika Universitas Islam Negeri Sultan Syarif Kasim Riau. Selama proses dalam menyelesaikan tugas akhir ini, telah mendapatkan bantuan, bimbingan, dukungan, serta motivasi baik secara langsung atau tidak langsung. Untuk itu, pada kesempatan ini penulis ingin menyampaikan ucapan terimakasih kepada:

1. Bapak Prof. DR. KH. Akhmad Mujahidin, S.Ag., M.Ag., selaku Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Ahmad Darmawi, M.Ag., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
3. Ibu Dr. Elin Hearani, ST., M.Kom, selaku Ketua Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
4. Bapak Benny Sukma Negara, S.T., M.T, selaku Pembimbing Akademik dan sekaligus Penguji I Tugas Akhir.
5. Bapak Febi Yanto, M.Kom, selaku Pembimbing I Tugas Akhir.
6. Bapak Dr.Alwis Nazir, M.Kom, selaku Pembimbing II Tugas Akhir.

7. Bapak Pizaini, M.Kom, selaku Penguji II Tugas Akhir.
8. Seluruh Dosen Teknik Informatika yang telah memberikan ilmu dan bimbingan yang bermanfaat untuk kami.
9. Ayah dan Ibu penulis yaitu, Bapak Ali dan Ibu Arneli. Saudari Erlina Fitri, S.Pd beserta suami Afri Rahman dan seluruh keluarga yang ikut mrndorong dan memotivasi penulis hingga ke tahap ini.
10. Teman-teman TIF F 2013 yang tidak bisa penulis sebutkan namanya satu-persatu yang telah saling membantu selama masa perkuliahan, memotivasi dan saling mendoakan.
11. Semua Pihak yang turut memberikan doa, bantuan dan motivasinya baik secara langsung atau tidak langsung. Semoga laporan Tugas Akhir ini dapat bermanfaat bagi para pembacanya. Mohon maaf apabila dalam penulisan Tugas Akhir ini terdapat kesalahan dalam penulisan atau bahasa dalam pembahasan. Apabila ada kritik dan saran untuk laporan Tugas Akhir ini dapat disampaikan melalui alamat email joni.saputra@students.uin-suska.ac.id. Selamat membaca dan semoga bermanfaat.

wassalamu'alaikum wa rahmatullah wa barakaatuh

Pekanbaru, 25 Januari 2021

Penulis

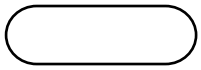
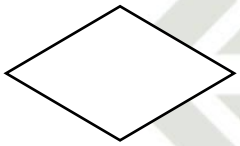
DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SIMBOL

Keterangan notasi simbol *flowchart* :

Simbol	Keterangan
	Terminator : Simbol terminator (mulai / selesai) merupakan simbol yang menunjukkan permulaan dan akhir dari proses
	Proses : Simbol yang digunakan untuk melakukan pemrosesan data baik oleh user maupun komputer (sistem).
	Verifikasi : Simbol yang digunakan untuk memutuskan apakah valid atau tidak validnya suatu kejadian.
	Data : Simbol yang digunakan untuk mendeskripsikan data yang digunakan

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada masa yang sangat berkembang cukup pesat saat ini begitu banyak dokumen yang tersebar luas di dunia maya maupun dunia nyata. Jika sebuah dokumen mempunyai informasi yang penting dan pada proses pengirimannya tidak dilakukan pengamanan, maka besar kemungkinan terjadinya penggandaan dokumen, pencurian hak cipta dan penyebar luasan informasi secara ilegal. Maka dari itu, dibutuhkan sebuah skema keamanan yang dapat mengamankan data dan dokumen tersebut.

Keamanan merupakan aspek penting dalam kehidupan di zaman yang sudah serba modern pada saat ini. Dalam penerapannya informasi bisa disebarluaskan secara rahasia sehingga hanya orang-orang tertentu saja yang dapat melihat isi pesan tersebut. Keamanan pada dokumen dapat dimanipulasi dengan berbagai cara, begitu pula dengan dokumen elektronik.

Pertukaran dokumen berbasis komputer atau dokumen elektronik dilakukan dengan berbagai cara atau media, salah satunya menggunakan *e-mail*. Dokumen dalam pesan *e-mail* di internet sudah sangat luas digunakan sebagai transaksi yang legal. Dokumen sering berisi informasi penting seperti kontrak resmi, transaksi keuangan, *record* penjualan, surat wasiat dan lain sebagainya. Pada beberapa dokumen penting tersebut ada dokumen yang memakai tanda tangan baik secara langsung atau tanda tangan digital.

Verifikasi suatu dokumen dalam hal memberi kuasa dilakukan terhadap seseorang yang menandatangani dokumen tersebut. Dokumen sangat penting dalam transaksi komersil lewat internet misalnya pada *e-mail*. Dokumen berbasis komputer disebut dokumen elektronik (*e-dokumen*) atau dokumen digital. Untuk menjamin bahwa *e-dokumen* yang diterima masih utuh artinya sama dengan *e-dokumen* yang dikirim dan penandatangan adalah penandatangan sebenarnya dari *e-dokumen* tersebut, salah satunya dengan memberi tandatangan digital (Wahyuni, 2011).

Pada sebuah kasus di Italia, saham perusahaan tiba-tiba berpindah tangan dari pemilik ke orang lain karena diakali oleh oknum akuntan, yang mengaktifkan tandatangan digital menggunakan fotocopy KTP (Putra, 2018). Maka dari itu salah satu cara teknik pengamanan pesan adalah tandatangan digital (*Digital Signature*) (Ahmaddul Hadi, 2013).

Pada penelitian sebelumnya yang dilakukan oleh (Ahmaddul Hadi, 2013), penelitian tersebut mengenkripsi dokumen atau pesan elektronik dengan model dan aplikasi keamanan dengan algoritma *Digital Signature Algorithm* (DSA) pada Sistem Informasi Akademik (SIA) menggunakan *digital signature* menghasilkan sebuah kode yang telah di-enkripsi sebelumnya kemudian dikonversikan ke dalam bentuk *barcode* lalu aplikasi men-dekripsi *barcode* menjadi informasi yang dimengerti oleh pengguna.

Kemudian pada penelitian sebelumnya yang dilakukan oleh (Precilia dan Izzuddin, 2015) yang menjelaskan tentang pengamanan dokumen yaitu surat pembritahuan dan surat penagihan yang di-enkripsi dengan menggunakan algoritma MD5 lalu menghasilkan nilai hash perbandingan antara data pada dokumen dan chipertextnya, kemudian dengan nilai tersebut akan dapat diketahui apabila ada perubahan pada isi dokumen tersebut.

Selanjutnya pada penelitian (Wahyuni, 2011), menjelaskan tentang rancang bangun sebuah aplikasi kriptografi *hybrid* dengan *Digital Signature Algorithm* (DSA) dengan mendigitalisasi tandatangan asli secara *offline*, yang mana penandatangan suatu dokumen boleh lebih dari satu penandatangan, kemudian dokumen dikirim melalui internet kepada penerima, kemudian penerima memverifikasi apakah dokumen tersebut asli atau tidak.

Kemudian pada penelitian (Ramayanti, 2007), menjelaskan perancangan dan pembuatan sebuah aplikasi untuk autentifikasi kartu tanda penduduk yang sah agar terhindar dari pemalsuan KTP. Algoritma yang digunakan untuk melakukan proses hashing adalah MD5. Dimana hasil dari MD5 adalah *Message digest*. Hasil dari MD5 ini akan dienkripsi dengan menggunakan algoritma AES (*Advanced Encryption Standard*) dengan *Cipher Mode Counter* sehingga menghasilkan tanda tangan dari nomor induk kependudukan.

Pada penelitian sebelumnya (Kusuma, 2014) dalam jurnalnya menyatakan bahwa *Elliptic Curve Digital Signature Algorithm* (ECDSA) yang membandingkan DSA dan ECDSA. ECDSA memiliki tingkat keamanan lebih baik dari algoritma *digital signature* yaitu *Digital Signature Algorithm* (DSA). Disebabkan karena waktu yang dibutuhkan perhitungan serangan utuk menemukan *private key* pada ECDSA 15,5 kali lebih lama dibandingkan dengan DSA. Maka dari itu penulis melakukan penelitian pengamanan dokumen menggunakan *digital signature* dengan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA). Pada penerapannya, pada aplikasi ini satu dokumen hanya dapat ditandatangani oleh satu penandatangan yaitu orang yang membuat dokumen secara sah dan diverifikasi kembali oleh penerima kepada si pengirim.

Dari penelitian diatas, metode yang telah dibahas termasuk ke dalam permasalahan matematis logaritma diskrit (*Discret Logaritma Problem, DLP*) dan pemfaktoran bilangan bulat (*Integer Factoryzation Problem, IFP*) sedangkan tidak ada algoritma waktu subeksponensial yang diketahui untuk memecahkan permasalahan matematis logaritma diskrit kurva eliptik (*Elliptic Curve Discret Logarith Problem, ECDLP*). Oleh karena itu, algoritma kurva eliptik mempunyai keuntungan dibandingkan dengan algoritma kunci publik lainya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama seperti yang disebutkan dalam jurnal (Triwinarko, 2005).

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka didapatlah rumusan masalah yaitu, "bagaimana menerapkan *Elliptic Curve Digital Signature Algorithm* (ECDSA) pada *digital signature* untuk pengamanan dokumen**?**"

1.3 Batasan Masalah

Dalam penulisan tugas akhir ini, yang menjadi ruang lingkup untuk batasan masalah adalah sebagai berikut:

1. Data yang di enkripsi hanya berupa dokumen surat wasiat atau surat kuasa dengan format *pdf.*
2. Pengamanan dokumen ini hanya satu tandatangan dan satu penandatangan untuk satu dokumen.

3. Penelitian ini tidak membandingkan metode yang digunakan dengan metode lain.
4. Penilitian ini tidak menghitung tingkat kekuatan algoritma yang digunakan.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah membangun aplikasi pengamanan data berupa dokumen penting dengan teknik kriptografi *Digital Signature* dengan menerapkan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) yang berfungsi sebagai peng-enkripsi dan dekripsi dokumen yang hanya dapat ditandatangani oleh satu orang.

1.5 Sistematika Penulisan

Sistematika penulisan skripsi dibagi menjadi 6 (enam) Bab, yang masing-masing bab telah dirancang dan disusun dengan suatu tujuan tertentu, berikut penjelasan masing-masing bab:

BAB I PENDAHULUAN

Pendahuluan berfungsi mengantar pembaca untuk membaca laporan tugas akhir secara keseluruhan. Bagian pendahuluan terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menguraikan teori yang berkaitan dalam pembuatan aplikasi dalam tugas akhir ini yaitu kriptografi, *Digital Signature* dan *Elliptic Curve Digital Signature Algorithm* (ECDSA).

BAB III METODE PENELITIAN

Menjelaskan metode pengerjaan tugas akhir, studi pustaka, perumusan masalah, analisis, perancangan, implementasi, pengujian dan kesimpulan beserta saran.

BAB IV ANALISA DAN PERANCANGAN

Pada bab ini akan membahas mengenai analisis data dan perancangan yang mencakup analisis masalah, data masukan dan keluaran (*input* dan *output*), deskripsi umum perangkat lunak (deskripsi umum sistem dan

karakteristik pengguna), deskripsi fungsional (*flowchart, context diagram, data flow diagram, entity relation diagram* dan rancangan *database*), rancangan menu dan *prototype*.

BAB V IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi penjelasan tentang pengertian dan tujuan implementasi sistem, batasan implementasi, lingkungan implementasi, impelmentasi sistem dan pengujian terhadap sistem yang dibangun.

BAB VI PENUTUP

Bab ini berisi kesimpulan, saran yang membangun serta daftar pustaka mengenai penelitian yang dilakukan.

BAB II
LANDASAN TEORI

2.1 Keamanan Data dan Informasi

Pada era digitalisasi yang berkembang sangat pesat ini, komunikasi dengan menggunakan perangkat dan jaringan komputer merupakan sebuah kebiasaan bahkan kebutuhan bagi setiap orang. Melalui jaringan, seseorang dapat berkomunikasi atau melakukan transaksi dengan sangat cepat dan praktis. Hal ini dipengaruhi oleh perkembangan yang signifikan dalam perkembangan teknologi informasi, dimana kecepatan internet semakin besar dan dengan biaya akses yang semakin murah dan terjangkau untuk semua kalangan.

Keamanan informasi menurut G.J. Simon dalam buku (Rahardjo, 2002) adalah cara untuk mencegah penipuan terhadap informasi atau setidaknya mendeteksi adanya penipuan yang terdapat di sebuah sistem informasi, walaupun informasi tersebut tidak berguna atau tidak bermanfaat sama sekali.

Keamanan informasi memiliki sebuah standar baku internasional dibawah organisasi yang bernama *ISO* (*the International Organization for Standarization)* dan *IEC* (*the International Electrotechnical Commission).* Dalam buku (Indrajit Eko, 2011) menjelaskan bahwa, badan nasional anggota *ISO* dan *IEC* berpatisipasi dalam pengembangan standarisasi internasional tentang keamanan informasi melaluli panitia teknik yang disepakati oleh organisasi-organisasi yang terpercaya keahliannya dalam aktivitas teknis yang berada di seluruh dunia.

Dalam keamanan data dan informasi harus terdapat empat aspek berikut, yaitu:

1. *Privacy/Confidentiality* yaitu memastikan bahwa informasi yang tersedia hanya bisa diakses dan diterima oleh pihak yang memiliki wewenang.
2. *Integrity* yaitu berusaha untuk memastikan bahwa isi informasi tidak dirubah, dikurangi dan ditambah dengan menggunakan metodologi yang efektif.
3. *Authentication* yaitu usaha untuk memastikan bahwa informasi yang diterima adalah benar keasliannya.
4. *Avalaibility* yaitu memastikan bahwa informasi terkait diakses oleh pihak yang berwenang sesuai dengan kebutuhannya.

2.2 Kriptografi

Kriptografi memiliki sejarah yang sangat panjang. Dalam buku (Menezes, Oorschot dan Vanstone, 1996), menjelaskan tentang buku yang ditulis oleh Kahn yang berjudul *The Codebreakers* merupakan buku yang menelusuri kriptografi dari awal-awal masa 4000 tahun yang lalu oleh bangsa Mesir, meski demikian penggunaannya pada saat itu sangat terbatas sampai abad ke 20 atau bahkan hingga saat ini. Buku ini selesai pada tahun 1963, *the Codebreakers* memiliki peran penting dalam berjalannya sejarah kriptografi. Hal yang paling berperan penting dalam penggunaan kriptografi pada saat itu adalah dibidang militer, pelayanan diplomatik dan pemerintahan. Kriptografi digunakan untuk melindungi informasi tentang strategi serta keaamanan negara.

Salah satu hal yang terlihat sangat signifikan pada kriptografi kunci publik adalah fitur yang dinamakan *Digital Signature.* Pada 1991, standar internasional pertama untuk *Digital Signature* (ISO/IEC 9796) telah diadopsi. Berbasis pada skema kunci publik *RSA* (Rivest Shamir Adleman). Tahun 1994, U.S. Government mengadopsi *Digital Signature Standard*, sebuah mekanisme yang berdasar pada skema kunci publik El-Gamal.

2.2.1 Definisi dan Terminologi Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani :"*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Menurut Sentot Kromoedimoeljo dalam jurnal (Purnamal dan Lestiawan, 2014) Kriptografi adalah ilmu yang mempelajari mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsinya. Sedangkan menurut (Schneier, 1996), kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pada pesan. Lalu menurut (Menezes et al, 1996), kriptografi adalah studi teknik matematika yang berkaitan dengan aspek informasi keamanan seperti kerahasiaan, integritas data, otentikasi, entitas, dan asal data.

Jadi kriptogafi adalah seni dalam menyembunyikan sebuah pesan baik fisik atau isi pesan agar tidak dapat diubah atau disalahgunakan dari orang yang bukan

penerima pesan resmi dengan teknik enkripsi dan di dekripsi oleh penerima resmi agar dapat membaca isi pesan tersebut.

Kriptografi pada dasarnya sangat sederhana yaitu ada text awal (*plaintext*) lalu dienkripsi dan menghasilkan *chipertext* atau secara matematis dapat dituliskan dengan rumus *C=E(M).* Kemudian untuk mengembalikan ke data semula disebut dengan dekripsi. Proses nya dari *chipertext* kemudian di dekripsi dan menghasilkan *plaintext* atau secara matematis dapat dituliskan dengan rumus *M = D(C).*

Kriptografi memiliki dua buah jenis kunci yaitu kunci simetris dan asimetris. Kunci simetris menggunakan satu buah kunci yaitu kunci privat dalam proses enkripsi dan dekripsi, dimana kunci hanya boleh diketahui oleh pengirim dan penerima. Sedangkan kunci asimetris menggunakan dua buah kunci yaitu kunci publik dan kunci privat, dimana kunci publik boleh disebarluaskan sedangkan kunci privat hanya pengirim dan penerima saja yang boleh mengetahuinya.

2.3 Algoritma Kriptografi Klasik

Menurut Rinaldi Munir, algoritma kriptografi klasik terbagi atas dua macam *chiper* yaitu:

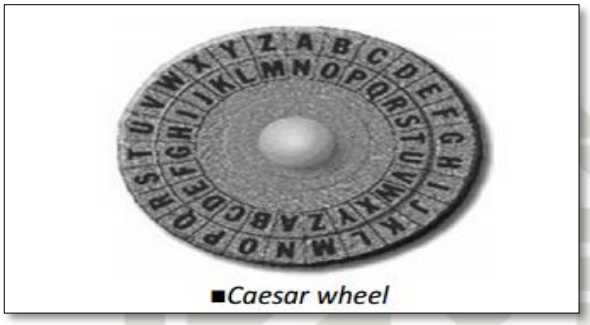
2.3.1 *Chiper* Subtitusi

Dalam *chipher* substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu “unit” di sini bisa berarti satu huruf, pasangan huruf, atau kelompok lebih dari dua huruf. *Chiper* substitusi dapat dikelompokkan ke dalam empat jenis, yaitu:

1. Cipher Alfabet Tunggal (*Monoalphabetic cipher*), satu huruf di plainteks diganti dengan tepat satu huruf cipherteks.
2. Cipher Alfabet Majemuk (*Polyalphabetic chiper*), merupakan cipher substitusi ganda.
3. Cipher Substitusi Homofonik (*homophonic substitution cipher*), seperti cipher alfabet tunggal tetapi setiap huruf dalam plainteks dapat dipetakan ke dalam salah satu dari unit cipherteks yang mungkin.
4. Cipher Substitusi Poligram (*Polygram substitution cipher*), setiap kelompok huruf disubstitusi dengan kelompok huruf cipherteks.

Algoritma substitusi tertua yang diketahui adalah caesarcipher yang digunakan oleh kaisar Romawi, Julius Caesar, untuk menyandikan pesan yang ia kirim kepada para gubernurnya.

Pada Gambar 2.1 memperlihatkan caesar wheel terdiri dari dua buah lempeng lingkaran besi. Pada lingkaran luar menyatakan huruf plaintext sedangkan untuk lingkaran dalam menggambarkan *chipertext*.



Gambar 2.1 Caesar Wheel *(Lindquist, Diarra* dan *Millard, 2004)*

2.3.2 *Cipher* Transposisi

Pada cipher transposisi, huruf-huruf di dalam plaintekstetap sama, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut. Kriptografi dengan alat *scytale* yang digunakan oleh tentara Sparta pada zaman Yunani termasuk ke dalam cipher transposisi. Algoritma Kriptografi Modern

Kriptografi modern mempunyai kerumitan yang sangat kompleks karena dioperasikan menggunakan komputer. Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma kriptografi modern terdiri dari dua bagian (Ariyus, 2006).

2.3.3 Algoritma Simetris

Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya (Munir, 2006). Keamanan algoritma simetris tergantung pada kuncinya. Algoritma simetris sering juga disebut algoritma kunci rahasia, algoritma kunci tunggal atau algoritma satu kunci. Dua kategori yang termasuk pada algoritma simetris ini adalah algoritma block cipher dan stream

cipher. Aplikasi dari algoritma simetris diantaranya adalah Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), A5, RC4 dan lain sebagainya.

2.3.4 Algoritma Asimetris

Algoritma asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu kunci lainnya untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki kunci rahasia yang dapat melakukan pembongkaran terhadap kode yang dikirim untuknya atau mendekripsi pesan tersebut (Mahmudi, Mantja dan Rozikin, 2016). Beberapa algoritma asimetris lainnya yaitu *RSA (Rivest Shamir Adleman), Diffie Hellman* dan lain sebagainya.

2.3.5 Algoritma *Hybrid*

Algoritma hibrid adalah algoritma yang memafaatkan dua tingkatan kunci, yaitu kunci rahasia atau simetri yang disebut juga *session key* (kunci sesi) untuk enkripsi data dan pasangan kunci rahasia kunci publik untuk pemberian tandatangan digital serta melindungi kunci simetri (Muttaqin, 2010).

2.4 Kriptografi Kunci Publik

Sistem kriptografi nirsimetri dipublikasikan pertama kali pada tahun 1976 oleh Whitfield Diffie dan Martin Hellman, duaorang ilmuwan dari Stanford University melalui makalah berjudul "*New Directions in Cryptography*". Makalah mereka membahas distribusi kunci rahasia pada saluran komunikasi publik dengan metode pertukaran kunci yang belakangan dikenal dengan nama algoritma pertukaran kunci Diffie-Hellman.

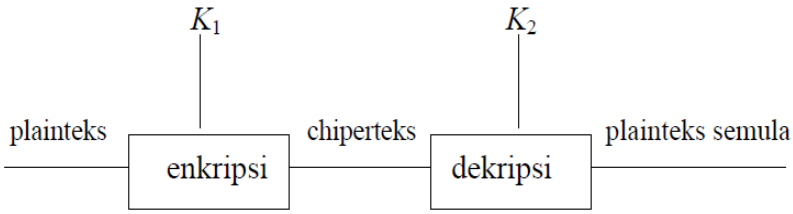
Pada tahun 1977, generalisasi dari ide Cocks ditemukan kembali oleh tiga orang ilmuwan dari MIT, yaitu Rivest, Shamir, dan Adleman. Algoritma enkripsi yang mereka buat dikenal dengan nama Rivest Shamir Adleman.

Akhirnya sejak tahun 1976 berbagai algoritma enkripsi, tanda tangan digital, pertukaran kunci, dan teknik lain dikembangkan dalam bidang kriptografi kunci publik, misalnya algoritma El Gamal untuk enkripsi dan algoritma DSA *(Digital Signature Algorithm)* untuk tandatangan digital. Pada tahun 1980 Neal Koblitz

memperkenalkan *elliptic curve cryptography* sebagai keluarga baru yang analog dengan algoritma kriptografi kunci publik (Munir, 2006).

2.4.1 Konsep Kriptografi Kunci Publik

Pada kriptografi kunci publik, setiap pengguna memiliki sepasang kunci, satu kunci untuk enkripsi, dan satu kunci untuk dekripsi (Gambar 2.2). Kunci untuk enkripsi diumumkan kepada publik (oleh karena itu tidak rahasia) sehingga dinamakan kunci publik (*public key*), disimbolkan dengan *e*. Kunci untuk dekripsi bersifat rahasia sehingga dinamakan kunci pribadi (*private key*), disimbolkan dengan *d*. Karena kunci enkripsi ≠ kunci dekripsi itulah kriptografi kunci publik disebut juga kriptografi nirsimetri (Munir, 2006)



Gambar 2.2 Skema Algoritma Kunci Publik (Munir, 2006)

Misalkan *E* adalah fungsi enkripsi dan *D* adalah fungsi dekripsi. Misalkan (*e*, *d*) adalah pasangan kunci untuk enkripsi dan dekripsi sedemikian rupa, sehingga:

$$E_e(m) = c \; dan \; D_d\,(c) = m \qquad (2.1)$$

Untuk suatu plainteks m dan cipherteks c. kedua persamaaan ini menyiratkan bahwa dengan mengetahui e dan c, maka secara komputasi hampir tidak mungkin menemukan m. asumsi lainnya, dengan mengetahui e, secara komputasi hampir tidak mungkin menurunkan d. Ee digambarkan sebagai fungsi pintu kolong *(trapdoor)* satu arah dengan d adalah informasi trapdoor yang diperlukan untuk menghitung fungsi inversinya, D yang dalam hal ini membuat proses dekripsi dapat dilakukan.

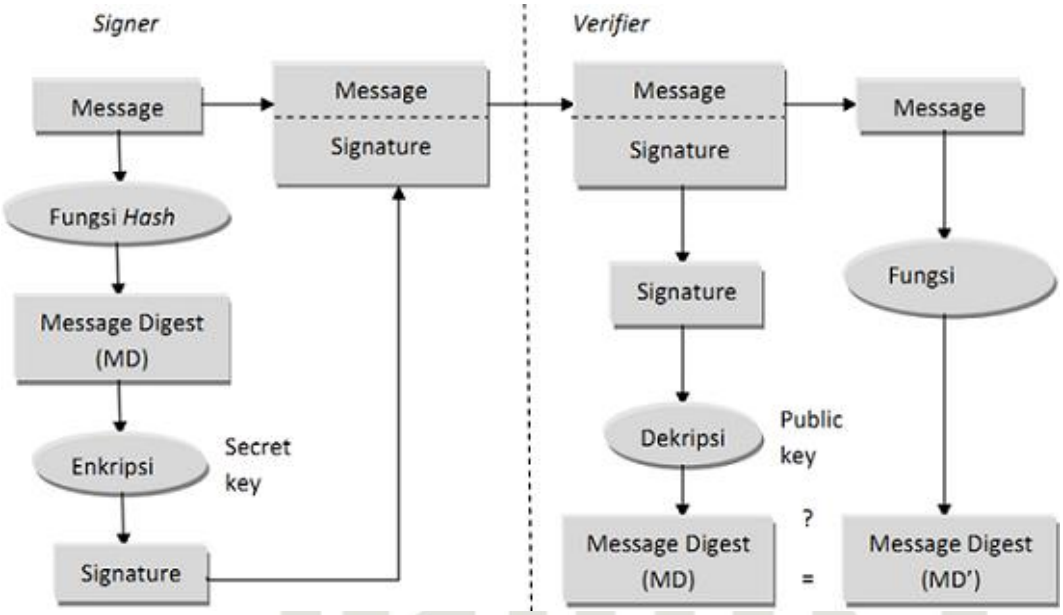
Sistem kriptografi kunci publik ini cocok digunakan di dalam kelompok pengguna di lingkungan jaringan komputer (LAN/WAN). Karena kunci publik tidak rahasia, biasanya disimpan di dalam basis data kunci yang dapat diakses oleh

pengguna lain. Hanya penerima pesan yang dapat mendekripsi pesan karena ia yang mengetahui kunci privatnya sendiri. Dengan sistem kriptografi kunci publik, tidak diperlukan pengiriman kunci privat melalui saluran komunikasi khusus sebagaimana pada sistem kriptografi simetris (Munir, 2006 : 176).

2.5 Tanda tangan Digital *(Digital Signature)*

Tanda tangan digital (*digital signature*) menurut Rinaldi Munir dalam jurnal (Ahmaddul Hadi, 2013) adalah suatu mekanisme untuk menggantikan tanda tangan secara manual pada dokumen kertas. Yang dimaksud dengan tanda tangan digital bukanlah tanda tangan yang di digitalisasi dengan alat berupa *scanner*, tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan. Kegunaan tanda tangan adalah menyatakan pengesahan (*data integrity*) atas apa yang tercantum dalam dokumen tersebut, menyatakan pertanggung jawaban penandatangan (*data origin*) atas apa yang tertulis dalam dokumen tersebut. Untuk mencegah satu saat penandatangan mengingkari apa yang tertulis di dokumen bertanda tangan tersebut (*non repudiation*). Adapun aspek keamanan kerahasiaan (*confidentiality*) tidak terdapat pada sistem tanda tangan digital, tanda tangan yang telah dienkripsikan terlebih dahulu dan menghasilkan sebuah kunci publik (*public key*) serta tanda dengan algoritma tertentu. Jika tanda tangan digital yang telah dienkripsi menggunakan kunci publik X, maka pada proses mendeskripsikan kembali dengan kunci pribadi X, maka pesan tidak akan terbuka akan tetapi hanya dapat dibuka dengan kunci pribadi Y.

Gambar berikut menunjukkan proses penandatanganan menggunakan *digital signature* dan proses verivikasinya



Gambar 2.3 Proses penandatanganan digital signature

Proses penandatanganan *digital signature* diawali dengan mengubah isi dokumen menjadi *message digest* menggunakan fungsi *hash*, kemudian *message digest* dienkripsi menggunakan kunci privat, hasil enkripsi inilah yang disebut sebagai *digital signature*, kemudian hasil enkripsi disematkan pada dokumen. Untuk proses verifikasi, *digital signature* didekripsi menggunakan kunci publik yang kemudian akan menghasilkan *message digest*. Kemudian *message digest* yang telah dihasilkan dari proses dekripsi tersebut dibandingkan dengan *message digest* dari dokumen yang asli. Apabila nilai *message digest* yang dihasilkan dari proses dekripsi tersebut sama maka pesan tersebut berasal dari pengirim yang sebenarnya

2.6 ECDSA (*Elliptic Curve Digital Signature Algorithm*)

Algoritma penandatanganan pesan menggunakan ECC yang disebutkan sebagai ECDSA adalah salah satu variasi dari *Digital Signature Algorithm* yang beroperasi dengan kelompok kurva elliptic sebagai basis perhitungan dari proses penandatanganan. Agar dapat menyamakan suatu tanda tangan digital dari sebuah pesan yang dikirim oleh dua orang, maka kedua orang tersebut harus memiliki kurva eliptik yang sama. Seorang pengirim pesan yang akan ditandatangani akan memiliki sebuah kunci pribadi yang merupakan sebuah integer yang dipilih acak kurang dari *n* yang merupakan urutan kurva, pada kurva eliptik domain. Dan kunci

publik yang merupakan titik yang digenerasikan dengan kurva eliptik domain dengan perhitungan sebagai berikut: QA = dA * G Proses ECDSA.

Seperti dengan kriptografi kurva eliptik pada umumnya, ukuran bit dari kunci publik diyakini diperlukan untuk ECDSA adalah sekitar dua kali ukuran tingkat keamanan, dalam bit. Sebagai perbandingan, pada tingkat keamanan 80 bit, berarti penyerang membutuhkan sekitar setara dengan sekitar 280 generasi tanda tangan untuk menemukan kunci pribadi, ukuran kunci DSA publik setidaknya 1024 bit, sedangkan ukuran sebuah kunci publik ECDSA akan menjadi 160 bit. Di sisi lain, ukuran tanda tangan adalah sama untuk kedua DSA dan ECDSA: 4t bit, dimana t adalah tingkat keamanan yang diukur dalam bit, yaitu sekitar 320 bit untuk tingkat keamanan 80 bit.

2.6.1 Bidang Terbatas

Bidang terbatas (*finite field*) atau yang biasa disebut dengan *Galois Field* (GF) adalah bidang yang hanya memiliki elemen bilangan yang terbatas. Derajat (*order*) dari finite field adalah banyaknya elemen yang ada di dalam bidang. Jika q adalah pangkat prima (prime power), maka hanya ada satu bidang terbatas dengan derajat q. Bidang tersebut dilambangkan dengan F_q atau GF(q). Banyak cara untuk merepresentasikan elemen dari F_q, jika $q=p^m$, dimana p adalah bilangan prima dan m adalah bilangan integer positif, maka p disebut sebagai karakteristik dari F_q dan m disebut sebagai derajat perluasan (*extension degree*) dari F_q. Bidang terbatas yang digunakan dalam kriptografi adalah q=p, dimana p adalah bilangan prima ganjil, yang dilambangkan dengan F_p (*odd prime*), dan $q=2^m$, dimana m adalah integer lebih besar dari satu, yang dilambangkan dengan F_{2^m} (*characteristic two or even*).

1. Kurva Eliptik Pada Bidang Terbatas F_p

Misalkan p > 3 adalah bilangan prima ganjil, dan a,b ∈ Fp memenuhi

$$4a^3 + 27b^2 \neq 0 \ (mod\ p) \qquad (2.2)$$

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 :

$$y^2 = x^3 + ax + b \quad (2.3)$$

dan sebuah titik khusus $\phi(\infty,\infty)$ yang merupakan titik tak hingga. Operasi penjumlahan pada $E(F_p)$ didefinisikan sebagai berikut :

1. $P + \phi = \phi + P = P$ untuk setiap $P \in E(F_p)$ Jika $P(x.y) \in E(F_p)$, maka $(x,y) + (x,-y) = \phi$ (titik $(x,-y) \in E(F_p)$ dinotasikan sebagai -P, disebut sebagai negatif dari P)
2. Misalkan $P(x_1,y_1) \in E(F_p)$, $Q(x_2,y_2) \in E(F_p)$, dan $P \neq \pm Q$, maka $P + Q = (x_3,y_3)$ dimana :

$$x_3 = \frac{(y_2 - y_1)}{x_2 - x_1} - x_1 - x_2 \quad (2.4)$$

$$y_3 = \frac{(y_1 - y_1)}{x_2 - x_1} - (x_1 - x_3) - y_1 \quad (2.5)$$

3. Misalkan $P(x_1,y_1) \in E(F_p)$, maka $P + P = 2P = (x_3,y_3)$, dimana :

$$x_3 = \frac{(3{x_1}^2 + a)^2}{2y_1} - 2x_1 \quad (2.6)$$

$$y_3 = \frac{(3{x_1}^2 + a)}{2y_1} - (x_1 - x_3) - y_1 \quad (2.7)$$

Operasi di atas disebut dengan penggandaan titik (*doubling a point*)

Kehebatan dari operasi penjumlahan pada kurva eliptik adalah jika menjumlahkan dua buah titik yang merupakan elemen dari kelompok kurva eliptik, maka hasil penjumlahannya adalah titik lain yang juga merupakan elemen dari kelompok kurva eliptik tersebut.

2. Kurva Eliptik Pada Bidang Terbatas F_2^m

Sebuah kurva eliptik E pada F_2^m didefinisikan sebagai sebagai sebuah persamaan dalam bentuk:

$$y^2 + xy = x^3 + ax^2 + b \quad (2.8)$$

dimana $a,b \in F_2^m$, dan $b \neq 0$. Set E (F_2^m) terdiri dari seluruh titik (x,y), $x \in F_2^m$, $y \in F_2^m$ yang memenuhi persamaan kurva eliptik tersebut, bersamaan dengan titik khusus $\phi(\infty, \infty)$ yang disebut titik tak hingga (*point at infinity*).

Sebagaimana kurva-kurva eliptik pada Fp, ada aturan-aturan untuk menjumlahkan titik–titik pada kurva eliptik $E(F_2^m)$ untuk mendapatkan sebuah titik ketiga kurva eliptik. Rumus aljabar untuk menjumlahkan dua titik dan menggandakan dua titik adalah sebagai berikut.

1. $P + \phi = \phi + P = P$ untuk seluruh $P \in E(F_2^m)$. Jika $P = (x,y) \in E(F_2^m)$, kemudian $(x,y) + (x, x+y) = \phi$. (Titik $(x,x+y)$ dinotasikan dengan $-P$, dan disebut negatif P.
2. Misalkan $P = (x_1,y_1) \in E(F_2^m)$ dan $Q = (x2,y2) \in E(F_2^m)$, dimana $P \neq \pm Q$. Kemudian $P + Q = (x_3,y_3)$,
   dimana

$$x_3 = \frac{(y_1+y_2)^2}{x_1+x_2} + \frac{(y_1-y_2)}{x_1+x_2} + x_1 + x_2 + \alpha \qquad (2.9)$$

$$y_3 = \frac{(y_1+y_2)}{x_1+x_2} + (x_1 + x_3) + x_3 + y_1 \qquad (2.10)$$

3. Penggandaan titik (*Point doubling*) Misalkan $P = (x_1,y_1) \in E(F_2^m)$, kemudian $2P = (x_3,y_3)$, dimana :

$$x_3 = {x_1}^2 + \frac{b}{{x_1}^2} \qquad (2.11)$$

$$y_3 = {x_1}^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3 \qquad (2.12)$$

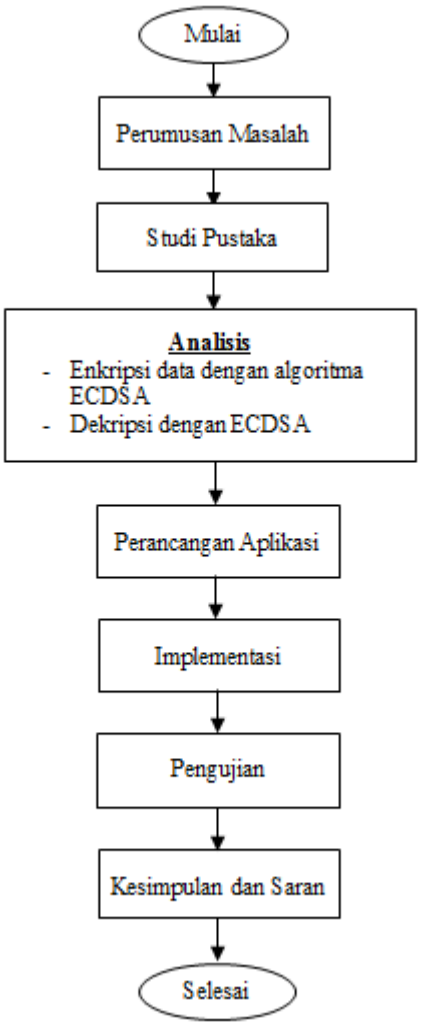
Dalam aturan Elliptic Curve Digital Signature Algorithm menurut (Triwinarko, 2005), penandatangan ditandai dengan D = {q, FR, a, b, G, n, h} dan pasangan kunci private d_A dan kunci publik Q_A. Kemudian pihak penerima memiliki salinan dokumen D yang otentik dan kunci publik Q_A. Kemudian proses yang terjadi adalah sebagai berikut:

1. Tahap menentukan kunci
   a. Memilih sebuah bilangan bulat random d_A, yang nilainya harus memenuhi syarat [1,n-1]
   b. Menghitung $Q_A = d_A \bullet G = (x_1,y_1)$
   c. Kunci private = d_A, dan kunci publik = Q_A.

2. Tahap penandatanganan
   a. Memilih sebuah bilangan bulat random k, yang nilainya diantara [1,n-1].
   b. Menghitung $Q_A = k \bullet G = (x_1,y_1)$ dan $r = x_1 \bmod n$, jika $r = 0$, maka kembali ke langkah 1.
   c. Menghitung $k^{-1} \bmod n$
   d. Menghitung $e = Hash(m)$
   e. Menghitung $s = k^{-1} \{e+d_A \bullet r\} \bmod n$ tanda tangan untuk message m adalah (r,s)
3. Tahap verifikasi
   a. Memverifikasi bahwa r dan s adalah bilangan bulat yang antara [1,n-1]
   b. Menghitung $e = Hash (m)$
   c. Menghitung $w = s^{-1} \bmod n$
   d. Menghitung $u_1 = ew \bmod n$ dan $u_2 = rw \bmod n$
   e. Menghitung $u_1 \bullet G + u_2 \bullet Q_A = (x_1,y_1)$
   f. Menghitung $v = x_1 \bmod n$
   g. Menerima tanda tangan jika dan hanya jika v = r

BAB III
METODOLOGI PENELITIAN

Beberapa tahapan dalam pengerjaan penelitian ini adalah seperti pada Gambar 3.1 berikut.



Gambar 3.1 Tahapan Penelitian

3.1 Perumusan Masalah

Tahapan ini merupakan tahapan awal dari metodologi penelitian. Berdasarkan latar belakang yang telah dijabarkan maka dapat dirumuskan permasalahan yang akan dijadikan sebagai penelitian tugas akhir yaitu bagaimana menerapkan *Elliptic Curve Digital Signature Algorithm* (ECDSA) pada *Digital Signature* untuk penandatanganan dokumen.

3.2 Studi Pustaka

Pada tahap ini dilakukan proses-proses pengumpulan teori yang terkait dengan penelitian ini dengan mencari referensi-referensi terkait yang dibutuhkan terkait penelitian ini. Referensi tersebut dapat berupa buku-buku, jurnal, tulisan para peneliti ahli, artikel dari internet dengan situs terpercaya mengenai kriptografi, *digital signature* dan *Elliptic Curve Digital Signature Algorithm* (ECDSA).

3.3 Analisis

Tahapan ini adalah menganalisis aplikasi yang akan dibangun dengan cara menganalisa hal-hal yang berhubungan dengan enkripsi teks dengan algoritma ECDSA *(Ellipic Curve Digital Signature Algorithm)*. Terdapat beberapa tahapan dalam proses penandatanganan menggunakan ECDSA yaitu:

1. Tahapan menentukan kunci.
2. Tahap penanda tanganan.
3. Tahap verifikasi.

3.4 Perancangan

Pada tahap ini dilakukan perancangan aplikasi yang akan digunakan untuk implementasi enkripsi text menggunakan algoritma ECDSA. Tahapan-tahapan adalah sebagai berikut:

1. Perancangan interface

   Aplikasi Perancangan *interface* aplikasi bertujuan untuk memperlihatkan bagaimana tampilan aplikasi yang akan dibangun.
2. Implementasi kedalam bahasa pemrograman

   Pada tahapan ini dilakukan tahapan pemrograman aplikasi dengan menggunakan aplikasi pendukung seperti *web browser.*

3.5 Implementasi

Setelah dilakukan perancangan aplikasi, maka akan dilakukan tahap implementasi. Implementasi merupakan tahap dimana aplikasi siap untuk dioperasikan sesuai dari hasil analisis dan perancangan yang telah dilakukan, sehingga akan diketahui apakah aplikasi yang dirancang benar-benar dapat menghasilkan tujuan yang ingin dicapai. Adapun spesifikasi *hardware* dan *software* yang akan digunakan pada implementasi ini adalah:

1. Perangkat Lunak (*Software*)

   Sistem Operasi : Windows 10

   Bahasa Pemrograman : *PHP*

   Tool : sublime text 3

2. Perangkat Keras (*Hardware*)

   Processor : Intel core i5

   Memori (RAM) : 4 GB

   Harddisk : 80 GB

3.6 Pengujian

Setelah tahap implementasi, selanjutnya akan dilakukan pengujian terhadap aplikasi yang telah dibangun. Dengan demikian dapat diketahui tingkat keberhasilan aplikasi, apakah telah mencapai tujuan yang diharapkan. Pengujian yang dilakukan penelitian ini yaitu pengujian penandatanganan dan proses verifikasi dokumen yang telah diberi tandatangan digital (*digital signature*).

3.7 Kesimpulan dan Saran

Tahapan terakhir pada penelitian ini adalah memberikan kesimpulan dan saran. Kesimpulan berisi hasil pengujian yang telah dilakukan pada penelitian ini yaitu penerapan *Elliptic Curve Digital Signature Algorithm* (ECDSA) pada *Digital Signature* untuk pengamanan dokumen. Serta memberikan saran terhadap topik terkait penelitian sehingga dapat menghasilkan penelitian terbaru.

BAB VI
PENUTUP

6.1 Kesimpulan

Berdasarkan dari tahap implmentasi hingga ke tahap pengujian sebelumnya dapat ditarik kesimpulan bahwa

1. Implementasi algoritma ECDSA (*Elliptic Curve Digital Signature Algorithm*) pada pengamanan surat wasiat berhasil dilakukan.
2. Sistem yang diimlementasikan dapat memenuhi standar keamanan *digital signature* yaitu otentikasi, integritas dan non-repudiation.

6.2 Saran

Terdapat beberapa saran terkait penelitian ini apabila ada penelitian lebih lanjut untuk pengembangan penelitian yang sudah diakukan

1. Mengembangkan aplikasi berbasis android agar lebih mudah diakses dimanapun dan kapanpun.
2. Menerapkan pada dokumen dengan berbagai format, seperti *doc*, *docx*, *txt*, *xls*, *ppt*, dan lain-lain.

DAFTAR PUSTAKA

Ahmaddul Hadi. (2013). Rancang Bangun Sistem Pengamanan Dokumenpada Sistem Informasi Akademik Dengan Menggunakan Digital Signature. *Jurnal Teknologi Dan Pendidikan*, *6*(2), 106–118.

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

Indrajit Eko, R. (2011). *Pengantar Konsep Keamanan Informasi di Dunia Cyber* (2nd ed.). preinexus.

Kusuma, V., Matematika, J., & Matematika, F. (2014). *Elliptic Curve dan Implementasinya pada Algoritma Tanda Tangan Digital*. *3*(2), 3–6.

Lindquist, T. E., Diarra, M., & Millard, B. R. (2004). A Java Cryptography Service Provider Implementing One-Time Pad. *Journal Arizona State University East*, *00*(C), 1–6.

Mahmudi, A., Mantja, S. N., & Rozikin, A. (2016). *Aplikasi Kriptografi dan Steganografi Menggunakan Metode Least Significant Bit (LSB) dan One Time Pad (OTP)*. *8*(1), 1–6.

Menezes, A. J., Oorschot, P. C. Van, & Vanstone, S. A. (1996). *HandBook Of Applied Cryptography*. CRC Press.

Munir, R. (2006). *Kriptografi*. Informatika.

Muttaqin, Z. (2010). *Pembuatan Aplikasi Enkripsi Menggunakan Metode Advance Encryption Standard dan Riverst Shamir Adleman : Studi Kasus CV. Maharta Mandiri Promo*. Uin Syarif Hidayatullah.

Purnama, R. D. O., & Lestiawan M.Kom, H. (2014). Algoritma Kriptografi Metode Operasi Cipher Block Chaining (CBC) Dan Steganografi Metode End Of File(EOF). *Universitas Dian Nuswantoro*, *1*(1), 1–11.

Putra, D. A. (2018). *Hati-hati, ini bahaya mengintai penggunaan tanda tangan digital palsu*. https://www.merdeka.com/uang/hati-hati-ini-bahaya-mengintai-penggunaan-tanda-tangan-digital-palsu.html

Rahardjo, B. (2002). *Keamanan Sistem Informasi Berbasis Internet* (5th ed., Vol.

5). PT Insan Infonesia - Bandung & PT INDOCISC - Jakarta.

Ramayanti, D. (2007). *APLIKASI DIGITAL SIGNATURE SEBAGAI AUTENTIKASI PADA KARTU TANDA PENDUDUK(KTP)*. *Mcdm*, 7–10.

Schneier, B. (1996). *Applied Cryptography Protocols*. John Wiley & Sons, Inc.

Sejati, A. (2007). Studi dan Perbandingan Steganografi Metode EOF (End of File) dengan DCS (Dynamic Cell Spreading). *Jurnal Strategi Algoritmik*, *1*(2), 6.

Triwinarko, A. (2005). *Elliptic Curve Digital Signature Algorithm (ECDSA)*. 1–6. https://doi.org/10.17487/RFC6605

Wahyuni, A. (2011). *Aplikasi Kriptografi Untuk Pengamanan Data E-Dokumen Dengan Metode Hybrid : Biometrik Tandatangan Dan Dsa (Digital Signature Algorithm)*. 1–150. http://core.ac.uk/download/pdf/11728847.pdf

DAFTAR RIWAYAT HIDUP

DATA PRIBADI		
	Nama	Joni Saputra
	Tempat / Tanggal Lahir	Perawang, 13 Juni 1994
	Jenis Kelamin	Laki-Laki
	Status Pernikahan	Belum Menikah
	Anak Ke-	2
	Tinggi Badan	175 cm
	Berat Badan	58 kg
	Kebangsaan	Indonesia
ALAMAT		
Alamat		BTN Cendrawasih, Perawang
Nomor HP		082387905420
Email		joni.saputra@students.uin-suska.ac.id
RIWAYAT PENDIDIKAN		
Tahun 2000-2001		TK YPLP PGRI
Tahun 2001-2007		SDN 005 Tualang
Tahun 2007-2010		SMPN 1 Tualang
Tahun 2010-2013		SMK YAMATU