Penerapan ECDSA Untuk Menjamin Keabsahan Dokumen Transkrip Nilai

Ade Surya Handika - 13518007
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail : 13518007@std.stei.itb.ac.id

***Abstract*—Surat transkrip nilai adalah surat kumpulan nilai yang didapatkan selama masa pembelajaran, baik di sekolah ataupun di perkuliahan. Surat transkrip nilai sering digunakan sebagai salah satu syarat pendaftaran beasiswa hingga lamaran pekerjaan. Untuk memastikan konten nilai pada dokumen transkrip asli dan tidak diubah, perlu dilakukan sebuah verifikasi. Salah satu cara menjamin keabsahan suatu dokumen adalah menggunakan Digital Signature. ECDSA atau Elliptical Curve Digital Signature Algoritma adalah suatu algoritma tanda tangan digital yang memanfaatkan sebuah kurva eliptik. Dengan Penerapan ECDSA pada dokumen transkrip nilai, diharapkan keabsahan dokumen dapat terjaga dari tindak pemalsuan dokumen.**

Kata Kunci; ECDSA, transkrip nilai, digital signature

I. Pendahuluan

Dewasa ini, penggunaan dokumen digital dalam pengiriman formulir ataupun dokumen untuk kepentingan pendaftaran sudah sering dilakukan. Penggunaan dokumen digital digunakan untuk memudahkan dalam pengiriman berkas informasi yang dibutuhkan agar lebih cepat dan mudah tanpa perlu terbatas jarak. Dokumen digital akan menyimpan informasi dalam bentuk file digital.

Pada pengiriman dokumen digital dilakukan dengan menggunakan media digital, meskipun dokumen digital yang dikirim merupakan dokumen penting, informasi yang ada pada didalamnya tidak dapat dipastikan keabsahannya. Ada kemungkinan pihak-pihak yang tidak bertanggung jawab memalsukan isi dokumen untuk kepentingan pribadi. Proses pemalsuan bisa dengan mengubah, menghapus, atau menambah isi dokumen digital. Salah satu dokumen digital yang mungkin dipalsukan adalah transkrip nilai.

Transkrip Nilai adalah dokumen sertifikat yang berisi kumpulan nilai yang merupakan hasil capaian seseorang dalam masa pembelajaran. Transkrip nilai merupakan gambaran capaian seseorang pada saat melakukan pembelajaran. Transkrip nilai digunakan untuk kualifikasi pada saat pendaftaran sekolah ataupun lamaran kerja. Dengan demikian, informasi nilai di dalam transkrip sangat penting. Pemalsuan isi informasi pada transkrip bisa terjadi jika tidak ada proses verifikasi pada dokumen transkrip. Salah satu cara verifikasi dokumen digital yaitu dengan menggunakan digital signature.

Digital signature atau tanda tangan digital bukanlah suatu tulisan tangan yang dibuat dalam bentuk digital. Digital signature adalah suatu nilai kriptografis yang bergantung pada isi pesan dan kunci yang digunakan. Salah satu implementasi dari tanda tangan digital yaitu menggunakan kurva eliptik pada tanda tangan digital, algoritma ini dinamakan dengan ECDSA (Elliptic Curve Digital Signature Algorithm).

Pada makalah ini, penulis mengusulkan penerapan ECDSA untuk menjamin keabsahan dari sebuah dokumen transkrip nilai. Dengan penggunaan ECDSA pada dokumen transkrip nilai, harapannya pengirim dan penerima dokumen transkrip nilai akan merasa aman dan terjamin keaslian dokumennya.

II. Dasar Teori

A. Tanda Tangan Digital

Tanda tangan digital (digital signature) merupakan tanda tangan yang digunakan untuk data digital. Tanda tangan digital bukan tulisan tangan dalam bentuk digital. Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Tanda tangan digital berbeda-beda pada setiap dokumen. Tanda tangan digital digunakan untuk menyelesaikan aspek *autentikasi*, keaslian pesan dan anti penyangkalan.

Tanda tangan digital mempunyai karakteristik sebagai berikut:

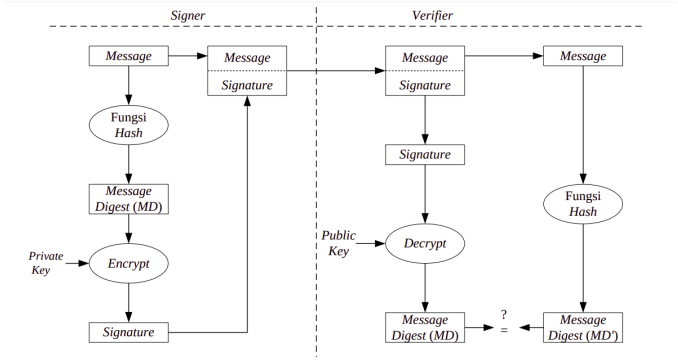
1. Tanda-tangan adalah bukti yang otentik.
2. Tanda tangan tidak dapat dilupakan.
3. Tanda-tangan tidak dapat dipindah untuk digunakan ulang.
4. Dokumen yang telah ditandatangani tidak dapat diubah.
5. Tanda-tangan tidak dapat disangkal.

Ada dua cara dalam menandatangani pesan, pertama dengan mengenkripsi pesan. Enkripsi pesan dilakukan dengan algoritma kriptografi kunci simetris, yaitu algoritma dengan nilai kunci sama untuk proses enkripsi dan dekripsi pesan. Cara tanda tangan yang kedua yaitu dengan menggunakan kombinasi fungsi hash dan algoritma kriptografi kunci publik.

Pada tanda tangan digital dengan enkripsi pesan dengan algoritma kunci simetris, pengirim dan pengirim pesan harus memiliki kunci yang sama. Cara ini dapat memberikan solusi autentikasi, akan tetapi belum ada mekanisme anti -penyangkalan. Selain itu, isi pesan akan terenkripsi dan informasi didalamnya tidak dapat dibaca.

Selanjutnya adalah dengan kombinasi fungsi hash dan algoritma kunci publik. Fungsi hash merupakan fungsi enkripsi satu arah, artinya pesan yang dienkripsi tidak akan bisa di dekripsi. Sedangkan algoritma kunci publik adalah algoritma kriptografi yang menggunakan dua buah kunci berbeda pada proses enkripsi dan dekripsi. Kunci publik digunakan untuk mengenkripsi pesan dan kunci privat digunakan untuk dekripsi pesan. Pada cara ini, isi pesan masih dapat dibaca atau tidak terenkripsi. Pada makalah ini, penulis menggunakan cara yang kedua karena informasi pada dokumen harus dapat terbaca meskipun dilakukan tanda tangan digital.

Berikut ini alur menggunakan metode fungsi hash dan kriptografi kunci publik.



Gambar 1.1. Proses Tanda Tangan Digital dengan Kombinasi Fungsi Hash dan Algoritma Kunci Publik

B. ECC dan ECDSA

ECC (Elliptic Curve Cryptography) adalah suatu pendekatan implementasi algoritma kriptografi kunci publik. ECC memanfaatkan elliptic curve pada suatu medan finite. Proses enkripsi dan dekripsi ECC dilakukan pada titik-titik yang terletak di kurva eliptik pada suatu ruang Gallois p, di mana p adalah suatu bilangan prima. Kurva eliptik pada algoritma akan memiliki persamaan berikut:

$$y^2 = x^3 + ax + b \bmod p$$

dengan parameter a, b, dan p tersebut merupakan parameter dari suatu elliptic curve.

ECC merupakan perluasan untuk algoritma algoritma kriptografi yang lain, misalnya:

1. ECDSA (Elliptic Curve Digital Signature Algorithm).
2. ECDH (Elliptic Curve Diffie-Hellman).
3. ECEG (Elliptic Curve ElGamal).

ECDSA (Elliptic Curve Digital Signature Algorithm) adalah suatu implementasi tanda tangan digital yang memanfaatkan elliptic curve cryptography. Terdapat dua bagian utama pada ECDSA, yaitu sign dan verify signature,

Pada ECDSA terdapat beberapa parameter lain sebagai tambahan parameter elliptic curve yang digunakan (a, b, p), yaitu:

1. G, elliptic curve base point, yang menjadi generator subgroup pada elliptic curve yang dipakai.
2. n yang merupakan orde dari elliptic curve. Hubungan antara n, G, dan O (elemen identitas) dapat dinyatakan dalam persamaan $n \times G = O$
3. d yang merupakan private key yang digunakan dalam
4. Q yang merupakan public key yang digunakan dalam ECDSA. Sebagai catatan hubungan antara d, Q, dan G dapat dinyatakan dalam persamaan $d \times G = Q$.

Tahapan untuk melakukan pembangkitan signature adalah sebagai berikut:

1. Hitung nilai hash h dari pesan yang ingin dibangkitkan signaturenya. Fungsi hash yang digunakan bebas asalkan aman secara kriptografi, misal SHA-256.
2. Hitung nilai z yaitu x most significant bit dari h dengan x adalah panjang bit dari n.
3. Ambil suatu angka k dari rentang $1 \leq k \leq n - 1$
4. Hitung $kG = (x1, y1)$.
5. Hitung $r = x1 \bmod n$. Jika $r \neq 0$ lanjut ke langkah berikutnya. Jika tidak, kembali ke langkah nomor 3.
6. Hitung $s = k^{-1}(z + dr) \bmod n$. Jika $s \neq 0$ lanjut ke langkah berikutnya. Jika tidak, kembali ke langkah nomor 3.
7. Didapat signature dari pesan masukan adalah pasangan nilai (r, s).

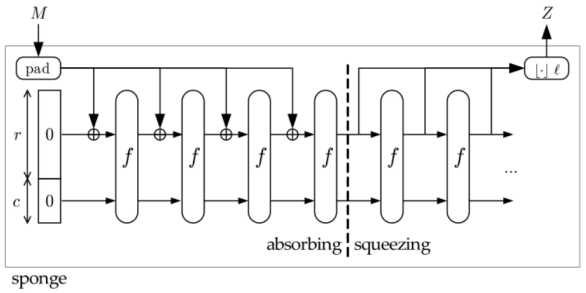
Tahapan untuk melakukan verifikasi signature adalah sebagai berikut:

1. Cek apakah $1 \leq s, r \leq n - 1$. Jika terpenuhi, lanjut ke langkah berikutnya. Jika tidak, signature tidak valid.
2. Hitung nilai z dengan metode yang sama dengan langkah 1 hingga 2 pada proses pembangkitan signature.
3. Hitung nilai $s_{inv} = s^{-1} \bmod n$.
4. Hitung nilai $u_1 = z s_{inv} \bmod n$ dan $u_2 = r s_{inv} \bmod n$.
5. Hitung nilai $X = u_1 G + u_2 Q$. Jika X adalah titik identitas O, signature tidak valid. Jika bukan, lanjut ke langkah berikutnya.
6. Misal (x_1, x_2) adalah koordinat titik X. Signature valid jika dan hanya jika $r = x_1 (\bmod n)$.

C. *Fungsi Hash SHA-3*

Fungsi Hash SHA-3 atau yang lebih dikenal sebagai Keccak merupakan fungsi hash yang dikembangkan oleh Guido Breton, Joan Daemen, Michaël Peeters, dan Gilles Van Assche. Keccak dipublikasikan pertama kali pada tahun 2015. Fungsi hash keccak dapat digunakan untuk melakukan autentikasi, enkripsi, dan sebagai pembangkit bilangan acak.

Pada proses pembangkitan bit, keccak menggunakan mekanisme sponge construction. Data akan diserap ke dalam sponge, kemudian diperas untuk menghasilkan bit-bit message digest. Algoritma keccak akan menghasilkan message digest sepanjang 256 bit. Berikut adalah skema dari algoritma Keccak:



Gambar 1.1. Skema algoritma keccak

Secara umum terdapat tiga proses pada algoritma keccak, yaitu praproses, absorb, dan squeezing. Berikut ini adalah langkah-langkah pada saat pra proses:

- Misalkan panjang digest yang diinginkan adalah d bit.
- Pertama, pesan M ditambah dengan bit-bit pengganjal (padding) menjadi string P sehingga habis dibagi dengan r atau n = length(P)/r
- Selanjutnya, P dipotong menjadi blok-blok Pi berukuran r-bit.
- Kemudian, b-bit dari peubah status (state) S diinisialisasi menjadi nol dan konstruksi spons berlangsung dalam dua fase: yaitu absorb dan squeezing.

Pada fase *absorb (penyerapan)* dilakukan proses berikut ini:

- Untuk setiap blok masukan Pi berukuran r-bit, XOR-kan dengan r-bit pertama dari state S, lalu hasilnya dimasukkan ke dalam fungsi permutasi f untuk menghasilkan state baru S.
- Bila semua blok masukan selesai diproses, konstruksi spons beralih ke fase pemerasan (squeezing).

Selanjutnya Pada fase *squeezing(pemerasan)* dilakukan proses sebagai berikut:

- Message digest akan disimpan di dalam Z.
- Inisialisasi Z dengan string kosong (null string).
- Selagi panjang Z belum sama dengan d, r-bit pertama dari state S disambungkan (append) ke Z.
- Jika panjang Z masih belum sama dengan d, masukkan ke dalam fungsi permutasi f menghasilkan state baru S.

D. *Transkrip Nilai*

Surat transkrip nilai adalah surat kumpulan nilai semua mata kuliah mulai dari semester 1 hingga semester terakhir yang telah ditempuh selama perkuliahan. Surat transkrip nilai sering digunakan sebagai salah satu syarat pendaftaran beasiswa hingga lamaran pekerjaan.

Transkrip nilai berbeda dengan rapor. Raport biasanya terdiri dari berbagai lembar sedangkan transkrip biasanya hanya satu lembar. Transkrip nilai didapatkan ketika seseorang lulus dari suatu sekolah atau perguruan tinggi.

III. Rancangan dan Analisis

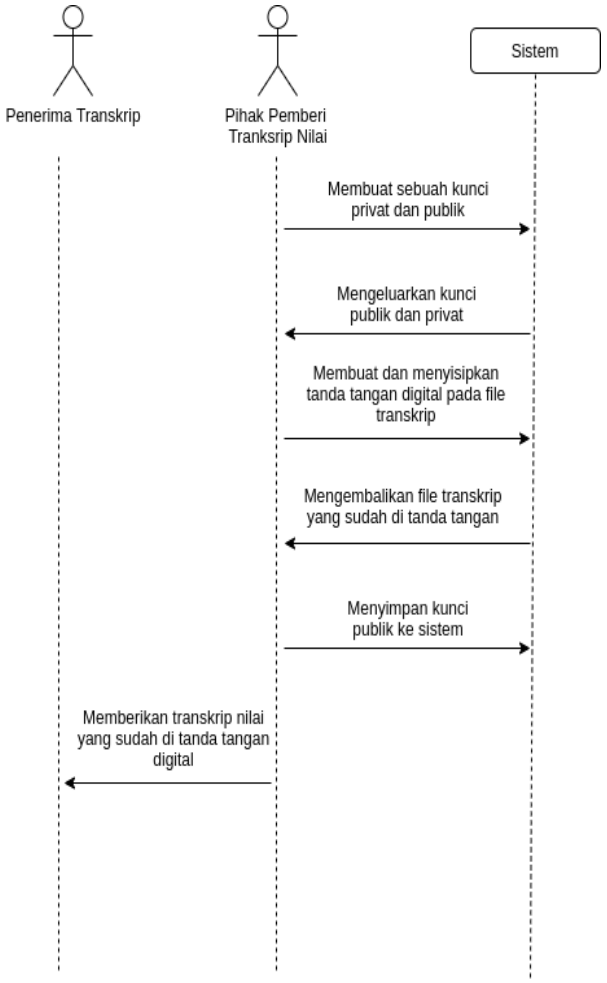
A. *Rancangan Umum*

Implementasi ECDSA terdiri dari dua buah proses, yaitu proses signing dan proses verifikasi. Pada proses signing, dokumen akan di tanda tangan dengan sebuah kunci privat milik pihak pemberi transkrip nilai seperti sekolah atau perguruan tinggi. Nilai kunci privat dijaga kerahasiaannya. Sedangkan pada proses verifikasi, tanda tangan digital akan diperiksa berdasarkan kunci publik milik pihak pemberi transkrip. Kunci publik dapat dibagikan secara luas ke pihak luar agar transkrip nilai dapat di verifikasi.

Dengan demikian, dibutuhkan suatu sistem yang dapat melakukan tanda tangan digital sekaligus menyimpan daftar kunci publik dari pihak pemberi transkrip. Sistem akan melabeli masing-masing kunci publik dengan nama dari perguruan tinggi atau sekolah yang melakukan tanda tangan digital pada sistem. Pelabelan diperlukan untuk mengidentifikasi pemilik kunci publik pada sistem. Dengan adanya pelabelan, pengguna yang akan melakukan verifikasi pada dokumen dapat dengan mudah memilih kunci publik mana yang akan digunakan.

Kemudian, kunci privat tidak perlu disimpan pada sistem dikarenakan pada saat proses verifikasi pihak luar tidak membutuhkan kunci privat. Selain itu, kunci privat hanya akan digunakan oleh pihak yang melakukan tanda tangan sehingga kerahasiaan kunci privat sangat diperlukan untuk memastikan tidak adanya pihak lain yang menyamar menjadi pihak tertentu untuk membuat dokumen palsu yang ditandatangani pada sistem.

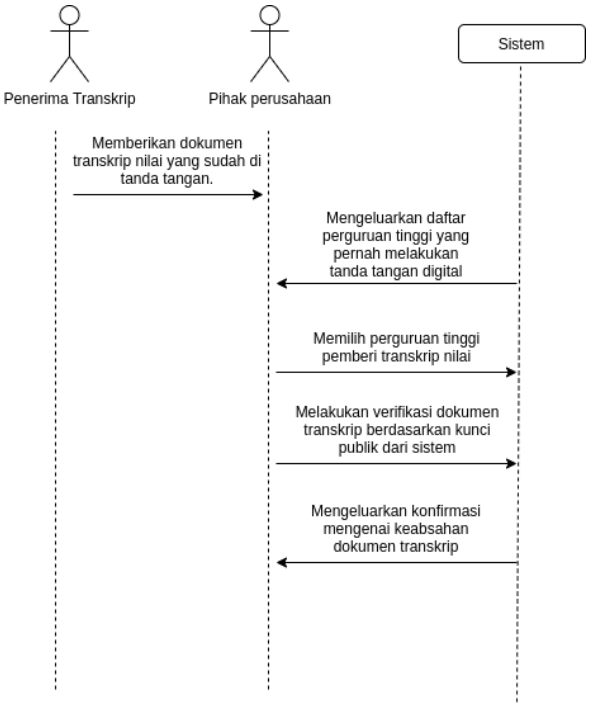
Berikut adalah skema dari proses tanda tangan digital pada transkrip nilai yang dilakukan oleh pihak sekolah



Gambar 3.1 Skema Tanda Tangan digital

Mula-mula pihak pemberi transkrip nilai akan membuat sebuah pasangan kunci publik dan kunci privat. Kemudian, kunci privat digunakan untuk menandatangani dokumen transkrip nilai yang asli. Setelah di tanda tangan, dokumen transkrip nilai dapat diberikan kepada penerima transkrip nilai. Transkrip yang sudah ditandatangani secara sah sudah dapat digunakan untuk keperluan pendaftaran atau lamaran pekerjaan. Pihak penerima transkrip hanya perlu memberikan transkrip nilai kepada pihak perusahaan. Setelah itu, proses verifikasi dokumen dilakukan oleh pihak perusahaan..

Berikut adalah skema verifikasi transkrip nilai yang dilakukan oleh pihak perusahaan dengan sistem



Gambar 3.2 Skema Verifikasi Tanda Tangan digital

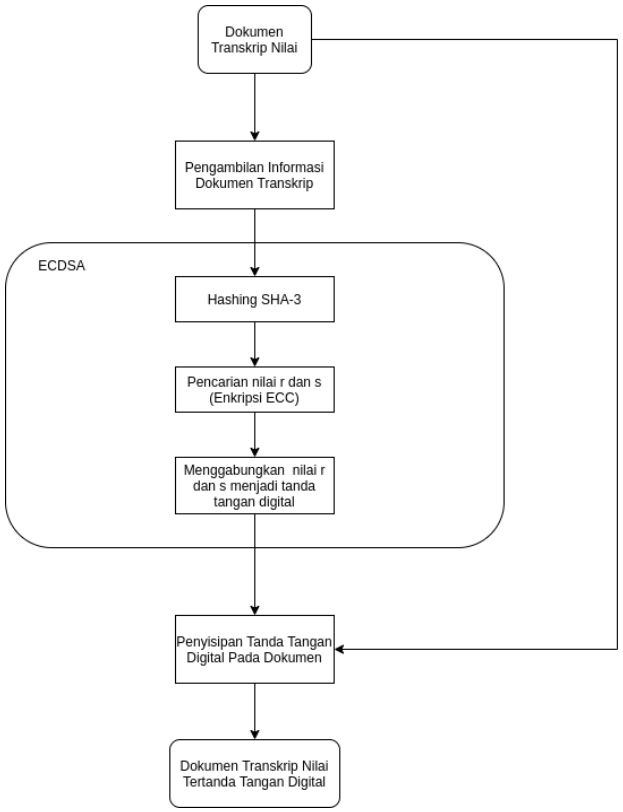
Dapat dilihat pada gambar 3.2, pihak perusahaan dapat langsung memverifikasi dokumen transkrip nilai ke sistem berdasarkan label perguruan tinggi yang dipilih pada sistem. Dokumen transkrip nilai akan di verifikasi dengan kunci publik milih pihak perguruan tinggi yang sudah dilabeli pada sistem sehingga keabsahan dokumen transkrip nilai dapat dicek untuk mengetahui dokumen yang diberikan pelamar adalah dokumen asli atau palsu. Selain itu, dengan verifikasi ini dapat menjaga keaslian informasi pada transkrip nilai dikarenakan perubahan sedikit pada isi transkrip akan membuat proses verifikasi gagal.

B. Analisis Proses Pembangkitan Kunci

Pada makalah ini, pembuatan kunci publik dan privat akan menggunakan Elliptic Curve Cryptography. Pertama akan dipilih sebuah nilai tetap dari konstanta G untuk titik dasar orde bilangan prima pada kurva dan sebuah nilai n untuk orde perkalian titik G. Pembangkitan kunci privat d akan diperoleh dengan mencari sebuah bilangan bulat secara acak. Setelah itu, dilakukan perkalian antara titik G dengan kunci privat d untuk menghasilkan kunci publik Q yang berupa titik. Kunci publik akan disimpan didalam sistem sedangkan kunci privat akan disimpan oleh pihak pembuat transkrip dan dirahasiakan nilainya. Nilai konstanta G dan n akan selalu sama pada sistem sehingga kurva eliptik yang digunakan pada proses tanda tangan dan verifikasi tidak berubah-ubah.

C. Analisis Proses Signing

Proses signing dilakukan dengan menggunakan sebuah kunci publik. Sistem akan menerima sebuah file dokumen transkrip nilai dan melakukan proses tanda tangan seperti berikut



Gambar 3.1 Skema Tanda Tangan digital

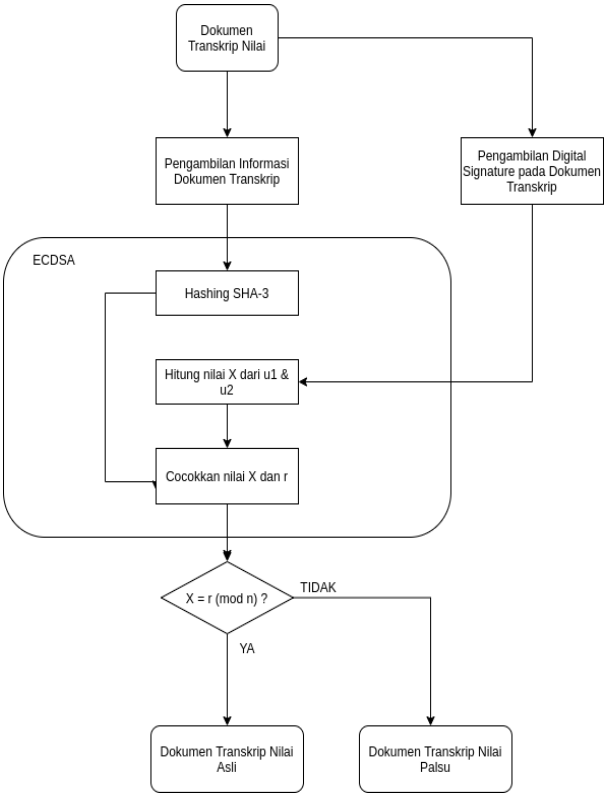
Sistem akan membaca isi dari dokumen transkrip nilai yang berupa kumpulan bit-bit pada dokumen. Informasi bit akan dimasukkan ke algoritma SHA-3 untuk diproses menjadi sebuah nilai hash sepanjang 256 bit. Hasil dari hash adalah sebuah message digest (MD).

Selanjutnya, MD akan diproses oleh algoritma eliptik untuk mencari nilai r dan s berdasarkan perhitungan yang sudah dijelaskan sebelumnya. Hasil perhitungan r dan s akan digabungkan menjadi sebuah tanda tangan digital dengan panjang 1024 bit.

Bit-bit akan diubah kedalam representasi hex untuk disisipkan kedalam dokumen transkrip nilai. Penyisipan digital signature bisa langsung pada isi dokumen atau bisa dengan melakukan steganografi pada dengan menyisipkan bit-bit pada akhir bit dokumen. Pada rancangan kali ini, bit-bit akan disisipkan pada akhir dokumen dengan sebuah penanda (flag) yang memisahkan bit dokumen dengan bit digital signature.

D. Proses Verifikasi

Proses Verifikasi tanda tangan digital dilakukan dengan menggunakan kunci publik pada sistem. Pemilih perusahaan akan memilih kunci publik yang sudah dilabeli oleh sistem yang kemudian akan digunakan pada proses verifikasi dokumen. Berikut ini adalah skema proses verifikasi tanda tangan digital pada dokumen transkrip nilai.



Mula-mula sistem akan memisahkan antara bit-bit dokumen dan bit-bit tanda tangan digital. Kemudian untuk dokumen akan dimasukkan kedalam fungsi SHA-3 untuk menghasilkan sebuah message digest.

Selanjutnya, digital signature pada dokumen transkrip nilai akan diproses dengan algoritma kurva eliptik untuk mencari nilai dari $u_1$dan u_2. Setelah diperoleh nilai u1 dan u2, dicari nilai X berdasarkan persamaan

$$X = u_1 G + u_2 Q$$

Hasil dari message digest dan juga dekripsi tanda tangan dengan kurva eliptik akan dibandingkan nilainya.

Jika nilai message digest sama dengan nilai dekripsi tanda tangan kurva eliptik, maka dokumen transkrip nilai dinyatakan asli. Jika berbeda, maka dokumen transkrip nilai dinyatakan palsu.

IV. KESIMPULAN

Dari sistem yang telah dirancang, didapatkan kesimpulan sebagai berikut :

1. Sistem verifikasi keabsahan dokumen digital dapat dibuat dengan memanfaatkan teori tanda tangan digital dan kriptografi kurva eliptik.
2. Dengan sistem yang dirancang, pihak perusahaan yang menggunakan transkrip nilai sebagai dokumen pada penilaian dapat mengetahui keaslian dari isi dokumen transkrip tersebut.

3. Pihak perusahaan dapat mengetahui ketika terjadi pemalsuan pada dokumen transkrip nilai sehingga bisa dijadikan pertimbangan dalam proses penerimaan.

V. SARAN

Penerapan Tanda Tangan Digital tidak hanya dilakukan dengan menggunakan Algoritma Kurva Eliptik. Masih banyak alternatif algoritma lain dan juga alternatif solusi yang serupa, Kedepannya, solusi dapat dikembangkan lebih lanjut pada beberapa menggunakan algoritma kunci public yang lain seperti RSA dan AES, penggunaan algoritma fungsi hash yang lain seperti MD5.

UCAPAN TERIMAKASIH

Penulis ingin berterima kasih kepada Tuhan yang Maha Esa atas berkat dan anugerah-Nya sehingga penulis dapat memiliki kesempatan untuk membuat sebuah makalah yang berkaitan dengan penerapan kriptografi pada kehidupan sehari-hari. Penulis juga ingin berterima kasih kepada Institut Teknologi Bandung yang telah memfasilitasi kegiatan belajar mengajar kami. Penulis berterima kasih kepada dosen khususnya kepada bapak Rinaldi Munir selaku dosen pengajar IF-4020 Kriptografi yang telah mengajari penulis mengenai Kriptografi. Dan yang terakhir, penulis berterima kasih kepada keluarga dan teman teman yang mendukung dalam pembuatan makalah ini.

REFERENSI

[1] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: Fungsi SHA-3 (Keccak)

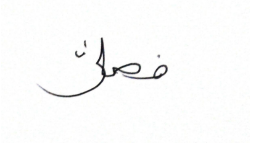
[2] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: Tanda-tangan Digital

[3] Munir, Rinaldi. 2021. Slide Kuliah IF4020 Kriptografi: Algoritma ECC

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Desember 2021



Ade Surya Handika
13518007