Implementasi Tanda Tangan Digital ECDSA untuk *Invoice* pada Platform *E-Commerce*

Ferdy Santoso / 13517116
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517116@std.stei.itb.ac.id

Abstraksi—Informasi telah tersebar secara cepat menggunakan internet. Salah satu informasi yang dikirimkan melalui internet adalah *invoice* pada suatu platform *e-commerce*. Data *invoice* tersebut dapat dengan mudah ditangkap oleh seseorang dan diubah isinya. Dibutuhkan suatu mekanisme yang dapat menjaga keamanan data tersebut. Algoritma ECDSA adalah suatu mekanisme untuk memberikan tanda tangan digital pada suatu data, termasuk data *invoice*. Algoritma ECDSA dapat digunakan untuk memenuhi prinsip-prinsip kriptografi untuk menjaga keamanan data *invoice* yakni Otentikasi, Integritas Data, dan Anti-Penyangkalan. Dengan dipenuhinya prinsip-prinsip kriptografi tersebut penggunaan ECDSA dapat lebih menjaga keamanan data.

Kata Kunci—kriptografi, tanda tangan digital, ECDSA, *Invoice, E-commerce*.

I. Pendahuluan

Pada era digital informasi telah tersebar secara luas dan mudah. Seluruh informasi terbagikan melalui internet dan semua orang dapat mengirim dan menerima informasi tersebut. Informasi tersebut dapat berupa publik maupun rahasia. Informasi yang bersifat publik maupun rahasia perlu dijaga keamanannya dan integritasnya.

E-commerce merupakan sebuah platform digital yang dapat digunakan untuk melakukan jual beli barang secara *online*. Informasi perjual-belian barang akan dikirimkan dan diterima melalui internet. Salah satu informasi tersebut adalah dalam bentuk *invoice*. *Invoice* berisi informasi perjual-belian barang yang terjadi antara penjual dan pembeli pada platform *E-commerce* tersebut.

Informasi *invoice* tersebut bersifat rahasia dan tidak boleh diketahui pihak lain selain penjual dan pembeli. Namun, selain rahasia, *invoice* juga harus memiliki integritas yang kuat. Integritas ini harus dijaga agar ketika informasi dikirimkan melalui internet dan ada yang mengintersepsi pesan dan mengubahnya, pesan akan dapat dideteksi bahwa isinya telah diubah.

Penjagaan integritas pesan dapat dilakukan dengan menggunakan tanda tangan digital. Tanda tangan digital merupakan sebuah cara untuk memberi tanda pada pesan yang akan dikirimkan yang dapat digunakan untuk memastikan validitas pesan dan validitas pengirim pesan. Salah satu algoritma tanda tangan digital yang digunakan pada makalah ini adalah ECDSA.

II. Landasan Teori

A. Tanda Tangan Digital

Tanda tangan digital adalah sebuah mekanisme autentikasi yang dapat digunakan oleh seorang pengirim pesan untuk menambahkan kode unik di akhir pesan mereka yang dapat digunakan oleh pengirim pesan dan penerima pesan untuk memastikan bahwa pesan terkirim dengan keamanan dan integritas yang baik. Ada 3 prinsip kriptografi yang mampu dipenuhi oleh tanda tangan digital, yakni:

1. Otentikasi (*Authentication*)

Autentikasi berguna untuk memastikan bahwa pengirim pesan berasal dari pihak yang tepat dan bukan dari pihak yang salah. Autentikasi sangatlah penting ketika ada komunikasi melalui sebuah jaringan internet karena jaringan internet dapat disadap oleh siapapun pada saat terjadi pertukaran data.

2. Keaslian Pesan (*Data Integrity*)

Keaslian pesan merujuk kepada kemampuan untuk melindungi data yang dikirimkan dari perubahan-perubahan yang mungkin terjadi baik yang tidak disengaja maupun yang disengaja, misalkan jika dilakukan oleh pihak lain. Data yang diterima haruslah benar-benar data yang dikirimkan oleh pengirim dan bukan data yang telah diubah, sehingga keaslian pesan ini penting dijaga.

3. Anti-penyangkalan (*non-Repudiation*)

Anti-penyangkalan memberikan keamanan dari penyangkalan bahwa suatu data atau pesan berasal dari pihak tertentu. Sehingga jika suatu pengirim mengirimkan sebuah pesan kepada seorang penerima, maka penerima dapat dengan yakin mengetahui bahwa pesan tersebut berasal dari pengirim tersebut.

B. Algoritma ECDSA

Elliptic Curve Digital Signature Algorithm (ECDSA) merupakan sebuah algoritma tanda tangan digital (digital signature) yang berfungsi untuk mengecek apakah pesan yang dikirimkan dari pengirim ke penerima merupakan pesan yang sesungguhnya dan tidak diubah nilainya. Tanda tangan digital

sangatlah berguna terutama di era digital seperti di jaman ini. ECDSA merupakan sebuah algoritma tanda tangan digital yang menggunakan konsep-konsep Elliptic Curve Cryptography (ECC). ECDSA memiliki operasi-operasi titik dasar yang harus diimplementasikan seperti penjumlahan titik, penggandaan titik dan perkalian titik yang akan dijelaskan lebih mendetail pada bagian implementasi. Secara garis besar ada 3 tahapan yang harus dipenuhi di dalam algoritma ECDSA: Key Generation, Sign, dan Verify. Masing-masing tahapan akan dijelaskan satu per satu.

1. Key Generation

Pada Tahap Key Generation dilakukan pembangkitan kunci publik dan kunci privat. Kunci privat adalah sebuah bilangan bulat acak yang akan digunakan untuk melakukan sign pada pesan yang akan dikirim. Kunci Publik merupakan sebuah titik koordinat (x,y) yang akan digunakan untuk melakukan verify pada pesan yang diterima.

2. Sign

Pada Tahap Sign dilakukan tahap pembentukan tanda tangan digital dari kunci privat yang telah dibangkitkan sebelumnya. Selain menggunakan kunci privat, pesan akan dilakukan hash terlebih dahulu, dalam pengerjaan makalah ini fungsi hash yang akan digunakan adalah SHA-3 atau yang biasa disebut dengan istilah Keccak.

3. Verify

Pada Tahap Verify dilakukan tahap verifikasi tanda tangan digital. Verifikasi dilakukan dengan menggunakan kunci publik yang telah dimiliki oleh penerima pesan sebelumnya. Sama dengan tahap sign, pesan akan dilakukan hash terlebih dahulu dengan menggunakan fungsi hash SHA-3 (Keccak) sebelum dilakukan pemrosesan dengan kunci publik. Jika hasil verifikasi valid, maka itu berarti tidak ada bagian dari pesan yang diubah, namun jika hasil verifikasi tidak valid, maka itu berarti ada bagian dari pesan yang diubah.

penjelasan lebih detail mengenai tahapan-tahapan ini akan dijelaskan lebih lanjut pada bagian implementasi.

C. Invoice pada Platform *E-Commerce*

Invoice merupakan sebuah kumpulan informasi mengenai sebuah pembelian yang dibentuk oleh sistem pada saat terjadi aktivitas jual-beli. Pada platform *e-commerce invoice* sangatlah penting untuk disimpan di dalam basis data informasi mengenai penjual, pembeli, barang yang dibeli, jumlah, harga, dan masih banyak lagi. *Invoice* yang dikirimkan ke basis data dari pembelian pengguna haruslah aman dan tidak boleh sampai diketahui atau bahkan diubah oleh pihak lain yang tidak berwenang. Untuk menjaga kerahasiaan *invoice* dapat digunakan proses enkripsi pesan, namun pada makalah kali ini akan lebih difokuskan pada aspek autentikasi, integritas data, dan anti-penyangkalan, sehingga akan digunakan tanda tangan digital untuk menjaga keamanan *invoice*.

III. Implementasi

A. Implementasi Algoritma ECDSA

ECDSA yang telah diimplementasikan memiliki konstruksi sebagai berikut: 2 Kelas yakni Kelas Point dan Kelas Curve; 3 Operasi matematis titik yakni add, double, dan multiply; dan 3 metode utama yakni Key Generation, Sign, dan Verify. Berikut ini merupakan penjelasan detail mengenai masing-masing komponen tersebut :

1. Kelas Point

Kelas Point terdiri dari 3 atribut, yakni:

Atribut	Tipe
x	*integer*
y	*integer*
z	*integer*

2. Kelas Curve

Kelas Curve terdiri dari 5 atribut, masing-masing nilai dari atribut tersebut telah terdefinisi menggunakan standar kurva secp256k1 (referensi: https://en.bitcoin.it/wiki/Secp256k1), yakni:

Atribut	Tipe	Nilai (*hexadecimal*)
a	*integer*	0x0000000000000000000000000000000000000000000000000000000000000000
b	*integer*	0x0000000000000000000000000000000000000000000000000000000000000007
p	*integer*	0xfffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f
n	*integer*	0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
G	*Point*	(0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798 ,

		0x483ada7726a3c4655da4fbfc0e1108 a8fd17b448a68554199c47d08ffb10d4 b8 , 0)

Berikut ini adalah operasi Matematis Titik :

1. Add
   Berikut ini adalah langkah-langkah penjumlahan titik pada ECC :
   01. Ingin didapatkan R = P + Q
   02. Hitung gradien, m = ((Yp - Yq)/(Xp-Xq)) mod p
   03. Hitung Xr = m2 – Xp – Xq mod p
   04. Hitung Yr = m(Xp – Xr) – Yp mod p
   05. Hasil R = (Xr, Yr)

2. Double
   Berikut ini adalah langkah-langkah penjumlahan titik pada ECC :
   01. Ingin didapatkan R = 2P
   02. Hitung gradien, m = ((3Xp2 + a) / 2Yp) mod p
   03. Hitung Xr = m2 – 2Xp mod p
   04. Hitung Yr = m(Xp – Xr) – Yp mod p
   05. Hasil R = (Xr, Yr)
   06. Jika Yp = 0 maka m tidak terdefinisi sehingga 2P = O, O adalah titik infinity

3. Multiply
   Misalkan, ingin dikalikan titik P dengan skalar k. Operasi perkalian titik menggunakan implementasi rekursif. Terdapat 2 basis, yakni :
   01. Jika k = 0, maka fungsi mengembalikan titik infinity
   02. Jika k = 1, maka fungsi mengembalikan titik P
   03. Untuk tahap rekursif, akan terdapat 2 perhitungan untuk kasus k genap dan k ganjil, yakni :
   04. Jika k genap, maka jalankan perintah multiply(double(P), k / 2)
   05. Jika k ganjil, maka jalankan perintah add(P, multiply(P, k - 1))

Berikut ini adalah metode utama dari implementasi ECDSA :

1. Key Generation

Di tahap ini akan dilakukan pembangkitan kunci privat dan kunci publik. Kunci privat merupakan sebuah bilangan acak yang berada pada rentang [1..n-1]. Kunci publik merupakan hasil perkalian titik dari titik G dari kurva, dengan kunci privat. Kunci privat dan publik akan dikembalikan oleh fungsi dan proses pembangkitan kunci selesai.

2. Sign

Di tahap ini akan dilakukan penandatanganan pesan yang akan dikirim oleh pengirim pesan. Pada tahap ini akan dibutuhkan kunci privat pengguna, dalam algoritma ini kunci privat merupakan variabel bernama ‘d’. Algoritma ini juga membutuhkan kurva eliptik yang nama variabel dan nilainya telah terdefinisi pada makalah ini. Berikut ini adalah algoritma yang telah diimplementasikan :

01. Membangkitkan bilangan bulat acak k yang berada pada rentang [1..n-1].
02. Menghitung perkalian titik (x1, y1) = kG. Hasil x1 akan dikonversi ke bentuk bilangan bulat.
03. Menghitung r = x1 mod n. Jika r = 0 maka ulangi ke langkah 1.
04. Menghitung k-1 mod n. Tujuan perhitungan ini untuk membantu perhitungan s di langkah 6.
05. Menghitung Message Digest dengan cara melakukan hash pada pesan menggunakan algoritma SHA-3 yang telah dibuat. Lalu, hasil Message Digest akan dikonversi ke bentuk bilangan bulat e dengan cara melakukan penjumlahan ke semua nilai bytearray dari Message Digest.
06. Menghitung s = k-1(e + dr) mod n. Jika s = 0 maka ulangi ke langkah 1.
07. Hasil tanda tangan digital adalah pasangan (r, s). Hasil tanda tangan digital tersebut akan dilakukan konkatenasi ke akhir pesan sebelum dikirim ke penerima pesan bersamaan dengan kunci publik.

3. Verify

Di tahap ini akan dilakukan verifikasi tanda tangan digital dari pesan yang telah diterima oleh penerima pesan. Pada tahap ini akan dibutuhkan kunci publik pengguna, dalam algoritma ini kunci publik merupakan variabel bernama ‘Q’. Algoritma ini juga membutuhkan kurva eliptik yang nama variabel dan nilainya telah terdefinisi pada makalah ini. Berikut ini adalah algoritma yang telah diimplementasikan :

01. Melakukan verifikasi bahwa r dan s adalah bilangan bulat pada rentang [1..n-1].
02. Menghitung Message Digest dengan cara melakukan hash pada pesan menggunakan algoritma SHA-3 yang telah dibuat. Lalu, hasil Message Digest akan dikonversi ke bentuk bilangan bulat e dengan cara melakukan penjumlahan ke semua nilai bytearray dari Message Digest.
03. Menghitung w = s-1 mod n.
04. Menghitung u1 = ew mod n dan u2 = rw mod n.
05. Menghitung X = u1G + u2Q dengan menggunakan perkalian titik untuk u1G dan u2Q.
06. Jika X merupakan titik infinity, maka tolak tanda tangan digital. Jika tidak, maka lakukan konversi koordinat x1 dari X menjadi bilangan bulat, serta hitung v = x1 mod n.
07. Tanda tangan digital akan diterima jika v = r.

B. Implementasi ECDSA pada Invoice Bertipe JSON

Berikut ini adalah contoh implementasi dari algoritma ECDSA pada sebuah *invoice* bertipe JSON. Kunci privat yang

digunakan adalah
0x451caf5a928253c2d1a4d73c325ea0cc1cf197e9818b3f799910cc9100f8bbea :

1. *Invoice* sebelum ditambahkan tanda tangan digital


```
{
 "DueDate": "2013-02-15",
 "Balance": 1990.19,
 "DocNumber": "SAMP001",
 "Status": "Payable",
 "Line": [
  {
   "Description": "Sample Expense",
   "Amount": 500,
   "DetailType": "ExpenseDetail",
   "ExpenseDetail": {
    "Customer": {
     "value": "ABC123",
     "name": "Sample Customer"
    },
    "Ref": {
     "value": "DEF234",
     "name": "Sample Construction"
    },
    "Account": {
     "value": "EFG345",
     "name": "Fuel"
    },
    "LineStatus": "Billable"
   }
  }
 ],
 "Vendor": {
  "value": "GHI456",
  "name": "Sample Bank"
 },
 "APRef": {
  "value": "HIJ567",
  "name": "Accounts Payable"
 },
 "TotalAmt": 1990.19
}
```


2. *Invoice* setelah ditambahkan tanda tangan digital


```
{
 "DueDate": "2013-02-15",
 "Balance": 1990.19,
 "DocNumber": "SAMP001",
 "Status": "Payable",
 "Line": [
  {
   "Description": "Sample Expense",
   "Amount": 500,
   "DetailType": "ExpenseDetail",
   "ExpenseDetail": {
    "Customer": {
     "value": "ABC123",
     "name": "Sample Customer"
    },
    "Ref": {
     "value": "DEF234",
     "name": "Sample Construction"
    },
    "Account": {
     "value": "EFG345",
     "name": "Fuel"
    },
    "LineStatus": "Billable"
   }
  }
 ],
 "Vendor": {
  "value": "GHI456",
  "name": "Sample Bank"
 },
 "APRef": {
  "value": "HIJ567",
  "name": "Accounts Payable"
 },
 "TotalAmt": 1990.19
}
--BEGIN SIGNATURE--
0x9a375f3b51ad5d6806a5846e5a25db02e1c2166789aad4b042edab19dd82bf20
0xe8006a6a561778faec08465f0137c085c010dca304f4f20ef4f8a5578e4ab645
--END SIGNATURE--
622172068486544529671928878089008591443161841389461713836122851051438475690 82,211865394744214965837586636300885427973111004337068229203235080641491285169 15
```


Setelah dilakukan verifikasi, hasilnya bernilai True, karena tidak ada bagian dari data *invoice* yang diubah.

IV. Eksperimen dan Hasil Analisis

Berikut ini adalah hasil eksperimen untuk 2 prinsip kriptografi, yakni otentikasi dan integritas data. Berikut ini adalah pesan dan tanda tangan digital serta kunci publik yang digunakan pada pengujian kali ini:


```
{
 "DueDate": "2013-02-15",
 "Balance": 1990.19,
 "DocNumber": "SAMP001",
 "Status": "Payable",
 "Line": [
  {
   "Description": "Sample Expense",
   "Amount": 500,
   "DetailType": "ExpenseDetail",
   "ExpenseDetail": {
    "Customer": {
     "value": "ABC123",
     "name": "Sample Customer"
```

```
      },
      "Ref": {
        "value": "DEF234",
        "name": "Sample Construction"
      },
      "Account": {
        "value": "EFG345",
        "name": "Fuel"
      },
      "LineStatus": "Billable"
    }
  }
 ],
 "Vendor": {
   "value": "GHI456",
   "name": "Sample Bank"
 },
 "APRef": {
   "value": "HIJ567",
   "name": "Accounts Payable"
 },
 "TotalAmt": 1990.19
}
--BEGIN SIGNATURE--
0xb4bb66034156d4b12b545b19e9454b87010f83e30d0c00d
7b224fd55ae3c773a
0xef166d081cd4ff8518114ef38b7ccd594490e4c28111fae91
46647613dd01e07
--END SIGNATURE--
859866596247233101835568212297500050470040759206
070217580185881256857566359 17,7631751960839235174
893507566186948646191030319105872971215555884058
8675435530
```


Akan dilakukan 4 pengujian yakni Perubahan Data *Invoice*, Modifikasi Karakter Tanda Tangan Digital, Penggunaan Kunci Privat yang Tidak Sesuai, dan Pengujian Penghapusan Tanda Tangan Digital.

1. Pengujian Perubahan Data *Invoice*
   Data yang diubah adalah DueDate, menjadi 2020-12-12.

Data Setelah Perubahan


```
{
 "DueDate": "2020-12-12",
 "Balance": 1990.19,
 "DocNumber": "SAMP001",
 "Status": "Payable",
 "Line": [
   {
    "Description": "Sample Expense",
    "Amount": 500,
    "DetailType": "ExpenseDetail",
    "ExpenseDetail": {
      "Customer": {
        "value": "ABC123",
        "name": "Sample Customer"
      },
```



```
      "Ref": {
        "value": "DEF234",
        "name": "Sample Construction"
      },
      "Account": {
        "value": "EFG345",
        "name": "Fuel"
      },
      "LineStatus": "Billable"
    }
  }
 ],
 "Vendor": {
   "value": "GHI456",
   "name": "Sample Bank"
 },
 "APRef": {
   "value": "HIJ567",
   "name": "Accounts Payable"
 },
 "TotalAmt": 1990.19
}
--BEGIN SIGNATURE--
0xb4bb66034156d4b12b545b19e9454b87010f83e30d0c00d
7b224fd55ae3c773a
0xef166d081cd4ff8518114ef38b7ccd594490e4c28111fae91
46647613dd01e07
--END SIGNATURE--
859866596247233101835568212297500050470040759206
070217580185881256857566359 17,7631751960839235174
893507566186948646191030319105872971215555884058
8675435530
```


Hasil Verifikasi
False

2. Pengujian Modifikasi Karakter Tanda Tangan Digital
   Karakter yang dimodifikasi adalah yang karakter ‘b’ pada tanda tangan digital yang ditandai dengan warna merah pada data di bawah ini.

Data setelah perubahan


```
{
 "DueDate": "2013-02-15",
 "Balance": 1990.19,
 "DocNumber": "SAMP001",
 "Status": "Payable",
 "Line": [
   {
    "Description": "Sample Expense",
    "Amount": 500,
    "DetailType": "ExpenseDetail",
    "ExpenseDetail": {
      "Customer": {
        "value": "ABC123",
```

```
        "name": "Sample Customer"
      },
      "Ref": {
        "value": "DEF234",
        "name": "Sample Construction"
      },
      "Account": {
        "value": "EFG345",
        "name": "Fuel"
      },
      "LineStatus": "Billable"
    }
  }
 ],
 "Vendor": {
  "value": "GHI456",
  "name": "Sample Bank"
 },
 "APRef": {
  "value": "HIJ567",
  "name": "Accounts Payable"
 },
 "TotalAmt": 1990.19
}
--BEGIN SIGNATURE--
0xb4bb66034156d4b12b545b19e9454b87010f83e30d0c00d
7b224fd55ae3c773b
0xef166d081cd4ff8518114ef38b7ccd594490e4c28111fae91
46647613dd01e07
--END SIGNATURE--
859866596247233101835568212297500050470040759206
070217580185881256857566359 17,7631751960839235174
893507566186948646191030319105872971215555884058
8675435530
```


Hasil Verifikasi
False

3. Penggunaan Kunci Privat yang Tidak Sesuai
   Kunci privat yang digunakan untuk melakukan pembangkitan kunci publik dengan yang digunakan untuk melakukan *sign* adalah 2 kunci privat yang berbeda.

Kunci Privat Asli	Kunci Publik Asli	Kunci Privat Modifikasi	Hasil Verifikasi
0x451caf5a928253c2d1a4d73c325ea0cc1cf197e9818b3f799910cc9100f8bbea	6221720684865445296719288780890085914431618413894617138361228510514384756908 2,2118653947442	0x451caf5a928253c2d1a4d73c325ea0cc1cf197e9818b3f799910cc9100f8bbeb	False
	1496583758663630088542797311100433706822920323508064149128516915		

4. Pengujian Penghapusan Tanda Tangan Digital
   Tanda tangan digital dihapus dan dicoba melakukan verifikasi.

Data setelah perubahan


```
{
 "DueDate": "2013-02-15",
 "Balance": 1990.19,
 "DocNumber": "SAMP001",
 "Status": "Payable",
 "Line": [
  {
   "Description": "Sample Expense",
   "Amount": 500,
   "DetailType": "ExpenseDetail",
   "ExpenseDetail": {
    "Customer": {
     "value": "ABC123",
     "name": "Sample Customer"
    },
    "Ref": {
     "value": "DEF234",
     "name": "Sample Construction"
    },
    "Account": {
     "value": "EFG345",
     "name": "Fuel"
    },
    "LineStatus": "Billable"
   }
  }
 ],
 "Vendor": {
  "value": "GHI456",
  "name": "Sample Bank"
 },
 "APRef": {
  "value": "HIJ567",
  "name": "Accounts Payable"
 },
 "TotalAmt": 1990.19
}
```


Hasil Verifikasi
Message not digitally signed

V. KESIMPULAN

Berdasarkan implementasi dan hasil eksperimen dapat disimpulkan bahwa ECDSA dapat digunakan untuk menandatangani *invoice* dari suatu platform *e-commerce* untuk menjaga keamanan data dengan cukup baik. Ketika ada perubahan pada pesan, kunci, maupun tanda tangan digital, program akan mengembalikan pesan False yang menandakan bahwa ada suatu modifikasi dari pesan yang diterima.

Dengan menggunakan ECDSA prinsip-prinsip kriptografi juga dapat terpenuhi. Prinsip Otentikasi dapat terpenuhi karena tanda tangan digital menandakan identitas pengirim. Prinsip integritas data dapat terjaga karena ketika data diubah pada saat eksperimen maka hal itu dapat terdeteksi dan program mengembalikan False. Prinsip anti-penyangkalan juga dapat teratasi karena dengan adanya tanda tangan digital seseorang pada suatu *invoice* maka tidak diragukan lagi bahwa *invoice* tersebut merupakan milik suatu pihak tertentu.

REFERENSI

[1] R. Kaur and A. Kaur, "Digital Signature," 2012 International Conference on Computing Sciences, Phagwara, 2012, pp. 295-301, doi: 10.1109/ICCS.2012.25.

[2] Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). Dept. of Combinatorics & Optimization, University of Waterloo, Ca. https://www.cs.miami.edu/home/burt/learning/Csc609.142/ecdsa-cert.pdf

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.

Semarang, 18 Desember 2020

Ferdy Santoso / 13517116