Implementasi Algoritma ElGamal dan Fungsi Hash SHA3 untuk Tanda Tangan Digital pada Audio

Dinda Yora Islami
Teknik Informatika / Sekolah Tinggi Elektro dan Informatika
ITB
Bandung, Indonesia
dindayorai@gmail.com

***Abstract*—Tanda tangan digital adalah tanda tangan elektronik yang digunakan untuk membuktikan keaslian identitas pengirim pesan. Tanda tangan digital digunakan untuk memastikan isi file yang dikirim tanpa ada perubahan setelah dikirim. File audio yang tersebar tak jarang memiliki informasi penting sehingga perlu membuktikan kepemilikan file. Kepemilikan file audio dapat dilakukan dengan menyisipkan tanda tangan digital pada audio. Pembentukan tanda tangan digital pada file audio menggunakan fungsi hash SHA3 dan algoritma Elgamal. Fungsi hash ini dapat mengubah pesan dengan ukuran sembarang menjadi pesan ringkas dengan ukuran tetap. Implementasi tanda tangan digital ini diharapkan dapat meningkatkan kepercayaan informasi yang terdapat pada file audio.**

Keywords—audio, tanda tangan digital, algoritma elgamal, fungsi hash.

I. PENDAHULUAN

Perkembangan teknologi mempermudah manusia dalam menyebarkan informasi, baik secara tekstual, audio, maupun video. Penyebaran informasi ini melalui pemberian langsung seperti lewat flashdisk, CD, maupun secara tidak langsung yaitu lewat internet.

Penyebaran audio seperti musik, rekaman suara, atau hal lainnya banyak dilakukan oleh manusia. Tidak sedikit orang yang mengirimkan informasi lewat audio. Informasi yang diperoleh tidak jarang merupakan informasi penting sehingga perlu dibuktikan keaslian informasi ini.

Untuk menentukan suatu informasi benar atau salah perlu mengetahui siapa pemilik dari audio tersebut. Dengan mengetahui pengirim dari file audio tersebut dapat ditentukan kebenaran dari isi informasi. Seperti informasi pemerintah lewat audio, dengan mengetahui bahwa pengirim file audio itu merupakan dari instansi pemerintah maka dapat diyakini bahwa pengumuman itu benar dan tanpa rekayasa.

Setiap pemilik dari file audio memiliki sesuatu nilai unik yang bisa digunakan untuk merepresentasikan identitas pemiliknya. Nilai unik ini adalah sebuah kunci private yang digunakan untuk membangkitkan tanda tangan digital yang akan disisipkan pada file audio. Tanda tangan digital ini akan memberikan informasi terhadap pemilik dari audio tersebut.

Pada Makalah ini akan dibahas implementasi Algoritma kunci publik yaitu ElGamal dan Fungsi Hash dalam pembentukan tanda tangan digital pada file audio.

II. DASAR TEORI

A. Algoritma ElGamal

Algoritma ElGamal merupakan salah satu algoritma kunci publik yang dikemukakan oleh Taher Elgamal pada tahun 1985. Algoritma Elgamal menggunakan permasalahan logaritma diskrit. Algoritma ini terdiri dari tiga proses, yaitu proses pembangkitan kunci, proses enkripsi, dan proses dekripsi.

Algoritma ElGamal merupakan salah satu algoritma block cipher, dimana melakukan enkripsi pada block-block plaintext yang menghasilkan block-block ciphertext yang kemudian digabungkan lagi menghasilkan ciphertext. Dalam proses dekripsi ciphertext dipecah menjadi block-block ciphertext yang kemudian di setiap block di dekripsi dan digabungkan menjadi plaintext semula.

B. Fungsi Hash SHA3

Fungsi hash merupakan fungsi yang mengubah suatu pesan dengan ukuran sembarang menjadi suatu pesan ringkas yang panjangnya selalu tetap meskipun panjang pesan aslinya berbeda-beda. Fungsi hash memiliki sifat satu arah, yang berarti setelah pesan diubah menjadi *message digest,* pesan tidak dapat diubah kembali menjadi pesan awal (*irreversible*).

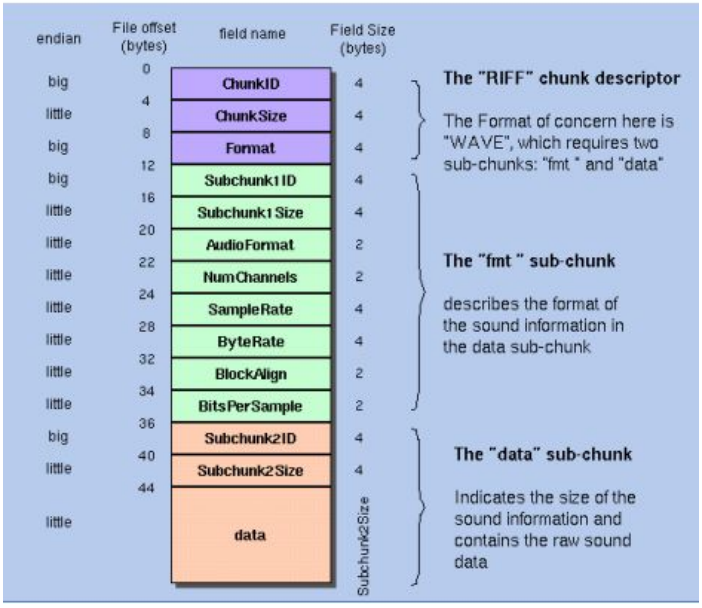
SHA3 merupakan fungsi hash satu arah yang dihasilkan oleh kompetensi yang diselenggarakan oleh NIST. Proses dari algoritma SHA3 adalah sebagai berikut:

- Preproses pesan masukan (P), yaitu menambahkan padding pada pesan masukan. Panjang pesan akhir harus merupakan kelipatan *r,* dimana r = bitrate.
- Pemecahan pesan masukan menjadi P0, P1, …, Pi, dimana i = jumlah kelipatan panjang bitrate untuk panjang pesan masukan.
- Absorbing pada semua pesan masukan
- Squeezing sebanyak j, dimana j = kelipatan panjang keluaran r/w, r = bitrte dan w panjang lane
- keluaran merupakan gabungan dari keluaran Squeezing pada rentang bitrate tertentu

C. Audio Wave

File Wave atau Wav merupakan bagian dari spesiikasi RIFF Microsoft untuk penyimpanan file multimedia. Sebuah file RIFF dimulai dengan sebuah header diikuti dengan urutan dari potongan data. Umumnya data audio di dalam format Wav adalah bentuk tidak terkompresi.

Format data pada wav:



Gambar 1. Format data wav

sumber : https://ccrma.stanford.edu/

D. Tanda Tangan Digital

Tanda tangan digital adalah tanda tangan elektronik yang digunakan untuk membuktikan keaslian identitas pengirim pesan. Tanda tangan digital digunakan untuk memastikan isi file yang dikirim tanpa ada perubahan setelah dikirim.

Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Tanda tangan digital selalu berbeda-beda antara satu file dengan file lain.

Terdapat dua cara dalam menandatangani pesan, yaitu melakukan enkripsi pesan dan menggunakan kombinasi fungsi hash dan kriptografi kunci-publik. Penandatangan pesan dengan cara mengenkripsinya memberikan dua fungsi yaitu kerahasiaan dan otentikasi pesan. Sedangkan penandatanganan pesan dengan kombinasi fungsi hash dan kunci publik hanya untuk keotentikan pesan saja.

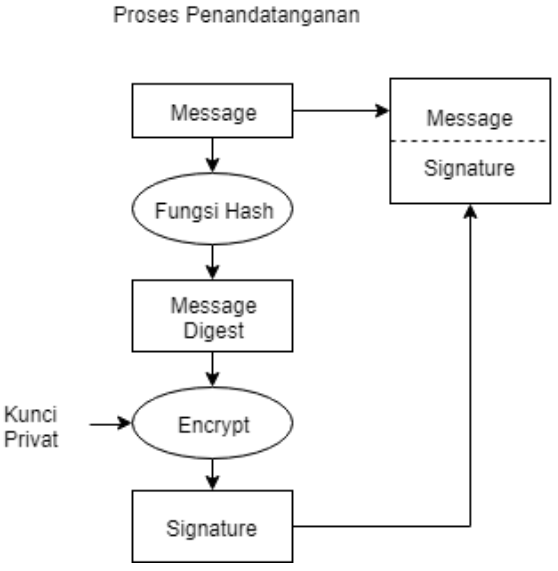
Untuk memeriksa integritas data yang telah diberi tanda tangan digital, digunakan publik key dari pihak yang memberi tanda tangan digital. Apabila hasil data yang diperoleh sama maka data tersebut tidak terjadi perubahan, namun jika hasil data yang diperoleh berbeda maka data yang telah diberi tanda tangan digital telah terjadi perubahan dan/atau pihak yang memberi tanda tangan berbeda dengan pemilik kunci publik.

III. PEMBAHASAN

A. Rancangan Algoritma

Proses tanda tangan digital yang memanfaatkan fungsi hash dan algoritma ElGamal terdiri dari beberapa tahap yaitu tahap penandatanganan dan tahap verifikasi. Pada tahap penandatangan terjadi proses seperti pada gambar 2, yaitu:

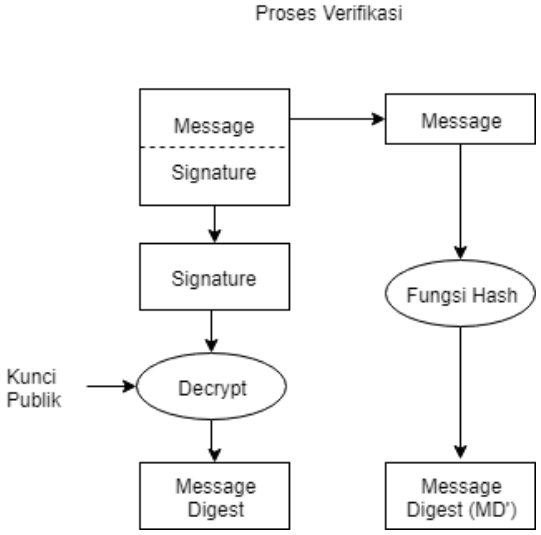
1. Menghitung *message digest* dari pesan menggunakan algoritma SHA3
2. Melakukan enkripsi pada *message digest* oleh algoritma ElGamal menghasilkan tanda tangan digital Pada tahap ini enkripsi dilakukan dengan menggunakan kunci private si pengirim yang telah dibangkitkan sebelumnya.
3. Menempelkan atau menyisipkan tanda tangan digital pada file audio



Gambar 2. Proses Penandatanganan pesan

Sedangkan pada tahap verifikasi terjadi proses seperti pada gambar 3 yaitu:

1. Memisahkan pesan dengan tanda tangan digital
2. Melakukan dekripsi tanda tangan digital dengan algoritma ElGamal menjadi *message digest*. Pada tahap ini dekripsi dilakukan dengan menggunakan kunci publik pengirim.
3. Menghitung nilai hash pesan yang diterima menggunakan algoritma SHA3
4. Membandingkan nilai yang diperoleh pada point 2 dan 3



Gambar 3. Proses Verifikasi pesan

Jika pada tahap verifikasi point 4 hasil perbandingan sama maka diketahui bahwa pengirim pesan terotentikasi dan data yang dikirim tidak terjadi perubahan. Namun jika perbandingan nilainya berbeda maka kemungkinan terjadi perubahan pada pesan saat dikirim dan /atau pengirim pesan ternyata orang yang berbeda.

Pengolahan data audio pada enkripsi dilakukan dengan mengambil nilai byte dari file audio, nilai byte tersebut yang akan diubah jadi message digest, kemudian message digest yang telah dilakukan enkripsi akan disisipkan setelah byte terakhir pesan.

Pengolahan data audio pada dekripsi dilakukan dengan mengambil nilai beberapa byte terakhir pada audio. Message digest yang dihasilkan oleh algoritma SHA3 memiliki ukuran panjang yang sama untuk setiap ukuran pesan yang berbeda sehingga dapat ditentukan banyak nilai byte yang diambil yang merupakan tanda tangan digital yang telah disisipkan pada pesan audio.

B. Eksperimen dan Pembahasan Hasil

Eksperimen dari algoritma ElGamal dan SHA3 pada file audio akan dilakukan dengan menggunakan data audio yang berukuran berbeda yang ditunjukan pada Tabel 1.

Tabel 1. Data Audio yang diuji

Nama File	Ukuran	Durasi
audio1.wav	705,7 kB	5 s
audio2.wav	1,8 MB	10 s
audio3.wav	2,6 MB	15 s

Audio1, Audio2, merupakan bagian dari audio3, dimana audio1 mengambil 5 detik pertama dari audio 3, dan audio2 mengambil 10 detik pertama dari audio3.

Untuk implementasi ini kita menggunakan kunci private dan kunci publik sebagai berikut

Kunci Private : 1200936,1716551,
Kunci Publik : 1535843,1303756,1716551,

1. Audio 1

   Pada audio1.wav didapatkan nilai hash

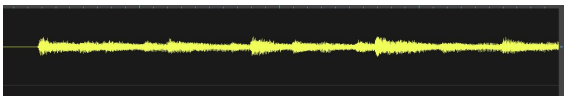
   520d93e3e67cb95d3a242b3d3791a90fac1a8f871d
   a307839b1e9d006d0204a9d2fcebe5a78a1031273b
   91c0525f3dbdcd121369b8105adbb0098aeab02bdf
   14

   nilai hash tersebut dienkripsi dengan algoritma ElGamal menggunakan kunci privat menghasilkan

   10b22d0bdec510b22d0b367b10b22d0d6b7310b22
   d1961d810b22d071d4c10b22d124b3510b22d10bb
   9810b22d04dcc510b22d08bb4c10b22d04a95010b
   22d169a5510b22d11bae510b22d11228110b22d0f
   58e010b22d12ae5d10b22d0a8fe310b22d0dcccf10
   b22d026b5610b22d18172f10b22d03eae610b22d0
   a3ec410b22d165e5a10b22d0e1adc10b22d051d761
   0b22d065c9d10b22d0650d710b22d12e60510b22d
   18bea610b22d0e755710b22d0ead8910b22d0a1f9b
   10b22d1989cb10b22d11ab2710b22d0967f810b22
   d11503210b22d0138b610b22d0b663610b22d157e
   6510b22d16c58c10b22d0ef9d610b22d03e77810b
   22d069ec310b22d0c340710b22d10648b10b22d0a
   fba410b22d0c343410b22d17a32410b22d0e83611
   0b22d0c495710b22d01b38910b22d04464d10b22d
   0e266610b22d16cdbd10b22d101ba910b22d16815

```
c10b22d05e8d010b22d10b29910b22d0ae7ad10b2
2d127b7310b22d05078e10b22d13918210b22d0b4
afc10b22d018ccf10b22d1208d110b22d13306910b
22d183ac410b22d0d44c010b22d0f2b8310b22d04
903c
```

Hasil dari enkripsi hash ini akan disisipkan di akhir audio. Dengan memanfaatkan https://sodaphonic.com/editor didapatkan tampilan grafik dari audio sebelum di sisipkan tanda tangan digital dan grafik audio sesudah disisipkan tanda tangan digital yang ditunjukan pada gambar 4 dan gambar 5 secara berturut-turut. Dapat kita lihat pada gambar 5 terjadi kenaikan grafik diakhir audio, yang merupakan tanda tangan digital.



Gambar 4. Grafik audio1 sebelum diberi tanda tangan

Gambar 5. Grafik audio1 sesudah diberi tanda tangan

2. Audio 2

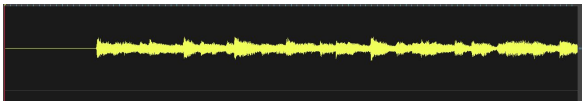
Pada audio1.wav didapatkan nilai hash

```
9125f169e560531ed8d41d3985e426e0890e536158
439fb9ebb31c0600736528f7e28e0cc1292cde0bffb
4f4f4dc92cbdf0a2887a3728fb2f93add5ec6f8c00e
```

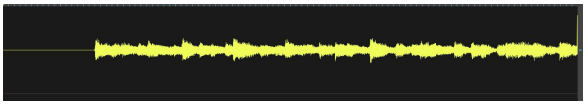
nilai hash tersebut dienkripsi dengan algoritma ElGamal menggunakan kunci privat menghasilkan

```
1a25131607d21a251304256d1a251313c23d1a251
3062d9e1a251306278a1a25130d84321a25130a49
2b1a251316d2aa1a25130b76481a251310de411a2
51308dff11a251312a4431a2513045dd61a251316b
1fc1a25131847be1a251302950f1a2513076b481a2
5130a14a41a25130f1ddc1a251309facb1a251300f0
cd1a25130d408e1a251305cd3b1a251307ac4c1a25
131281b91a2513000bd71a25130203191a25130d0
9801a251311d5f61a251302c30a1a251319fd0b1a2
5130faeb51a25131159d11a251304c3641a2513137
e991a25130d57841a251315dab21a25130823e11a
2513040b971a251303bca11a25131607d21a25130
e93261a251308a9fc1a251313246d1a2513131fb01
a25130bd7a61a25130b0bd71a251307b1d91a2513
0a08fb1a25130966b31a25130c47c51a25131249f0
1a2513001f941a25130ea9da1a25130facab1a2513
0562ad1a251305d1be1a2513092bd41a25130506a
71a25130503f51a251302b6ac1a251302a6f01a251
31906821a251316b51c1a2513038c9d1a25130a37
8b1a25130842511a25130c2b021a251301b64d
```

Hasil dari enkripsi hash ini akan disisipkan di akhir audio. Dengan memanfaatkan https://sodaphonic.com/editor didapatkan tampilan grafik dari audio sebelum di sisipkan tanda tangan digital dan grafik audio sesudah disisipkan tanda tangan digital yang ditunjukan pada gambar 6 dan gambar 7 secara berturut-turut. Dapat kita lihat pada gambar 7 terjadi kenaikan grafik diakhir audio, yang merupakan tanda tangan digital.



Gambar 6. Grafik audio1 sebelum diberi tanda tangan



Gambar 7. Grafik audio1 sesudah diberi tanda tangan

3. Audio 3

Pada audio1.wav didapatkan nilai hash

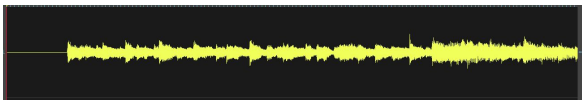
```
0cdfa0607025aafa7395fabded31f45b2103acccd19
d9c853d7dff076e6563279dab25f314f72f0b0862ec
c6f5bcc0cbd9464fe393a5286b72afe4a588f02103
```

nilai hash tersebut dienkripsi dengan algoritma ElGamal menggunakan kunci privat menghasilkan

```
0540970e0b190540970758df0540970ac76d05409
70230e105409706a33c054097063a48054097190f
d60540970e42af0540971512da05409709ba41054
09701c3e4054097189fa4054097085cc3054097079
a2905409705c930054097019a680540970a52e205
4097004da90540970a257a054097172e420540970
69a3a0540970b9f2b0540971008c005409704a197
05409716ac2905409718da5c0540970b73e905409
711754c0540970407320540971 3a698054097063c
8105409708bc5a05409718382d054097021268054
09718a0560540970eee4b05409707869b05409711
03a605409705c930054097071c4b0540971360e10
5409717f3fb05409713570a0540970bfbb80540970
7d9f8054097081174054097 02aa110540970d1080
05409702e81d054097057a030540970fccc0054097
```

14cf5b05409708ced00540971629600540971403ca054097168d650540970dd95b0540970f2903054097021d470540971061b70540971310ca0540970e743f0540970df2da054097023a900540970eb3540540970e42a20540970ff9cb0540970d6a590540971362c5

Hasil dari enkripsi hash ini akan disisipkan di akhir audio. Dengan memanfaatkan https://sodaphonic.com/editor didapatkan tampilan grafik dari audio sebelum di sisipkan tanda tangan digital dan grafik audio sesudah disisipkan tanda tangan digital yang ditunjukan pada gambar 8 dan gambar 9 secara berturut-turut. Dapat kita lihat pada gambar 9 terjadi kenaikan grafik diakhir audio, yang merupakan tanda tangan digital.



Gambar 8. Grafik audio1 sebelum diberi tanda tangan

Gambar 9. Grafik audio1 sesudah diberi tanda tangan

C. Analisis Keamanan

1. Analisis perubahan pada audio dan kunci publik valid

   Tanda tangan digital memanfaatkan algoritma SHA3 yang mengambil nilai message digest dari suatu file. Perubahan satu byte pada file audio akan mengubah nilai message digest sehingga jika audio mengalami perubahan atau kerusakan maka hasil dekripsi dari tanda tangan digital yang disisipkan pada file audio tidak akan sama dengan nilai message digest file audio itu. Hal ini akan membantu dalam mendeteksi keaslian dari file audio.

2. Analisis perubahan pada audio dan kunci publik tidak valid.

   Tanda tangan digital memanfaatkan algoritma SHA3 yang mengambil nilai message digest dari suatu file. Perubahan satu byte pada file audio akan mengubah nilai message digest sehingga jika audio mengalami perubahan atau kerusakan maka hasil message digest akan mengalami perubahan. Selain itu diperlukan kunci publik untuk melakukan dekripsi tanda tangan digital. Jika kunci publik tidak valid maka nilai dari message digest dan hasil dekripsi tidak akan sama.

3. Analisis tidak terjadi perubahan pada audio dan kunci publik tidak valid

   Tanda tangan digital memanfaatkan algoritma ElGamal dalam melakukan enkripsi dan dekripsi dari nilai message digest. Dengan berbedanya pasangan kunci publik,private yang digunakan untuk enkripsi dan dekripsi maka pada proses pengecekan keaslian ataupun otentikasi file akan gagal

Tanda tangan digital memanfaatkan algoritma SHA3 untuk menghitung message digest dan ElGamal dalam melakukan enkripsi dan dekripsi dari nilai message digest. Untuk melakukan otentikasi pemilik tanda tangan digital pada file audio, dapat dilakukan pengecekan dengan mendekripsikan tanda tangan digital dengan kunci publik si Pengirim. Jika nilai message digest yang dihasilkan berbeda maka kunci publik tidak valid atau terjadi kerusakan pada file audio. Hal ini akan membantu untuk melakukan otentikasi pengirim file audio

IV. KESIMPULAN DAN SARAN PENGEMBANGAN

Penggunaan tanda tangan digital pada file audio dapat meningkatkan keamanan atas audio tersebut berupa keaslian audio dan kepemilikan audio. Hal ini dikarenakan dengan tanda tangan digital dapat dilakukan analisis kondisi dan kepemilikan berdasarkan kunci public pemilik audio.

Berdasarkan hasil implementasi yang telah dilakukan, penggunaan tanda tangan digital pada audio ini tidak merusak kualitas dari audio tersebut, hanya pada penambahan data pada file audio. Namun perlu diperhatikan lagi untuk proses penyisipan tanda tangan digital agar tidak terjadi kesenjangan suara antara file audio dengan tanda tangan digital.

Penggunaan tanda tangan digital dapat dimanfaatkan dalam berbagai bidang seperti pada Pemerintahan dan produksi musik. Pengembangan tanda tangan digital pada makalah ini masih memiliki kekurangan sehingga penulis berharap penggunaan tanda tangan digital dikembangkan lebih dalam lagi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Allah SWT, karena berkat rahmat dan karunianya makalah ini dapat selesai pada waktunya. Tak lupa juga, penulis ingin menyampaikan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT selaku dosen mata kuliah IF4020 Kriptografi yang telah membagikan ilmunya kepada penulis. Selain itu, penulis juga ingin menyampaikan terima kasih kepada kedua orang tua yang selalu mendukung penulis.

REFERENSI

[1] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Algoritma ElGamal.

[2] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Fungsi Hash.

[3] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: SHA-3:Kompetensi Fungsi Hash oleh NIST

[4] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Tanda-tangan Digital .

[5] Goukm.id (2017, 22 Januari). *Apa Fungsi Tanda Tangan Digital (eSignature) dan Bagaimana Cara Membuatnya*. Dikutip 9 Mei 2019 dari GOukm.id : https://goukm.id/tanda-tangan-digital-esignature/

PERNYATAAN

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

Bandung, 10 Mei 2019

Dinda Yora Islami
13516067