

Implementasi Digital Signature pada Form Biodata

Fritz Gerald Tjie - 13518065
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13518065@std.stei.itb.ac.id

Abstrak—Di era modern sekarang, seringkali kita membutuhkan berbagai macam layanan jasa. Layanan ini dapat berupa layanan kesehatan, reparasi, hingga pembelian barang. Ketika kita ingin menggunakan layanan tersebut, seringkali kita diharuskan untuk memberikan data diri yang dibutuhkan oleh layanan tersebut. Memanfaatkan teknologi yang sudah ada, data diri biasanya diberikan dengan menggunakan suatu form biodata *online* yang diisi melalui aplikasi atau situs layanan tersebut. Untuk menjamin integritas dari data yang kita berikan dan menjamin bahwa penerima dari data mendapatkan data yang sesungguhnya, *digital signature* dapat diimplementasikan dalam menyelesaikan permasalahan integritas data. Pada makalah ini akan dibahas mengenai implementasi *digital signature* pada form biodata dengan memanfaatkan algoritma RSA dan SHA256.

Kata kunci—*Digital Signature*, RSA, SHA256, manipulasi data, form biodata, data diri.

I. PENDAHULUAN

Manusia sebagai makhluk sosial membutuhkan bantuan orang lain dalam bertahan hidup dan memenuhi kebutuhan sehari-harinya. Bantuan orang lain ini dapat berupa bantuan barang ataupun jasa. Di era modern ini, jasa yang ditawarkanpun berbagai macam dan dapat berupa berbagai macam layanan. Memanfaatkan teknologi yang sudah maju dan tersebar luasnya jangkauan jaringan Internet, jumlah pihak-pihak yang menyediakan jasa berupa layanan *online* pun semakin besar. Namun, seringkali kita diharuskan untuk mengisi suatu form biodata untuk memberikan data diri kepada pihak-pihak penyedia layanan jasa untuk diperbolehkan menggunakan layanan tersebut.

Praktik ini sudah sangatlah marak dilakukan dan merupakan suatu aturan tidak tertulis yang ada dimasyarakat. Baik penyedia layanan reparasi, perbankan, hingga jasa transportasi atau kurir juga mewajibkan calon pengguna layanan untuk memberikan data diri mereka sebelum dapat menggunakan berbagai macam layanan yang pihak-pihak tersebut sediakan. Hal ini juga berguna untuk memastikan bahwa pengguna merupakan pengguna asli dan memiliki identitas yang jelas, bukan pengguna fiktif atau *bot* yang berpotensi digunakan untuk mengacaukan alur operasi dari penyedia layanan.

Terlebih lagi dengan adanya peningkatan aktivitas *online* yang disebabkan oleh pandemic COVID-19 yang masih berlanjut hingga saat makalah ini ditulis, penggunaan layanan

berbasis *online* semakin meningkat. Hal ini dapat menyebabkan meningkatnya tingkat penipuan dan manipulasi data yang dapat dilakukan oleh oknum-oknum yang tidak bertanggung jawab. Data diri yang diberikan oleh pengguna dapat dimanipulasi ataupun berubah dikarenakan oleh proses pengiriman data yang tidak aman.

Digital Signature (tanda tangan digital) merupakan salah satu solusi dalam menjamin integritas dan keaslian suatu informasi atau data, khususnya pada dokumen atau data yang bersifat digital. *Digital Signature* dapat “merangkum” isi dari suatu dokumen digital dan menghasilkan suatu kode khusus yang berfungsi sebagai tanda pengenal dan penanda dokumen tersebut. Dengan memanfaatkan *digital signature*, permasalahan mengenai integritas data dapat diselesaikan.

II. DASAR TEORI

A. Form Biodata

Berdasarkan KBBI, data merupakan keterangan yang benar dan nyata^[1], dan biodata merupakan riwayat hidup singkat^[2]. Biodata sendiri merupakan data-data mengenai informasi personal dari seseorang. Informasi personal ini dapat berupa nama, Nomor Induk Kependudukan, tempat dan tanggal lahir, jenis kelamin, tanda tangan, foto, hingga sidik jari.

Ketika menggunakan layanan *online*, biasanya pengguna diminta untuk memasukkan data diri melalui *text field* yang telah disusun menjadi form biodata. Form biodata ini nantinya akan digunakan untuk berbagai macam kebutuhan dari penyedia layanan.

The image shows a digital form for data collection. It includes the following fields and options:

- NPM:
- Nama Lengkap:
- IPK:
- Lama Study: Tahun Bulan
- Jurusan: T. Informatika T. Elektro T. Sipil
- Tempat dan Tanggal Lahir: Tgl Bln Thn
- Jenis Kelamin: Laki-laki Perempuan
- Alamat:

At the bottom, there are two buttons: "Kembali" and "Tambah Data".

Gambar 1. Contoh *Form Biodata* yang digunakan oleh Penyedia Layanan. Sumber: <https://communityofcomm2.blogspot.com/2012/12/membuat-biodata-menggunakan-html-dan-php.html>

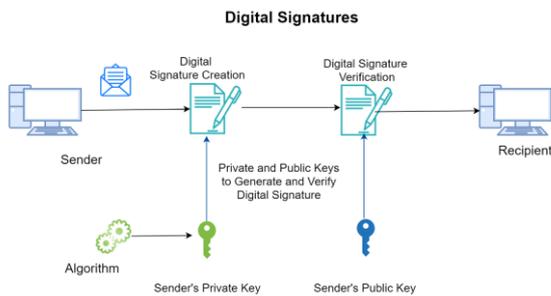
B. Digital Signature

Digital Signature (tanda tangan digital) merupakan suatu metode matematis yang berfungsi untuk membuktikan keaslian pesan atau dokumen digital. *Digital signature* dapat digunakan sebagai alat bukti yang menunjukkan bahwa data atau informasi yang ada merupakan versi aslinya dan tidak mengalami modifikasi sama sekali^[3]. *Digital signature* pada dasarnya adalah suatu nilai yang dihitung dengan memanfaatkan ilmu kriptografi. Nilai ini dihitung berdasarkan isi pesan atau dokumen, kunci yang digunakan dalam perhitungan tersebut, dan algoritma yang digunakan dalam penghitungan nilai tersebut.

Berbagai macam faktor tersebut akan menghasilkan suatu nilai unik yang akan digunakan sebagai *digital signature*. Nilai unik dimana setiap dokumen yang berbeda akan memiliki *digital signature* yang berbeda juga, bahkan perbedaan satu karakter dalam isi dokumen dapat menghasilkan *digital signature* yang berbeda^[4].

Ketika suatu dokumen sudah memiliki *digital signature*, dokumen tersebut dapat dicek *digital signature*-nya melalui proses validasi. Jika dokumen tersebut dan *digital signature*-nya sesuai, maka dokumen tersebut valid. Jika dokumen tersebut invalid, maka terdapat perubahan isi dari dokumen yang menyatakan integritas dokumen tersebut telah terganggu.

Keberadaan *digital signature* juga dapat digunakan sebagai mekanisme pertanggungjawaban oleh pembuat dokumen. Dengan adanya *digital signature* pembuat dari dokumen dapat dilacak dan ketika dokumen tersebut diminta sebagai barang bukti, pembuat dokumen tidak dapat menyangkal bahwa pihak tersebut merupakan pembuat dokumen sesungguhnya.



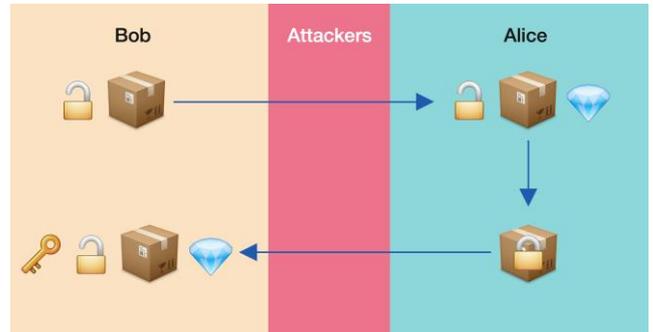
Gambar 2. Proses Pembuatan Digital Signature. Sumber: <https://www.esigngenie.com/blog/electronic-signatures-vs-digital-signatures/>

C. RSA

Rivest-Shamir-Adleman (RSA) merupakan enkripsi kunci public yang biasa digunakan dalam transmisi data. Sistem kunci public privat menggunakan kunci enkripsi dan dekripsi dalam menjamin data tidak dapat diakses oleh pihak-pihak

yang tidak seharusnya memiliki akses akan data tersebut. Kunci public digunakan untuk melakukan enkripsi data dan kunci privat digunakan untuk melakukan dekripsi data. Algoritma RSA memanfaatkan bilangan prima yang besar dalam menghasilkan kunci public dan privat.

Keamanan dari algoritma RSA ini terletak dalam penggunaan bilangan prima. Algoritma RSA memanfaatkan hasil operasi dan kombinasi dua buah bilangan prima yang besar, dimana hasil operasi ini sulit untuk difaktorisasi dan membutuhkan kekuatan komputasi yang kuat. Secara teori, jika bilangan prima atau besar kunci yang dihasilkan cukup besar, maka hampir tidak mungkin kunci dan algoritma RSA ini untuk dipecahkan tanpa mengetahui bilangan prima yang digunakan dalam operasi tersebut^[5].



Gambar 3. Ilustrasi Proses RSA. Sumber: <https://brilliant.org/wiki/rsa-encryption/>

Pembangkitan kunci RSA adalah sebagai berikut:

1. Memilih dua bilangan prima yang berbeda, yaitu p dan q
 - a. Untuk meningkatkan keamanan dari kunci, maka nilai p dan q dipilih secara acak dan memiliki panjang yang berbeda.
 - b. Nilai p dan q bersifat rahasia.
2. Menghitung nilai n , dimana $n = pq$.
 - a. Nilai n ini nantinya akan digunakan sebagai nilai modulus dari kunci public dan privat.
3. Menghitung nilai $\lambda(n)$
 - a. Nilai $\lambda(n)$ bersifat rahasia
4. Memilih suatu bilangan bulat e , dimana $1 < e < \lambda(n)$ dan nilai dari FPB e dan $\lambda(n)$ adalah 1. Hal ini menunjukkan bahwa nilai dari e dan $\lambda(n)$ merupakan pasangan koprima.
 - a. Nilai e merupakan bagian dari kunci public
5. Menentukan nilai d , dimana $d \equiv e^{-1} \pmod{\lambda(n)}$
 - a. Nilai d bersifat rahasia dan merupakan bagian dari kunci privat.

Kunci public yang dibangkitkan berupa nilai n dan nilai e , sedangkan kunci privat yang dibangkitkan berupa nilai d . Nilai p , q , dan $\lambda(n)$ harus tetap disimpan secara rahasia karena nilai-nilai tersebut dapat digunakan untuk menghitung pembangkitan kunci public dan privat.

Proses enkripsi dengan menggunakan algoritma RSA adalah sebagai berikut:

$$c^d \equiv m^e \pmod{n}$$

dimana c merupakan hasil enkripsi dan m merupakan pesan asli.

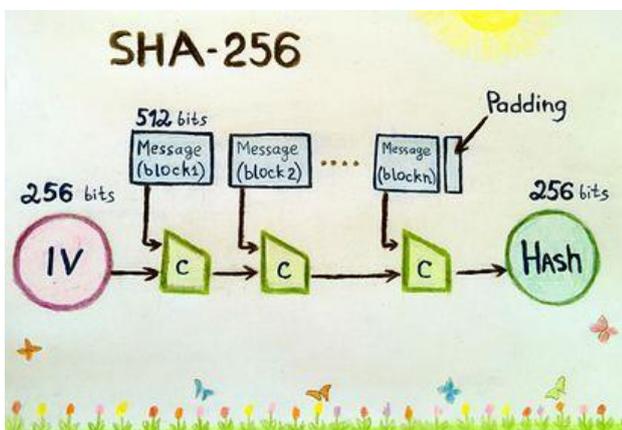
Proses dekripsi dengan menggunakan algoritma RSA adalah sebagai berikut:

$$c^d \equiv (m^e)^d \equiv m \pmod{n}$$

dimana c merupakan hasil enkripsi dan m merupakan hasil dekripsi.

D. SHA-256

Secure Hash Algorithm 2 (SHA-2) merupakan fungsi hash kriptografik sebagai kelanjutan dari algoritma SHA-1. SHA-256 merupakan salah satu algoritma yang terkumpul dalam SHA-2. SHA-256 adalah operasi matematis yang dilakukan kepada data digital untuk menghasilkan suatu nilai berdasarkan isi dari data tersebut. SHA-256 dapat digunakan untuk menjamin integritas data. SHA-256 memiliki kelebihan dibandingkan SHA-1 dibagian keamanan. Hal ini dikarenakan oleh jumlah bit yang dapat dihasilkan lebih besar dibandingkan dengan SHA-1. SHA-256 sendiri menggunakan jumlah bit sebesar 256 bit. Jumlah bit yang lebih besar ini berpengaruh terhadap kompleksitas hasil hash yang dapat dihasilkan.



Gambar 4. Ilustrasi Proses Hash Menggunakan Algoritma SHA-256. Sumber: <https://en.bitcoinwiki.org/wiki/SHA-256>

III. APLIKASI DIGITAL SIGNATURE PADA FORM BIODATA

Form biodata yang digunakan oleh penyedia layanan jasa online merupakan salah satu bentuk dokumen digital. Form biodata ini berisikan data-data pribadi dan seringkali sensitive milik pengguna. Form biodata itu juga dapat digunakan sebagai bukti penjamin ketika pengguna ingin mengajukan garansi, klaim, dan sebagainya. Namun, terkadang data yang diberikan oleh pengguna tidak disimpan atau diproses dengan baik oleh pihak penyedia layanan, sehingga dapat terjadi manipulasi data, kehilangan sebagian data, dan lain-lain.

Ketika pengguna ditanyakan kembali data tersebut untuk proses penjaminan informasi oleh pihak penyedia layanan, terkadang data yang disimpan oleh pihak penyedia layanan berbeda dengan data original. Hal ini juga seringkali terjadi

karena kesalahan dari pihak penyedia layanan. Kesalahan ini mengakibatkan pengguna kehilangan haknya untuk mendapatkan layanan.

Dengan menggunakan *digital signature*, kesalahan seperti ini dapat dihindari dan dapat dipertanggungjawabkan oleh pihak yang melakukan manipulasi data.

IV. IMPLEMENTASI

Implementasi *digital signature* yang dihasilkan merupakan *digital signature* dengan menggunakan kombinasi dari kriptografi kunci public dan fungsi hash. Sistem kriptografi kunci public yang digunakan adalah algoritma RSA dan fungsi hash yang digunakan adalah SHA-256.

A. Implementasi RSA

Rivest-Shamir-Adleman (RSA) yang merupakan sistem kriptografi kunci public digunakan dalam pembangkitan kunci public dan privat. Kunci public dan privat ini nantinya akan digunakan sebagai *signature* dari dokumen digital.

Kelas RSA berisi metode-metode yang dibutuhkan untuk menjalankan algoritma RSA dimana fungsi utamanya adalah membangkitkan kunci public dan privat, serta melakukan enkripsi dan dekripsi berdasarkan kunci public dan privat yang ada. Metode-metode yang diimplementasikan yaitu `generatePrime()`, `rsaEncrypt()`, `rsaDecrypt()`, dan `generateKeyPair()`.

B. Implementasi SHA-256

SHA-256 yang merupakan algoritma fungsi hash digunakan untuk menghasilkan nilai hash yang nantinya akan digunakan dalam membandingkan *digital signature* yang dimiliki oleh dokumen digital tersebut.

Kelas SHA berisi metode-metode yang dibutuhkan untuk menjalankan algoritma SHA-256 dimana fungsi utamanya adalah menghasilkan suatu nilai hash yang unik, serta melakukan hashing. Metode-metode yang diimplementasikan yaitu `preprocess()`, `chunk()`, `init()`, dan `hash()`.

C. Implementasi Signer

Kelas Signer berfungsi untuk melakukan proses *sign* dan *verification*. Kelas Signer akan menerima suatu dokumen digital (dalam hal ini dokumen berupa form biodata pengguna). Dokumen digital yang diterima nantinya akan diolah sebagai input dan dihasilkan suatu *digital signature* yang merepresentasikan kondisi dari dokumen digital tersebut saat *digital signature* tersebut dihasilkan.

Untuk kemudahan implementasi dari tugas ini, *digital signature* yang dihasilkan akan dimasukkan kedalam bagian paling terakhir dokumen dan diawali serta diakhiri oleh suatu tag khusus untuk menandakan bahwa teks yang berada diantara tag tersebut merupakan *digital signature*.

Jika dokumen digital yang dijadikan input sudah memiliki tag khusus tersebut, maka kelas Signer akan melakukan proses verifikasi terkait isi dari dokumen digital dan *digital signature* yang terdapat dalam dokumen digital tersebut. Setelah *digital signature* selesai diverifikasi maka program akan

mengeluarkan output berupa hasil verifikasi, jika *digital signature* dan isi dokumen sesuai, maka program akan mengeluarkan output berupa “DOKUMEN VALID”, jika *digital signature* dan isi dokumen tidak sesuai, maka program akan mengeluarkan output berupa “DOKUMEN INVALID”.

Kelas Signer berisi metode-metode yang dibutuhkan untuk menjalankan proses *sign* dan *verification*. Metode-metode yang diimplementasikan yaitu `sign()` dan `verify()`.

V. EKSPERIMEN DAN HASIL ANALISIS

A. Eksperimen

Terdapat lima eksperimen yang dilakukan dalam implementasi *digital signature* pada form biodata. Kelima eksperimen tersebut adalah:

1. Proses Sign pada form biodata.
2. Proses Verify pada form biodata.
3. Perubahan data pada form biodata.
4. Perubahan *digital signature* pada form biodata.
5. Perubahan data dan *digital signature* pada form biodata.

Hasil dari kelima eksperimen tersebut akan ditunjukkan dalam bentuk *screenshot* dengan mengikutsertakan isi dari form biodata, *digital signature*, serta hasil dari verifikasi *digital signature*.

1. Proses Sign pada form biodata

Eksperimen dilakukan dengan menggunakan form biodata dummy yang telah dibuat oleh penulis. Berikut merupakan form biodata penulis,

FORM BIODATA

Badan Pengamanan Waifu
JABODETABEK

Nama : Fritz Gerald Tjie
NIM : 13518065
TTL : Bulan, 30 Februari 2000
Agama : -
Nomor Telepon : 0123456789
NIK : 0123456789
Pekerjaan : Pengangguran
Tinggi : 200km
Berat : 200ton
Domisili : Bumi
Tanda Tangan : XXX

Tanggal Pengisian FORM
20 Desember 2021

Tertanda,
Fritz Gerald Tjie
13518065
Pluto, 20 Desember 2021

Form biodata ini akan di-*sign* dengan menggunakan kelas Signer, *digital signature* akan dimasukkan ke dalam dokumen dibagian paling akhir dari isi dokumen

FORM BIODATA

Badan Pengamanan Waifu
JABODETABEK

Nama : Fritz Gerald Tjie
NIM : 13518065
TTL : Bulan, 30 Februari 2000
Agama : -
Nomor Telepon : 0123456789
NIK : 0123456789
Pekerjaan : Pengangguran
Tinggi : 200km
Berat : 200ton
Domisili : Bumi
Tanda Tangan : XXX

Tanggal Pengisian FORM
20 Desember 2021

Tertanda,
Fritz Gerald Tjie
13518065
Pluto, 20 Desember 2021

*DS*0x609a7*DS*

2. Proses Verify pada form biodata

Eksperimen dilakukan dengan menggunakan form biodata dummy yang telah dibuat oleh penulis dan di-*sign* menggunakan kelas Signer. Pada bagian akhir dari dokumen terdapat *digital signature* dari dokumen tersebut.

FORM BIODATA

Badan Pengamanan Waifu
JABODETABEK

Nama : Fritz Gerald Tjie
NIM : 13518065
TTL : Bulan, 30 Februari 2000
Agama : -
Nomor Telepon : 0123456789
NIK : 0123456789
Pekerjaan : Pengangguran
Tinggi : 200km
Berat : 200ton
Domisili : Bumi
Tanda Tangan : XXX

Tanggal Pengisian FORM
20 Desember 2021

Tertanda,
Fritz Gerald Tjie
13518065
Pluto, 20 Desember 2021

*DS*0x609a7*DS*

Selanjutnya dokumen ini akan di-*verify* menggunakan Kelas Signer. Program akan memberikan output berupa hasil verifikasi dari dokumen yang memiliki *digital signature* tersebut.

DOKUMEN VALID

Program memberikan output “DOKUMEN VALID” yang menandakan isi dari dokumen dan *digital signature* yang terdapat pada dokumen tersebut sesuai.

3. Perubahan data pada form biodata

Eksperimen dilakukan dengan menggunakan form biodata dummy yang telah dibuat oleh penulis dan di-*sign* menggunakan kelas Signer. Pada bagian akhir dari dokumen terdapat *digital signature* dari dokumen tersebut. Data pada form biodata tersebut diubah secara manual oleh penulis.

FORM BIODATA

Badan Pengamanan Waifu
JABODETABEK

Nama : Fritz Gerald Chong
NIM : 13518065
TTL : Bulan, 30 Februari 2000
Agama : -
Nomor Telepon : 0123456789
NIK : 0123456789
Pekerjaan : Pengangguran
Tinggi : 200km
Berat : 200ton
Domisili : Bumi
Tanda Tangan : XXX

Tanggal Pengisian FORM
20 Desember 2021

Tertanda,
Fritz Gerald Tjie
13518065
Pluto, 20 Desember 2021

*DS*0x609a7*DS*

Penulis mengubah nama dari “Fritz Gerald Tjie” menjadi “Fritz Gerald Chong”. Kemudian dokumen yang telah dimanipulasi ini akan diverifikasi oleh program.

DOKUMEN INVALID

Program memberikan output “DOKUMEN INVALID” yang menandakan isi dari dokumen dan *digital signature* yang terdapat pada dokumen tersebut tidak sesuai, hal ini menandakan bahwa dokumen telah dimanipulasi oleh pihak yang tidak bertanggung jawab.

4. Perubahan *digital signature* pada form biodata

Eksperimen dilakukan dengan menggunakan form biodata dummy yang telah dibuat oleh penulis dan di-*sign* menggunakan kelas Signer. Pada bagian akhir dari dokumen terdapat *digital signature* dari dokumen tersebut. *Digital signature* pada form biodata tersebut diubah secara manual oleh penulis.

FORM BIODATA
Badan Pengamanan Waifu
JABODETABEK

Nama : Fritz Gerald Tjie
NIM : 13518065
TTL : Bulan, 30 Februari 2000
Agama : -
Nomor Telepon : 0123456789
NIK : 0123456789
Pekerjaan : Pengangguran
Tinggi : 200km
Berat : 200ton
Domisili : Bumi
Tanda Tangan : XXX

Tanggal Pengisian FORM
20 Desember 2021

Tertanda,
Fritz Gerald Tjie
13518065
Pluto, 20 Desember 2021

*DS*0x6666*DS*

Penulis mengubah *digital signature* dari “0x609a7” menjadi “0x6666”. Kemudian dokumen yang telah dimanipulasi ini akan diverifikasi oleh program.

DOKUMEN INVALID

Program memberikan output “DOKUMEN INVALID” yang menandakan isi dari dokumen dan *digital signature* yang terdapat pada dokumen tersebut tidak sesuai, hal ini menandakan bahwa dokumen telah dimanipulasi oleh pihak yang tidak bertanggung jawab.

5. Perubahan data dan *digital signature* pada form biodata

Eksperimen dilakukan dengan menggunakan form biodata dummy yang telah dibuat oleh penulis dan di-sign menggunakan kelas Signer. Pada bagian akhir dari dokumen terdapat *digital signature* dari dokumen tersebut. Data dan *digital signature* pada form biodata tersebut diubah secara manual oleh penulis.

FORM BIODATA
Badan Pengamanan Waifu
JABODETABEK

Nama : Fritz Gerald Chong
NIM : 13518065
TTL : Bulan, 30 Februari 2000
Agama : -
Nomor Telepon : 0123456789
NIK : 0123456789
Pekerjaan : Pengangguran
Tinggi : 200km
Berat : 200ton
Domisili : Bumi
Tanda Tangan : XXX

Tanggal Pengisian FORM
20 Desember 2021

Tertanda,
Fritz Gerald Tjie
13518065
Pluto, 20 Desember 2021

*DS*0x6666*DS*

Penulis mengubah nama dari “Fritz Gerald Tjie” menjadi “Fritz Gerald Chong” dan mengubah *digital signature* dari “0x609a7” menjadi “0x6666”. Kemudian dokumen yang telah dimanipulasi ini akan diverifikasi oleh program.

DOKUMEN INVALID

Program memberikan output “DOKUMEN INVALID” yang menandakan isi dari dokumen dan *digital signature* yang terdapat pada dokumen tersebut tidak sesuai, hal ini menandakan bahwa dokumen telah dimanipulasi oleh pihak yang tidak bertanggung jawab.

B. Hasil Analisis

Berdasarkan eksperimen yang dilakukan, pemanfaatan *digital signature* dengan menggunakan kombinasi RSA dan SHA-256 terimplementasi dengan baik. Kelima eksperimen yang dilakukan menunjukkan hasil yang diharapkan dari eksperimen tersebut.

VI. KESIMPULAN DAN SARAN

Digital signature dapat mengatasi permasalahan integritas data dan manipulasi data yang dapat dilakukan oleh oknum-oknum yang tidak bertanggung jawab. Dengan adanya *digital signature*, data pribadi pengguna dapat dengan aman dijamin integritasnya dan verifikasi dari data tersebut dapat dengan mudah dilakukan.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan puji syukur kepada Tuhan Yang Maha Esa, karena telah diberikan kemudahan dalam menyelesaikan karya tulis ini. Selain itu, penulis juga ingin mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T. yang telah memberikan kesempatan dan wawasan mengenai ilmu kriptografi dengan jelas sehingga penulis dapat menyelesaikan penulisan karya tulis ini.

REFERENSI

- [1] <https://kbbi.web.id/data>
- [2] <https://kbbi.web.id/biodata>
- [3] HR, EMPTrust. "What is Digital Signature- How it works, Benefits, Objectives, Concept"
- [4] R. Munir, "Tanda Tangan Digital," Teknik Informatika STEI - ITB, Bandung.
- [5] Casteivecchi, Davide, [*Quantum-computing pioneer warns of complacency over Internet security*](#), Nature, October 30, 2020 interview of [Peter Shor](#).

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



Fritz Gerald Tjie - 13518065