Implementasi Digital Signature pada Kartu Garansi Pembelian Barang

Hafidz Nur Rahman Ghozali - 13520117
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520117@std.stei.itb.ac.id

***Abstract*—Kartu garansi pembelian barang merupakan dokumen yang berisi jaminan bagi konsumen bahwa penjual memiliki tanggung jawab untuk mengganti atau memperbaiki produk yang rusak dalam kurun waktu tertentu setelah pembelian. Namun, kartu garansi tersebut seringkali dimanipulasi atau dipalsukan. Tanda tangan digital dapat digunakan untuk memberikan jaminan keaslian pada dokumen tersebut.**

Keywords—Kartu garansi, tanda tangan digital

I. Pendahuluan

Saat ini, transaksi elektronik sangat masif terjadi di kalangan masyarakat Indonesia. Konsumen sering melakukan pembelian barang, baik secara *online* maupun *offline*, dan mengharapkan adanya jaminan atas barang yang dibeli. Penjual biasanya menyediakan jaminan/garansi sesuai dengan barang yang dibeli oleh konsumen. garansi pembelian barang adalah dokumen yang menyatakan bahwa penjual akan bertanggung jawab untuk memperbaiki atau mengganti produk yang rusak dalam kurun waktu tertentu setelah pembelian.

Kartu garansi pembelian seringkali diberikan dalam bentuk fisik. Kartu tersebut dapat hilang atau rusak sehingga penjual kesulitan dalam melakukan validasi ketika konsumen ingin melakukan klaim garansi. Selain itu, kartu garansi dalam bentuk fisik juga sangat rawan untuk dipalsukan atau dimanipulasi. Dalam kartu garansi fisik, penjual dapat membubuhkan tanda tangan secara asli dan memberikan cap toko, namun hal tersebut masih terdapat celah pemalsuan.

Kartu garansi dalam bentuk digital memberikan keleluasaan bagi penjual dan pembeli dalam menyimpan dokumen tersebut. Untuk menyelesaikan selah pemalsuan, tanda tangan digital merupakan pilihan yang sangat baik. Tanda tangan digital pada dokumen kartu garansi pembelian dapat menjamin keaslian dokumen dan mendukung layanan anti penyangkalan.

II. Dasar Teori

A. Kartu Garansi Pembelian Barang

Kartu garansi pembelian adalah dokumen yang diberikan oleh produsen atau penjual kepada pembeli sebagai jaminan bahwa produk yang dibeli akan berfungsi dengan baik dalam jangka waktu tertentu. Kartu garansi pembelian biasanya mencakup beberapa informasi, seperti detail produk, durasi garansi, syarat dan ketentuan, tanggung jawab penjual/produsen, pengecualian garansi, dan proses klaim garansi. Kartu garansi pembelian sangat berguna dalam pembelian barang yang mahal. Kartu garansi harus dapat divalidasi kebenarannya, baik dari penjual atau pembeli. Kartu garansi sangat rawan untuk dimodifikasi sehingga dapat merugikan pihak penjual/produsen.

Gambar 1. Contoh kartu garansi pembelian barang

B. File PDF

PDF atau *Portable Document Format* merupakan sebuah format berkas yang dibuat oleh Adobe Systems pada tahun 1993. Format berkas ini mendukung representasi dokumen yang berisi teks, huruf, citra, dan grafik dua dimensi [4]. Format dokumen pdf bersifat *portable* sehingga dokumen dapat dibuka di berbagai perangkat dengan program pembaca pdf dan. Dokumen dengan format file pdf akan menampilkan tampilan yang sama dengan versi cetak dari dokumen tersebut. Dokumen pdf akan memiliki metadata yang biasanya akan berisi judul, penulis, dan tanggal modifikasi dokumen. Metadata pada file pdf juga dapat dimodifikasi oleh pengguna.

C. Kriptografi

Menurut Schneier (1996) [1], Kriptografi merupakan sebuah ilmu dan seni untuk menjaga keamanan pesan. Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, Menezes (1996) [2]. Terdapat 4 aspek keamanan informasi yang dijaga di dalam kriptografi, yaitu:

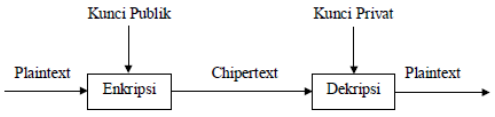
1) Kerahasiaan *(confidentiality)*, yaitu layanan yang menjaga isi pesan agar tidak dapat dibaca oleh pihak yang tidak memiliki hak untuk membacanya.
2) Integritas Data *(integrity)*, yaitu layanan yang menjamin bahwa pesan bersifat asli atau utuh dan tidak berubah selama pengiriman pesan.
3) Otentikasi *(authentication)*, yaitu layanan untuk mengidentifikasi entitas yang sedang berkomunikasi dan kebenaran sumber pesan.
4) Nirsangkal *(non-repudiation)*, yaitu layanan untuk mencegah entitas yang melakukan komunikasi melakukan penyangkalan pengiriman atau penerimaan pesan.

Sistem kriptografi terdiri dari beberapa komponen, yaitu algoritma kriptografi, plainteks, cipherteks, dan kunci. Berdasarkan jenis kunci, algoritma kriptografi terbagi menjadi 2, yaitu:

1) Algoritma kunci simetri *(symmetric key algorithm)*, yaitu algoritma enkripsi dan dekripsi yang menggunakan kunci yang sama
2) Algoritma kunci asimetri *(asymmetric key algorithm)*, yaitu algoritma enkripsi dan dekripsinya menggunakan kunci yang berbeda. Algoritma ini juga disebut sebagai teknik kriptografi kunci publik

D. Kriptografi Kunci Publik

Kriptografi kunci publik merupakan salah satu teknik dalam kriptografi yang menggunakan dua kunci yang berbeda untuk melakukan enkripsi dan dekripsi pesan. Terdapat dua buah kunci yang digunakan dalam algoritma ini, yaitu kunci privat dan kunci publik. Kunci privat bersifat rahasia dan tidak boleh diketahui oleh orang lain. Sedangkan kunci publik bersifat terbuka dan dapat disebarkan kepada orang lain.



Gambar 2. Proses enkripsi dan dekripsi kriptografi kunci publik

Dalam algoritma ini, kunci publik digunakan untuk melakukan enkripsi pesan yang akan mengubah plainteks menjadi ciphertext. Kunci privat digunakan untuk mendekripsi pesan dari ciphertext menjadi plainteks semula. Dengan sistem ini, pihak yang ingin berkomunikasi tidak perlu menyepakati kunci terlebih dahulu. Kedua pihak hanya perlu menyimpan kunci publiknya masing-masing dan mengetahui kunci publik milik pihak yang lain.

E. Hash

Hash merupakan sebuah mekanisme untuk memetakan pesan yang berukuran sembarang menjadi pesan dengan panjang yang tetap [3]. Pesan hasil pemetaan tersebut biasa disebut sebagai *message digest*. Fungsi hash hanya bersifat satu arah sehingga plainteks tidak dapat diperoleh kembali dari *message digest* yang diketahui.

Fungsi hash memiliki 3 karakteristik utama, yaitu:

1) *collision resistance*, yaitu kemampuan fungsi hash untuk menghindari atau meminimalkan kemungkinan terjadinya kolisi, yaitu ketika dua masukan berbeda menghasilkan nilai hash yang sama, yaitu $H(x) = H(y)$ dengan H adalah fungsi hash.
2) *preimage resistance*, yaitu kemampuan fungsi hash untuk menghindari penemuan masukan berdasarkan nilai hash yang diberikan. Fungsi hash yang baik harus sulit menemukan x sehingga $H(x) = y$ dengan y adalah nilai hash yang diketahui.
3) *second preimage resistance*, yaitu kemampuan fungsi hash untuk menghindari penemuan masukan kedua yang menghasilkan nilai hash yang sama dengan masukan yang telah diketahui. Sulit untuk menemukan y yang memenuhi $H(x) = H(y)$ dengan x merupakan masukan yang telah diketahui.

Fungsi hash memberikan layanan integritas data dengan membandingkan *message digest* yang dihasilkan oleh pesan. Apabila *message digest* dari pesan yang dikirimkan berbeda dengan *message digest* yang dihasilkan dari pesan yang diterima, maka pesan tersebut telah dimodifikasi selama pengiriman.

F. Tanda Tangan Digital

Tanda tangan digital merupakan sebuah metode untuk mengamankan keamanan informasi, keaslian, dan otentikasi dokumen atau data elektronik [3]. Tanda tangan digital digunakan untuk memastikan bahwa pesan atau dokumen elektronik tidak diubah dan berasal dari sumber yang sah. Tanda tangan digital pada sebuah pesan/dokumen merupakan nilai kriptografis yang bergantung pada isi pesan/dokumen. Oleh karena itu, tanda tangan digital setiap dokumen pasti berbeda dengan dokumen yang lain, tidak seperti tanda tangan biasa.

Tanda tangan digital memberikan layanan keamanan kriptografi berupa integritas data, otentikasi, dan nirsangkal.

1) Integritas data

   Tanda tangan digital dapat digunakan untuk memastikan keaslian pesan dengan melakukan verifikasi terhadap tanda tangan tersebut. Tanda tangan digital sangat bergantung pada isi pesan/dokumen sehingga apabila terjadi perubahan/modifikasi pada isi pesan maka tanda tangan digital tersebut tidak valid.

2) Otentikasi

   Tanda tangan digital memberikan keyakinan pada kedua pihak yang berkomunikasi untuk bisa melakukan verifikasi kebenaran pengirim pesan.

Apabila tanda tangan valid maka pesan tersebut berasal dari pengirim yang sah.

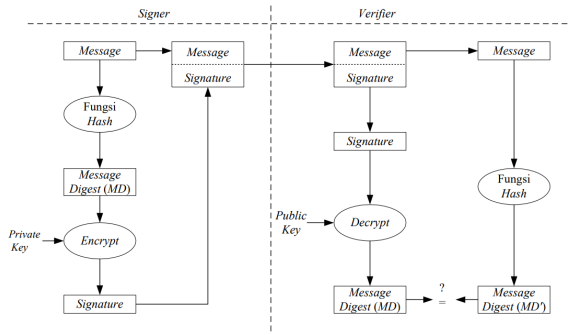
3) Nirsangkal

Tanda tangan digital memberikan layanan sehingga pengirim tidak dapat menyangkal bahwa tanda tangan tersebut merupakan tanda tangan yang berasal dari dirinya. Tanda tangan digital dibangun menggunakan kunci privat pengirim sehingga tanda tangan tersebut dapat digunakan sebagai bukti pengiriman.

Tanda tangan digital dapat diimplementasikan dengan 2 cara, yaitu dengan mengenkripsi pesan dan menggunakan kombinasi fungsi hash dan kriptografi kunci publik. Tanda tangan digital dengan mengenkripsi pesan digunakan ketika pesan yang dikirimkan bersifat rahasia. Enkripsi pesan dapat menggunakan kriptografi kunci simetri dan kriptografi kunci publik. Enkripsi dengan kriptografi kunci simetri dapat memberikan layanan otentikasi namun tidak dapat memberikan layanan nirsangkal.

Sedangkan cara kedua digunakan ketika pesan yang dikirimkan tidak perlu dirahasiakan. Berikut merupakan langkah-langkah penandatanganan dengan menggunakan kombinasi fungsi hash dan kriptografi kunci publik.

1) Pengirim menghitung nilai hash dari pesan yang akan dikirim dan menghasilkan *message digest*
2) *Message digest* tersebut dienkripsi menggunakan kunci privat pengirim dan menghasilkan *signature*/tanda tangan digital
3) Pengirim melakukan pengiriman pesan beserta tanda tangan digitalnya kepada penerima
4) Penerima menghitung nilai hash dari pesan yang diterima dan menghasilkan *message digest 1*
5) Penerima mendekripsi *signature*/tanda tangan digital menggunakan kunci publik pengirim dan menghasilkan *message digest 2*
6) Penerima melakukan verifikasi *signature* dengan membandingkan *message digest 1* dan *2*. Apabila kedua *message digest* bernilai sama, maka *signature* tersebut valid. Apabila nilainya berbeda, makan *signature* tersebut tidak valid dan pesannya dapat dianggap tidak asli



Gambar 3. Tanda tangan digital dengan kombinasi fungsi hash dan kriptografi kunci publik

G. Algoritma ECDSA

Algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) merupakan pengembangan dari *Digital Signature Algorithm* (DSA) biasa. Algoritma ini menggunakan *Elliptical Curve* untuk komponen kriptografi kunci publik. ECDSA menggunakan pasangan kunci privat dan kunci publik dalam pembuatan dan validasi tanda tangan digital. ECDSA memiliki keunggulan, yaitu memberikan keamanan yang sama dengan algoritma DSA namun dengan ukuran kunci yang lebih kecil karena berbasis kurva eliptik.

Terdapat 3 tahapan dalam algoritma ECDSA, yaitu *Key generation, Sign,* dan *Verify*

1) Key generation

Tahap *key generation* merupakan tahap pembangkitan kunci privat dan kunci publik sesuai dengan *Elliptic Curve Cryptography*. Kunci privat akan digunakan untuk melakukan enkripsi/tahap *sign*. Sedangkan kunci publik akan digunakan untuk melakukan dekripsi/tahap *verify*.

2) Sign

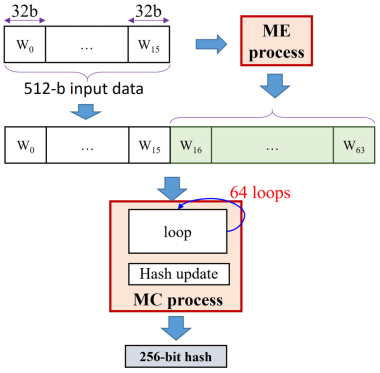
Tahap *sign* merupakan tahap penandatanganan pesan. Tahap ini mencakup tahapan *hashing* pada pesan dan dilanjutkan dengan enkripsi dengan kunci privat yang telah dibangkitkan sebelumnya.

3) Verify

Tahap *verify* merupakan tahap pengecekan keabsahan *signature*. Keaslian pesan diverifikasi pada tahap ini. Tahap ini mencakup *hashing* pada pesan dan mengecek kesamaan hasil dekripsi *signature* dengan kunci publik.

H. Algoritma Hash SHA-256

Algoritma SHA-256 merupakan algoritma *hash* yang menyempurnakan pendahulunya, yaitu SHA-1 dan SHA-2. Algoritma SHA-256 akan menghasilkan nilai *hash* dengan panjang yang tetap, yaitu 256 bit.



Gambar 4. Tahapan algoritma SHA-256

Terdapat 2 proses, yaitu Message Expander (ME) dan Message Compressor (MC). Proses ME akan mengekspansi pesan 512 bit menjadi 64 *chunk* berukuran 32 bit. Pada 16 putaran pertama, pesan akan dipecah menjadi 16 *chunk*

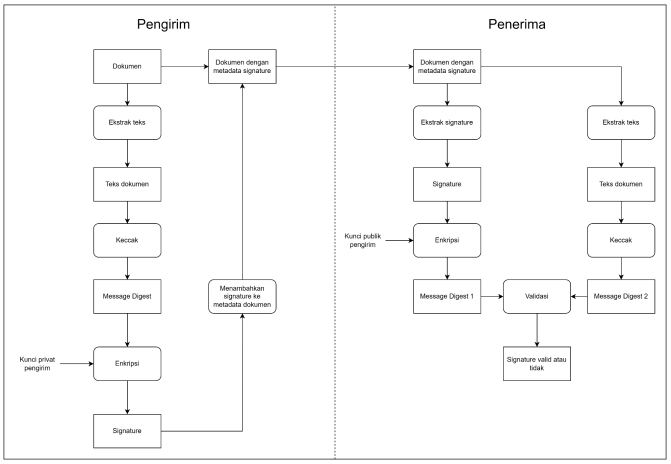
berukuran 32 bit. Pada sisa 48 putaran, *chunk-chunk* tersebut akan diproses sesuai dengan persamaan SHA-256. Proses MC akan melakukan komputasi yang akan menghasilkan nilai hash 256 bit dari setiap proses ME. Nilai hash pada putaran terakhir akan menjadi nilai hash yang akan dikeluarkan oleh algoritma SHA-256 ini.s

III. Desain Penandatanganan dan Implementasi

A. Deskripsi

Kartu garansi pembelian barang yang akan ditandatangani merupakan dokumen dalam format pdf. Tanda tangan digital akan dibangkitkan menggunakan teks yang diekstrak dari dokumen. Pemilihan teks ini didasari oleh kemudahan dalam melakukan ekstraksi teks dari dokumen pdf. Tanda tangan digital yang dibangkitkan akan disisipkan ke dalam metadata dokumen. Penyisipan ini tidak akan mengganggu isi dari dokumen. Perubahan metadata dokumen seperti judul juga tidak akan mengganggu keaslian dari dokumen. Hal ini didasarkan pada fleksibilitas penyimpanan dokumen bagi konsumen. Penyisipan tanda tangan digital pada metadata dokumen juga relatif mudah dilakukan dan juga mudah diekstraksi sehingga memudahkan penjual dalam melakukan validasi.

B. Desain Penandatanganan



Gambar 5. Skema penandatanganan

Desain penandatanganan kartu garansi pembelian mengikuti skema pada gambar 4. Skema tersebut menggunakan algoritma SHA-256 sebagai fungsi hash dan algoritma *Elliptic Curve Cryptography* dengan kurva NIST256p sebagai algoritma pembangkitan kunci.

Pengirim merepresentasikan penjual karena dokumen kartu garansi diterbitkan oleh penjual. Konsumen dan penjual dapat berperan sebagai penerima yang dapat melakukan validasi terhadap dokumen kartu garansi pembelian.

Pengirim perlu membangkitkan kunci dengan algoritma yang sudah ditetapkan. Kunci tersebut akan digunakan untuk mengenkripsi dan mendekripsi *message digest*. Berikut merupakan alur penandatanganan dokumen pada pengirim

1) Teks diekstrak dari dokumen yang akan ditandatangani
2) Nilai hash dihitung dari teks hasil ekstraksi dokumen, menghasilkan *message digest*
3) *Message digest* tersebut dienkripsi menggunakan kunci publik pengirim, menghasilkan *signature*
4) *Signature* tersebut akan disisipkan ke dalam metadata berkas pdf menghasilkan file pdf yang baru

Berikut merupakan alur validasi tanda tangan pada sisi penerima:

1) *Signature* diekstrak dari metadata berkas pdf
2) *Signature* tersebut didekripsi menggunakan kunci publik pengirim, menghasilkan *message digest 1*
3) Teks diekstrak dari dokumen
4) Nilai hash dihitung dari teks hasil ekstraksi dokumen tersebut, menghasilkan *message digest 2*
5) Penerima melakukan validasi dengan membandingkan kedua *message digest* yang diperoleh. Apabila keduanya bernilai sama, maka *signature* tersebut valid dan dokumen dapat dijamin keasliannya. Namun, apabila keduanya berbeda, maka *signature* tersebut tidak valid dan dokumen tersebut dapat dianggap sudah dimodifikasi.

C. Implementasi

Program tanda tangan digital diimplementasikan dengan menggunakan kombinasi fungsi hash dan kriptografi kunci publik. Program dibuat dalam bahasa Python dan menggunakan kakas *ecdsa* untuk algoritma kriptografi dan kakas *PyPDF2* untuk pembacaan dan penulisan file pdf. Fungsi hash yang digunakan dalam algoritma ini adalah algoritma SHA-256. Pembangkitan kunci privat dan kunci publik menggunakan algoritma *Elliptic Curve Cryptography* dengan kurva NIST256p. Penulis mengimplementasikan beberapa menu pada program, yaitu

1) Pembangkitan kunci privat dan kunci publik
2) Penandatanganan file pdf
3) Validasi tanda tangan pada file pdf
4) Pengecekan tanda tangan pada file pdf

IV. Pengujian dan Analisis

Program Tanda Tangan Digital menyediakan 6 menu, yaitu:

```
Please select a Menu
1. Generate Private Key and Public Key
2. Show Private Key and Public Key
3. Create Signature
4. Validate Signature
5. Get Signature File
6. Exit Program
Enter your choice:
```

Gambar 6. Tampilan menu program

Sebelum melakukan tanda tangan digital, pengguna harus membangkitkan kunci privat dan kunci publik terlebih dahulu. Pembangkitan kunci tersebut dilakukan dengan memilih menu 1 pada program. Berikut merupakan kunci yang akan digunakan dalam tahap pengujian ini

```
Private Key:
6c662d635ce365defbac2c431b9dc3ee00a0c971d
9f7667b3038d202d29b643d
Public Key:
5fb55b06cffc15583d92e773abeb41516b3463974
ebfa2f3df06371e25787ae6755c523c7697a40ba5
aef11e9233743236cc415a1933ec945a571c0d801
628b3
```

Setelah membangkitkan kunci, pengguna dapat menampilkan kembali kunci yang telah dibangkitkan dengan menu 2. Pengguna dapat melakukan tanda tangan digital dengan menu 3. Pada pengujian ini, dokumen kartu garansi yang digunakan adalah dokumen yang terdapat pada gambar 1 dalam format pdf.

```
Enter your choice: 3
Enter filename: kartu-garansi.pdf
Enter Private key: 6c662d635ce365defbac2c431b9dc3ee00a0c971d9f7667b3038d202d29b643d
Enter result filename: kartu-garansi-signed.pdf
File written successfully
```

Gambar 7. Pembuatan *signature*

Pengguna perlu memasukkan nama berkas dan kunci privat yang akan digunakan untuk menandatangani dokumen tersebut. Setelah itu, pengguna diminta memasukkan nama berkas baru setelah ditambahkan *signature*.

Pengguna dapat melakukan validasi *signature* pada dokumen dengan memilih menu 4. Pengguna perlu memasukkan nama berkas dan kunci publik pengirim.

```
Please select a Menu
1. Generate Private Key and Public Key
2. Show Private Key and Public Key
3. Create Signature
4. Validate Signature
5. Get Signature File
6. Exit Program
Enter your choice: 4
Enter filename: kartu-garansi-signed.pdf
Enter Public Key: 5fb55b06cffc15583d92e773abeb41516b3463974ebfa2f3df06371e25787ae6755c523c7697a40ba5a
ef11e9233743236cc415a1933ec945a571c0d801628b3
Signature is valid
```

Gambar 8. Validasi *signature*

Untuk menguji validitas *signature*, dokumen tersebut akan dimodifikasi dengan menambahkan teks pada file yang telah ditandatangani.

Gambar 9. Dokumen yang telah dimodifikasi

```
Enter your choice: 4
Enter filename: kartu-garansi-signed-modified1.pdf
Enter Public Key: 5fb55b06cffc15583d92e773abeb41516b3463974ebfa2f3df06371e25787ae6755c523c7697a40ba5a
ef11e9233743236cc415a1933ec945a571c0d801628b3
Signature is invalid
```

Gambar 10. *Signature* pada dokumen yang telah dimodifikasi gagal divalidasi

Pengujian juga dilakukan dengan memasukkan kunci publik yang berbeda dengan kunci publik yang seharusnya. Kunci publik yang digunakan telah dimodifikasi pada dua karakter terakhir dari "`b3`" menjadi "`a1`"

```
Enter your choice: 4
Enter filename: kartu-garansi-signed.pdf
Enter Public Key: 5fb55b06cffc15583d92e773abeb41516b3463974ebfa2f3df06371e25787ae6755c523c7697a40ba5a
ef11e9233743236cc415a1933ec945a571c0d801628a1
Signature is invalid
```

Gambar 11. *Signature* pada dokumen yang telah dimodifikasi gagal divalidasi

Signature pada dokumen tersebut dianggap invalid karena kunci publik yang dimasukkan tidak sesuai dengan yang seharusnya.

Pengujian juga dilakukan dengan melakukan modifikasi pada metadata signature pada berkas.

```
Enter your choice: 5
Enter filename: kartu-garansi-signed-modified2.pdf
Signature: b69b03c717d8279f57993b7c9cc6ed98c247fc17d22ac4c09325eb6651a0ef27b31e2dd2ac2f846ae44fb194ad
3e2a216d6cc973d321f25c1f9749e1d285f60a
```

Gambar 12. *Signature* pada berkas setelah dimodifikasi

Modifikasi pada dokumen dilakukan dengan mengganti karakter terakhir dari "`9`" menjadi "`a`".

```
Enter your choice: 4
Enter filename: kartu-garansi-signed-modified2.pdf
Enter Public Key: 5fb55b06cffc15583d92e773abeb41516b3463974ebfa2f3df06371e25787ae6755c523c7697a40ba5a
ef11e9233743236cc415a1933ec945a571c0d801628b3
Signature is invalid
```

Gambar 13. *Signature* pada dokumen yang telah dimodifikasi gagal divalidasi

Setelah *signature* dimodifikasi, maka keaslian dokumen tersebut tidak dapat dipertanggungjawabkan sehingga *signature* tersebut dianggap invalid.

Berdasarkan pengujian yang dilakukan, pemanfaatan tanda tangan digital dengan kombinasi fungsi hash SHA-256 dan algoritma kunci publik dengan *Elliptic Curve Cryptography* telah diimplementasikan dengan baik.

V. KESIMPULAN DAN SARAN

Tanda tangan digital dapat diimplementasikan dengan kombinasi fungsi hash dengan algoritma SHA-256 dan kriptografi kunci publik *Elliptic Curve Cryptography* P256. Tanda tangan digital dilakukan untuk memastikan keaslian kartu garansi pembelian barang. Tanda tangan digital tersebut membantu penjual/produsen dalam melakukan verifikasi kartu garansi pembelian barang. Berdasarkan pengujian yang telah

dilakukan, program yang dibuat sukses melakukan verifikasi keaslian kartu garansi.

Pesan yang digunakan dalam penyusunan *signature* hanya memperhitungkan konten teks pada file pdf. Program tidak akan menghiraukan konten gambar yang ada di dalam file pdf. Sebagai peningkatan program, penulis menyarankan untuk menggunakan konten selain teks untuk membangkitkan *signature* pada file pdf.

Pranala Kode Program

Kode program dapat diakses melalui pranala berikut https://github.com/hafidznrg/ECDSA-pdf

Ucapan Terima Kasih

Pertama, penulis mengucap syukur kepada Tuhan karena atas rahmatnya penulis dapat menyelesaikan makalah ini dengan baik. Penulis juga mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam makalah ini. Penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada bapak Dr. Ir. Rinaldi Munir, M.T. selaku dosen pengajar Mata Kuliah IF4020 Kriptografi Tahun Ajaran 2022/2023 yang telah mengajarkan berbagai pengetahuan sehingga penulis mampu menyelesaikan makalah ini.

Referensi

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[1] B. Schneier, Applied Cryptography, 2 ed., John Wiley & Sons, 1996.

[2] P. v. O. S. V. Alfred Menezes, Handbook of Applied Cryptography, CRC Press, 1996.

[3] Munir R. Kriptografi. 2023.

[4] Adobe Systems. Document Management - Portable Document Format Part 1.7. 2008

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, 21 Mei 2023

Hafidz Nur Rahman Ghozali