Digital Signature pada STNK Untuk Memperketat Keamanan Parkir Kendaraan Bermotor di ITB

Indra Mukmin - 13506082
Jurusan Teknik Informatika ITB, Jalan Ganesha 10 Bandung 40132, email: if16082@students.if.itb.ac.id

Abstraksi

Surat Tanda Nomor Kendaraan (STNK) merupakan tanda bukti pendaftaran dan pengesahan suatu kendaraan bermotor berdasarkan identitas dan kepemilikannya yang telah terdaftar. STNK berisi identitas kepemilikan dan identitas kendaraan bermotor. Salah satu informasi tersebut yaitu nomor polisi dan masa berlakunya yang tertera dalam STNK yang kemudian dicetak pada plat nomor untuk dipasang pada kendaraan bermotor yang bersangkutan. Keberadaan STNK ini mutlak menjadi tanda bukti kepemilikan kendaraan yang otentik si pemilik kendaraan.

Dalam beberapa tahun terakhir, tindak kejahatan pencurian kendaraan bermotor khususnya motor, marak terjadi di lingkungan kampus ITB. Banyak motor yang di parkir di area parkir kendaraan di dalam kampus hilang dicuri oleh komplotan pencuri yang beroperasi cukup lihai, terbukti dengan sulitnya menangkap si pelaku pencurian tersebut. Menanggapi permasalahan ini, pihak ITB akhirnya melakukan beberapa tindakan pencegahan, salah satunya yaitu pengecekan STNK untuk setiap kendaraan bermotor yang akan keluar dari area parkir.

Berkaitan dengan masalah keamanan parkir di ITB, penulis akhirnya mencoba menawarkan solusi tambahan untuk meningkatkan keamanan otentikasi kepemilikan kendaraan bermotor. Caranya adalah dengan membuat digital signature untuk STNK dengan memanfaatkan nomor polisi yang tertera pada STNK yang nilainya pasti unik. Dengan adanya digital signature pada STNK ini, diharapkan tingkat validitas otentikasi menjadi lebih tinggi sekaligus dapat pula menanggulangi pemalsuan STNK yang mungkin terjadi. Hal ini disebabkan, pemilik yang sah lah yang hanya memiliki kunci privat yang akan digunakan untuk otentikasi sehingga pihak yang tidak berhak akan memberikan message diggest yang berbeda dengan message digest hasil dekripsi digital signature pada STNK.

Sekarang ini, digital signature telah banyak digunakan mengingat aspek keamanan yang ditawarkan cukup lengkap antara lain penangan masalah kerahasiaan pesan, otentikasi, keaslian pesan, dan nirpenyangkalan. Untuk makalah ini, algoritma digital signature yang dipakai adalah RSA Algorithm dengan menggunakan fungsi hash MD5.

Dalam makalah ini, penulis juga akan memaparkan mengenai kelebihan serta kelemahan penggunaan digital signature pada STNK.

Kata Kunci

Digital signature, STNK, MD5, RSA, pencurian

1. PENDAHULUAN

Kriptografi telah dipergunakan secara luas untuk mengenkripsi dan menjaga kerahasiaan pesan maupun informasi penting. Utilitas kriptografi ini sendiri tidak lepas dari aspek keamanan yang ditawarkannya antara lain: kerahasiaan (*confidentiality*), integritas data (*data integrity*), otentikasi (*authentication*), dan nirpenyang-kalan (*non-repudiation*). Selain fungsionalitasnya dalam hal penjagaan kerahasiaan pesan, kriptografi juga dapat diaplikasikan dalam bentuk lain semisal penggunaan kriptografi untuk pencegahan dan penanggulangan masalah pencurian kendaaraan bermotor. Dalam hal ini, salah satu contoh aplikasi kriptografi yang dapat digunakan adalah tanda tangan digital (*digital signature*).

2. TANDA TANGAN DIGITAL

Tanda tangan telah digunakan sejak berabad – abad lalu untuk membuktikan otentikasi dokumen. Adanya tanda tangan pada dokumen ini, membuat dokumen menjadi tidak mudah diubah oleh pihak yang tidak berhak. Fungsi tanda tangan ini juga diterapkan pada data digital lewat tanda tangan digital. Dengan adanya tanda tangan digital ini, integritas data dapat dijamin. Disamping itu, tanda tangan digital juga dapat digunakan untuk membuktikan asal pesan dan masalah nirpenyangkalan. Penandatangan pesan dapat dilakukan dengan salah satu dari dua cara berikut:

a. Enkripsi pesan
b. Tanda tangan digital dengan fungsi *hash*

Terdapat dua tahap utama dalam proses penandatanganan ini. Tahap pertama adalah proses untuk memperoleh *message diggest* dari pesan dengan menggunakan fungsi *hash* satu arah. Tahap kedua yaitu pengenkripsian *message diggest* yang telah diperoleh sebelumnya dengan menggunakan kunci privat pemilik dokumen. Hasil tahap kedua berupa tanda tangan digital untuk dokumen tersebut. Selanjutnya, pengirim dapat mengirimkan dokumen beserta tanda tangan digitalnya.

Untuk verifikasi tanda tangan digital, juga terdapat dua tahap utama. Pertama, dilakukan dekripsi terhadap tanda tangan digital dengan menggunakan kunci publik pengirim untuk mendapatkan *message diggest* pesan. Selanjutnya pada tahap kedua, pesan dikenakan dengan fungsi *hash* satu arah. *Message diggest* yang diperoleh dari fungsi *hash* tadi kemudian dibandingkan dengan *message diggest* yang diperoleh dari dekripsi tanda tangan digital yang disertakan pada dokumen tersebut. Apabila kedua *message diggest* sama, maka pesan yang dikirimkan masih asli. Jika tidak sama, maka pesan sudah tidak asli lagi atau telah mengalami modifikasi.

Dua algoritma tanda tangan yang digunakan secara luas adalah *RSA* dan *ElGamal*. Pada *RSA*, algoritma enkripsi dan dekripsi identik, sehingga proses tanda tangan dan verifikasi juga identik.

3. ALGORITMA *RSA*

Algoritma *RSA* dibuat oleh 3 orang peneliti dari *MIT* (*Massachussets Institute of Technology*) pada tahun 1976, yaitu: Ron Rivest, Adi Shamir, dan Leonard Adleman. Keamanan algoritma *RSA* terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor – faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor – faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma *RSA* tetap terjamin.

Algoritma *RSA* memiliki properti sebagai berikut:

1. p dan q bilangan prima
2. $n = p.q$
3. $\Phi(n) = (p-1)(q-1)$
4. e (kunci enkripsi)
5. d (kunci dekripsi)
6. m (plainteks)
7. c (cipherteks)

prosedur pembangkitan sepasang kunci yang yaitu kunci privat d dan kunci publik e dapat dijelaskan sebagai berikut.

1. Pilih dua buah bilangan prima sembarang, p dan q
2. Hitung $n = p.q$ (sebaiknya $p \neq q$ karena apabila $p = q$ maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n)
3. Hitung $\Phi(n) = (p-1)(q-1)$
4. Pilih kunci publik e yang relatif prima terhadap $\Phi(n)$
5. Bangkitkan kunci privat dengan menggunakan persamaan berikut

   $$e \,.\, d = 1 \pmod{\Phi(n)}$$

   perhatikan bahwa $e \,.\, d = 1 \pmod{\Phi(n)}$ ekivalen dengan $e \,.\, d = 1 + k\Phi(n)$, sehingga secara sederhana d dapat dihitung dengan $d = 1 + k\Phi(n) / e$

hasil dari algoritma di atas yaitu:

- Kunci publik sebagai pasangan (e, n)
- Kunci privat sebagai pasangan (d, n)

Untuk proses enkripsi dan dekripsi algoritma *RSA*, dapat dijelaskan sebagai berikut.

1. Enkripsi
   - Ambil kunci publik penerima pesan e dan modulus n
   - Nyatakan plainteks m menjadi blok m_1, m_2, … sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang $[0, n-1]$
   - Setiap blok m_i dienkripsi menjadi blok c_i dengan $c_i = m_i^e \bmod n$

2. Dekripsi
   - Setiap blok cipherteks c_i didekripsi kembali menjadi blok m_i dengan rumus $m_i = c_i^d \bmod n$

4. FUNGSI *HASH MD5*

Merupakan fungsi *hash* satu-arah yang dibuat oleh Ronald Rivest pada tahun 1991 sebagai perbaikan dari *MD4* setelah *MD4* berhasil diserang oleh kriptanalis. Algoritma *MD5* menerima masukan berupa pesan pesan dengan ukuran sembarang dan menghasilkan *message diggest* yang panjangnya 128 bit.

Langkah – langkah pembuatan *message diggest* dapat dijelaskan sebagai berikut:

1. Penambahan bit – bit pengganjal
   Pesan ditambah dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512, yaitu panjang pesan setelah ditambahi bit – bit pengganjal adalah 64 bit kurang dari kelipatan 512. Apabila pesan memiliki panjang 448 bit, maka pesan tersebut tetap ditambahkan 512 bit sehingga menjadi 960 bit. Panjang bit pengganjal adalah 1 – 512 yang terdiri atas sebuah bit 1 diikuti oleh bit 0.

2. Penambahan nilai panjang pesan semula
   Pesan yang telah diberi bit pengganjal kemudian ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Jika panjang pesan > 2^{64} maka yang diambil adalah panjangnya dalam modulo 2^{64}. Dengan kata lain, jika panjang pesan semula adalah K bit, maka 64 bit yang ditambahkan menyatakan K modulo 2^{64}. Setelah ditambah dengan 64 bit, panjang pesan sekarang menjadi kelipatan 512 bit.

3. Inisialisasi penyangga MD
   MD5 membutuhkan 4 buah penyangga yang masing – masing panjangnya 32 bit. Total panjang penyangga adalah 4 x 32 = 128 bit. Keempat penyangga ini menampung hasil antara dan hasil akhir. Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai – nilai (dalam notasi HEX) sebagai berikut:
   A = 01234567
   B = 89ABCDEF
   C = FEDCBA98
   D = 76543210

4. Pengolahan pesan dalam blok
   Pesan dibagi ke dalam beberapa blok dengan panjang setiap blok adalah 512 bit. Masing – masing blok ini diproses dengan penyangga dan menghasilkan keluaran 128 bit. Proses ini disebut H_{MD5}. Pada awal proses, penyangga masih berisi nilai inisialisasi penyangganya. Akan tetapi, untuk prosesnya berikutnya penyangga berisi nilai dari proses pengolah H_{MD5}

5. TANDA TANGAN DIGITAL PADA STNK

Penggunaan tanda tangan digital pada STNK disini lebih tepat diartikan sebagai pembuatan suatu dokumen tambahan yang berisi *message diggest* dari data yang tertera pada STNK, bukan membubuhkan tanda tangan digital pada STNK yang sudah ada. Data yang akan kita gunakan adalah nomor polisi yang tertera di STNK. Aplikasi tanda tangan digital menggunakan data nomor polisi ini dimaksudkan sebagai salah satu solusi yang ditawarkan untuk mengurangi jumlah pencurian kendaraan bermotor, khususnya sepeda motor di area parkir kendaraan, dalam hal ini area parkir ITB. Untuk rancangan ini, diasumsikan telah terdapat basisdata pada komputer petugas parkir yang akan menyimpan informasi nomor plat, *message digest*, dan kunci publik, serta informasi tambahan lainnya. Mekansme penerapan penggunaan tanda tangan digital ini dapat dijelaskan dengan urutan proses sebagai berikut.

a. Pembuatan *message diggest*

STNK berisi identitas kepemilikan (nomor polisi, nama pemilik, dan alamat pemilik) serta identitas kendaraan bermotor (merk/tipe, jenis/model, tahun pembuatan, tahun perakitan, isi silinder, warna, nomor rangka/NIK, nomor mesin, nomor BPKB, warna TNKKB, bahan bakar, kode lokasi, dsb). Untuk pembuatan *message diggest* ini, data yang digunakan adalah nomor polisi.

Sebagai contoh, digunakan nomor polisi berikut yang diambil dari STNK milik salahs atu kerabat penulis.

BG-4709-UP

Dengan menggunakan bantuan fungsi *hash MD5* yang *built-in* dalam bahasa pemrograman PHP, diperoleh hasil berikut:

a56c992dc226f021861f3be1091b802c

Selanjutnya, *message diggest* yang telah dihasilkan akan disimpan pada basisdata di komputer petugas parkir.

Gambar 1. Pembangkitan *message diggest*

b. Pembangkitan kunci privat dan kunci publik

Proses selanjutnya adalah pembangkitan sepasang kunci yakni kunci publik dan kunci privat. Langkah – langkahnya adalah sebagai berikut:

1. Pilih bilangan prima p dan q sembarang
   $p = 47$
   $q = 71$
2. Hitung n yang memenuhi $n = p \cdot q$
   $n = 3337$
3. Hitung $\Phi(n)$ yang memenuhi $\Phi(n) = (p-1)(q-1)$
   $\Phi(n) = 3220$
4. Selanjutnya pilih e (kunci enkripsi) relatif prima terhadap $\Phi(n)$. misalkan
   $e = 79$
5. Selanjutnya kita dapat menghitung d (kunci dekripsi) yang memenuhi $d = 1 + k\Phi(n) / e$
   $d = 1019$

lewat proses pembangkitan kunci di atas, kita peroleh kunci publik dan kunci privat yang akan digunakan untuk proses enkripsi dan dekripsi *message diggest* untuk memperoleh tanda tangan digitalnya. Selain itu,

kunci publik yang diperoleh juga akan disimpan pada basisdata petugas parkir.

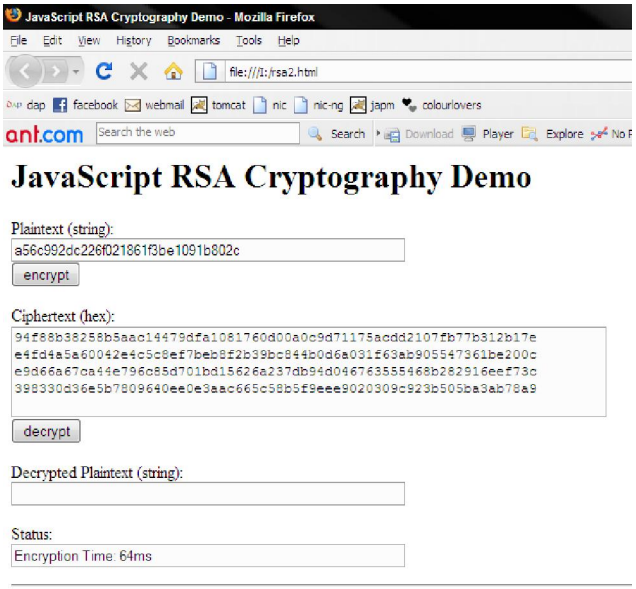
c. Enkripsi *message diggest*

Setelah diperoleh kunci publik dan privat, selanjutnya dilakukan enkripsi terhadap *message diggest* yang sebelumnya telah diperoleh.
Sebagai contoh, kita gunakan *message diggest*

a56c992dc226f021861f3be1091b802c

dengan menggunakan kunci privat yang telah kita bangkitkan sebelumnya, diperoleh tanda tangan digitalnya (ekivalen dengan cipherteks pada enkripsi plainteks) sebagai berikut.

94f88b38258b5aac14479dfa1081760d00a0c9d71175a cdd2107fb77b312b17ee4fd4a5a60042e4c5c8ef7beb8f 2b39bc844b0d6a031f63ab905547361be200ce9d66a6 7ca44e796c85d701bd15626a237db94d046763555468 b282916eef73c398330d36e5b7809640ee0e3aac665c5 8b5f9eee9020309c923b505ba3ab78a9



Gambar 2. Enkripsi *message diggest* dengan *RSA*

Tanda tangan digital ini tidak disimpan dalam basisdata di komputer petugas parkir namun hanya digunakan pada saat verifikasi terhadap kendaraan yang akan keluar dari area parkir kampus ITB.

6. MEKANISME VERIFIKASI TANDA TANGAN DIGITAL

Verifikasi atau pengecekan terhadap tanda tangan digital yang telah tersimpan dalam basisdata di komputer petugas parkir dapat dijabarkan dalam langkah – langkah berikut.

- Pertama, petugas parkir akan mencari *message diggest* dalam basisdata dengan kunci pencarian berupa nomor plat kendaaran bermotor (unik) yang akan diverifikasi.
- petugas kemudian akan meminta pengendara kendaraan untuk memasukkan kunci privat miliknya untuk mengenkripsi *message diggest* yang ditemukan tersebut. Sebelumnya, *message diggest* ini akan disalin juga ke variabel perantara *md* untuk proses perbandingan di tahap selanjutnya.
- Hasil enkripsi tadi akan membentuk tanda tangan digital. Selanjutnya petugas akan mencoba mendekripsi *digital signature* tadi dengan kunci publik yang disimpan di basisdata. Hasil dekripsi ini kemudian dibandingkan dengan *message diggest* yang disimpan di variabel perantara *md*. Apabila kedua *message diggest* memberikan hasil yang sama, maka verifikasi valid. Selanjutnya, pengendara kendaraan boleh keluar dari pintu gerbang
- Apabila perbandingan kedua *message diggest* tidak sama, maka dapat dilakukan verifikasi sekali lagi dengan pertimbangan bahwa petugas parkir dapat saja salah memasukkan nomor plat pada proses pencarian *message diggest* atau pengendara kendaraan memasukkan kunci privat yang salah (akibat salah menekan tombol)
- Apabila verifikasi kedua juga gagal setelah dipastikan bahwa petugas parkir telah memasukkan nomor plat dengan benar, maka kecurigaan patut diarahkan kepada pengendara kendaaran. Dalam hal ini, dapat dilakukan tindakan lebih lanjut baik oleh petugas parkir sendiri maupun oleh petugas keamanan untuk memastikan kepemilikan kendaraan.

7. PERANCANGAN ANTARMUKA APLIKASI

Pada dasarnya aplikasi baru memiliki desain antarmuka saja. Beberapa *screenshot*-nya pada dilihat pada bagian lampiran. Pada antarmuka tersebut, kolom untuk pengisian kunci privat dibuat sebagai *field* sandi lewat. Hal ini dilakukan agar kunci privat tetap aman.

8. KEUNTUNGAN DAN KEKURANGAN

a. Keuntungan

1. *Tingkat keamanan yang lebih tinggi disertai penurunan tingkat pencurian kendaraan bermotor di area parkir.*
Keamanan parkir akan meningkat karena hanya pemilik yang berhak saja yang dapat mengambil kendaraannya. Hal ini disebabkan setiap kali dilakukan verifikasi tanda tangan digital, pengendara diminta untuk memasukkan kunci privat miliknya. Andaikata si pengendara bukanlah pemilik sah dan memasukkan kunci privatnya secara asal - asalan, maka ketidak-sahan kepemilikan ini dapat segera dideteksi pada saat *message diggest* hasil dekripsi dan *message diggest* yang disimpan pada basisdata komputer petugas parkir memberikan hasil yang berbeda.

2. *Pengurangan pemakaian kertas nota parkir*
   Sistem parkir di ITB saat ini masih menggunakan sistem kertas. Apabila sistem parkir di ITB ini kemudian menerapkan metode tanda tangan digital, maka tidak perlu ada kertas lagi yang digunakan karena penanganannya yang bersifat elektronik.

3. *Nirpenyangkalan terhadap pengakuan palsu pemilik kendaraan*
   Dapat saja suatu saat terjadi si pemilik kendaraan mengaku belum mengambil kendaraan miliknya sedangkan berdasarkan status di basisdata, si pemilik telah mengambil kendaraannya. Argumen si pemilik kendaraan ini tentu dapat kita bantah dengan alasan bahwa hanya si pemilik lah yang mengetahui kunci privatnya. Sekalipun bahwa ternyata benar si pemilik tidak mengambil kendaraannya, tentu kecurigaan dapat dialihkan kepada orang terdekat si pemilik dengan asumsi bahwa si pemilik hanya mungkin memberitahukan kunci privat miliknya kepada orang terdekat saja.

4. *Kemudahan dalam penggantian kunci privat dan kunci publik*
   Karena sesuatu hal, misalnya kunci privat pemilik kendaraan telah diketahui beberapa orang sehingga si pemilik akhirnya bermaksud untuk mengganti kunci privatnya, maka seharusnya penggantian kunci privat ini dapat dilakukan dengan mudah. Agar modifikasi ini tidak dilakukan oleh sembarang orang, maka salahsatu parameter masukannya adalah kunci privat lama pemilik kendaraan.

b. Kekurangan

1. *Petugas harus dapat mengoperasikan mekanisme ini dengan baik*
   Agar sistem parkir dengan tanda tangan digital ini dapat berjalan dengan baik, petugas parkir harus dapat mengoperasikan mekanisme ini dengan baik. Kemampuan yang diharapkan adalah petugas parkir minimal dapat mengoperasikan komputer dengan baik. Oleh sebab itu, tentu dibutuhkan pelatihan serta harus tersedianya sistem komputer yang baik di tiap pos petugas parkir. Hal ini tentunya membutuhkan biaya yang tidak sedikit.

2. *Dibutuhkan basisdata yang cukup besar*
   Terdapat ribuan kendaraan baik sepeda motor maupun mobil yang parkir di area parkir ITB. Tentunya dibutuhkan basisdata yang cukup besar untuk menampung data semua kendaraan ini.

3. *Proteksi terhadap basisdata*
   Salahsatu informasi yang disimpan dalam basisdata ini adalah status parkir kendaraan yang berisi informasi apakah kendaraan yang diparkir telah diambil pemiliknya atau belum. Apabila ada pihak yang tidak berhak mengutak – atik basisdata ini, maka salahsatu dampaknya adalah penyangkalan terhadap pernyataan pemilik kendaraan dapat menjadi tidak valid. Oleh sebab itu, basisdata harus memiliki mekanisme proteksi yang ketat dan ini tentunya cukup sulit untuk diimplementasikan.

9. KESIMPULAN DAN SARAN

Berdasarkan pembahasan yang telah diuraikan di atas, dapat ditarik beberapa kesimpulan sebagai berikut.

- Kriptografi amat luas penggunaannya. Selain untuk enkripsi dan menjaga kerahasiaan pesan, kriptografi dapat pula diaplikasikan pada bidang lainnya.
- Salah satu bentuk aplikasi kriptografi yang cukup sering digunakan adalah tanda tangan digital mengingat beberapa aspek keamanan yang ditawarkannya cukup lengkap antara lain: aspek kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan.
- Dalam makalah ini, tanda tangan digital dicoba untuk diaplikasikan pada nomor polisi yang tertera di STNK dalam rangka penanggulangan masalah pencurian kendaraan bermotor di lingkungan kampus ITB.
- Algoritma enkripsi yang digunakan adalah algoritma *RSA* yang merupakan algoritma kunci publik yang telah digunakan secara luas. Sedangkan *MD5* digunakan sebagai fungsi *hash* satu arah.
- Tujuan dari penggunaan aplikasi ini nantinya adalah untuk pengecekan terhadap setiap kendaraan yang akan keluar dari lingkungan kampus sehingga dapat dipastikan bahwa modus operandi pencurian dapat dicegah.

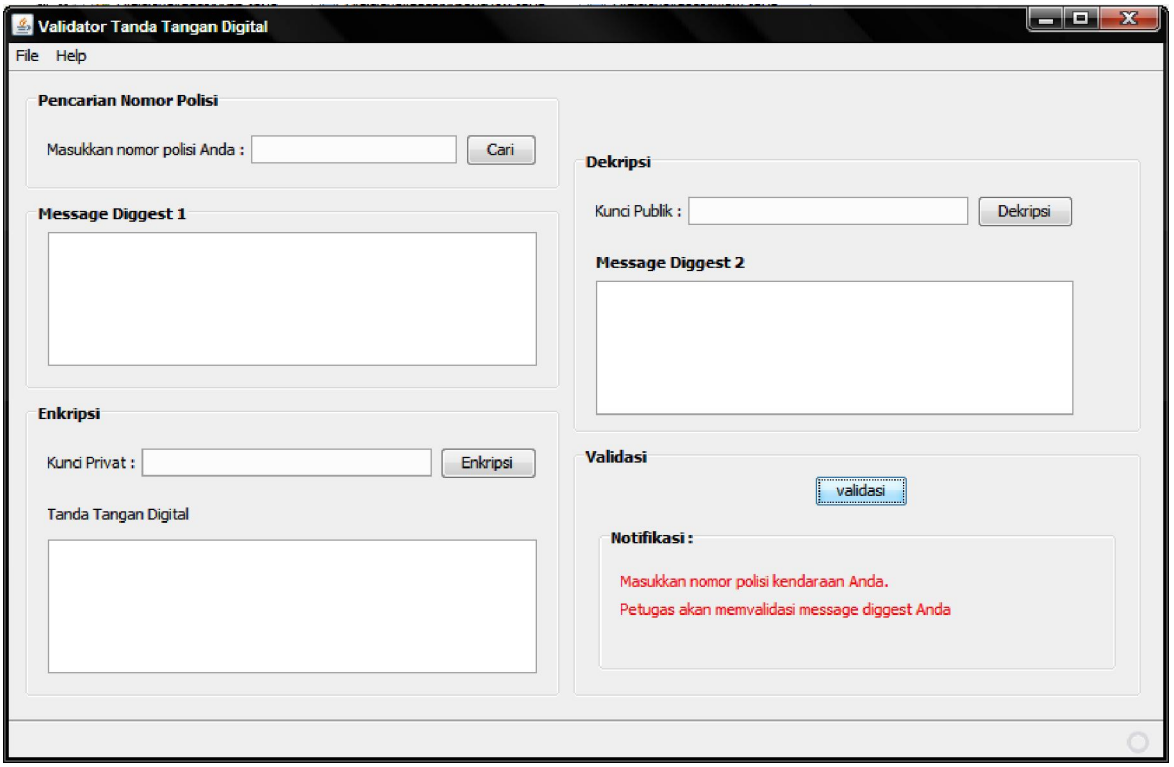
Aplikasi ini belum diimplementasikan namun masih berupa rancangan antarmuka saja. Saran dari penulis bagi yang ingin mengembangkan aplikasi ini lebih jauh antara lain:

- Penggunaan algoritma enkripsi yang lebih sukar
- Penggunaan fungsi *hash* yang tidak menimbulkan kolisi
- Perbaikan dalam hal tampilan sehingga aplikasi tampak lebih menarik dan *user-friendly*
- Penyediaan petunjuk penggunaan yang mudah dimengerti sehingga aplikasi ini nantinya dapat digunakan tanpa kesulitan yang berarti.

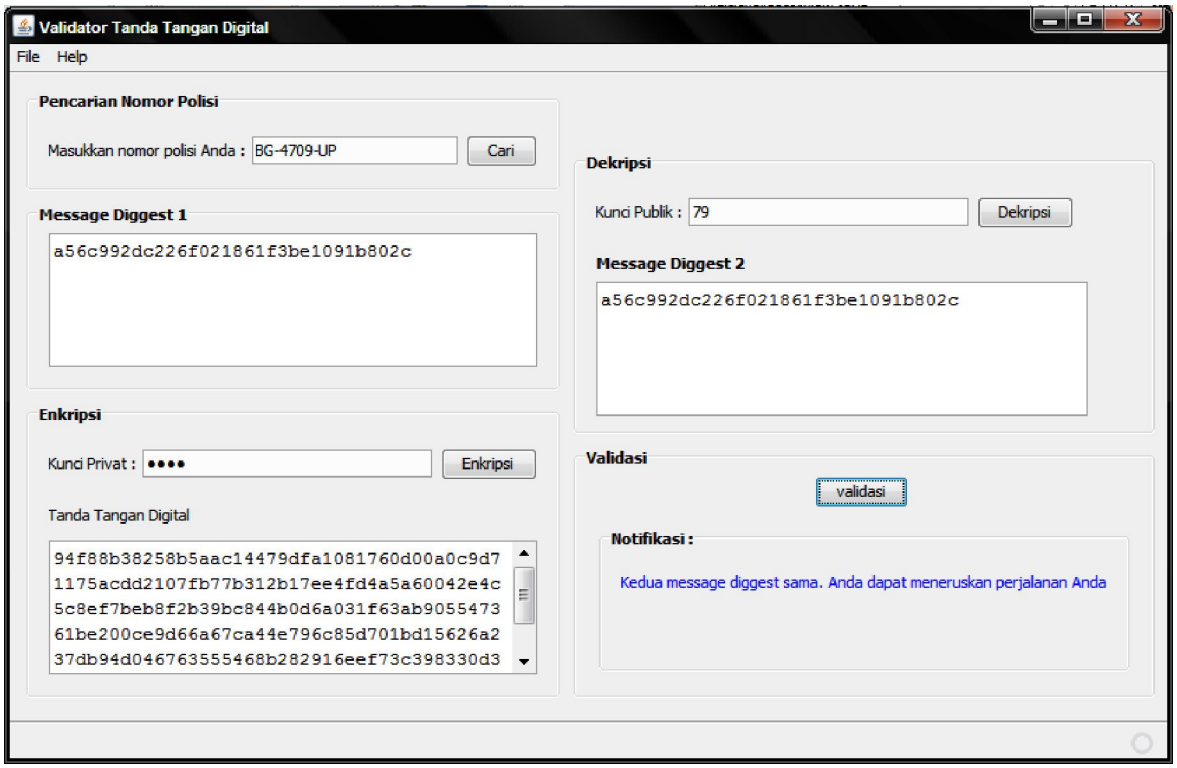
Daftar Pustaka

[1] Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Institut Teknologi Bandung 2006
[2] http://id.wikipedia.org/wiki/STNK
[3] http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
[4] http://en.wikipedia.org/wiki/Md5

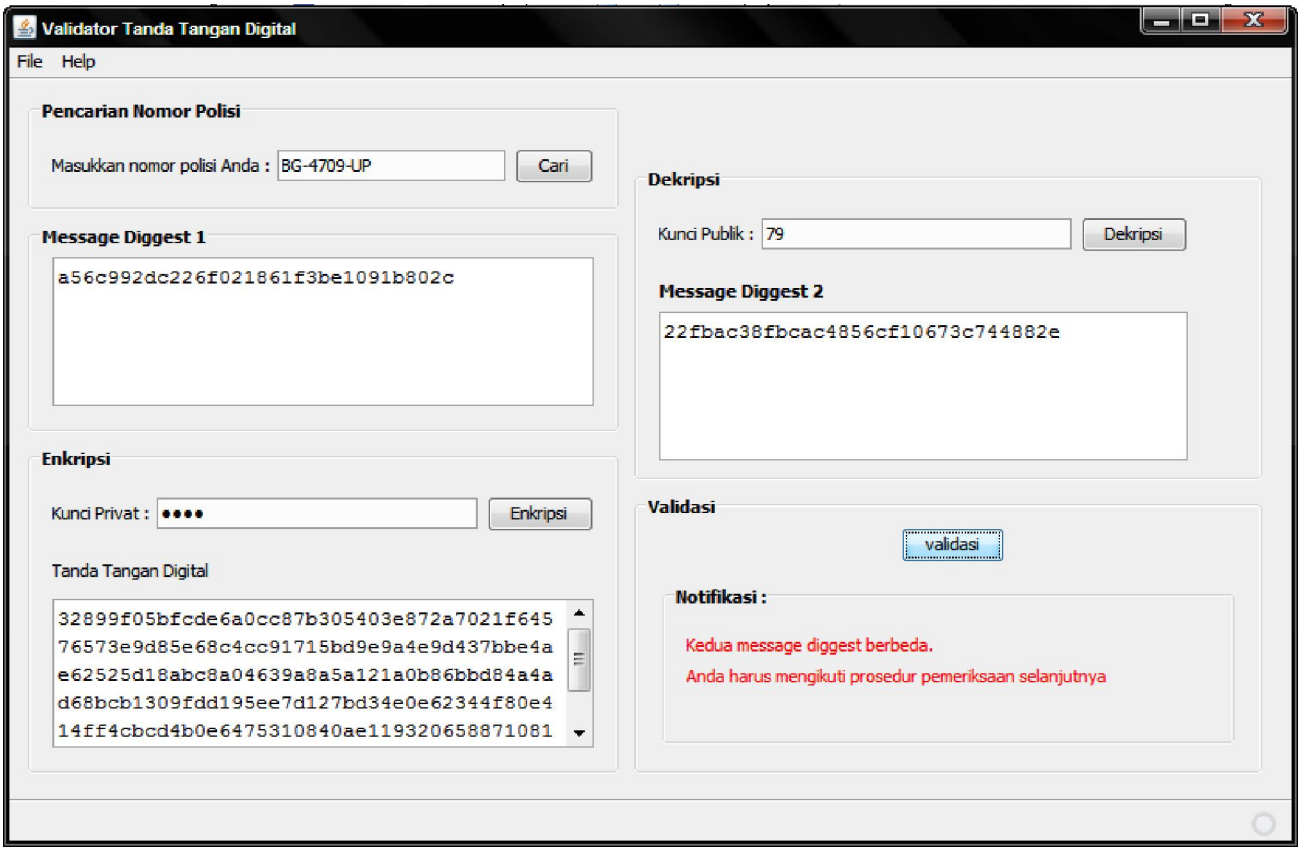
Lampiran



Gambar 3. Notifikasi saat tidak ditemukan *message diggest* yang akan dibandingkan



Gambar 4. Notifikasi saat validasi berhasil



Gambar 5. Notifikasi saat *message diggest* berbeda (misal karena pengendara salah memasukkan kunci privat)