Program StudiTeknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas Besar ke-3 IF3058 Kriptografi

Implementasi Program Tanda-tangan Digital dengan Menggunakan Algoritma RSA dan Fungsi *hash* SHA

Batas pengumpulan : 29 April 2011
Tempat pengumpulan : Lab IRK
Arsip pengumpulan :
- disket/cd berisi program, arsip *readme.txt*, laporan, arsip contoh, arsip parameter dan kunci.
- kertas A4 untuk laporan (*printout)*

Deskripsi tugas :

Tanda-tangan digital dapat digunakan untuk otentikasi data digital, seperti pesan yang dikirim melalui saluran komunikasi dan dokumen elektronis yang disimpan dalam komputer.

Pada tugas ke-3 ini, anda diminta:
1. Membuat aplikasi desktop yang mengimplementasikan algoritma *RSA* + SHA untuk memberi tanda-tangan digital pada dokumen (*file*) elektronis. Dalam hal ini, anda sebagai pemilik dokumen mempunyai sepasang kunci, yaitu kunci publik dan kunci privat.
2. Mengimplementasikan program tanda-tangan digital sebagai program *add-in* (*plug-in*) pada aplikasi *e-mail* seperti *Microsoft Outlook*, *Mozilla Thundrbird*, atau yang lainnya sehingga setiap *e-mail* dapat dibubuhi tanda-tangan digital.

Untuk aplikasi *add-in*, tanda-tangan digital dapat dilekatkan (*embedded*) di dalam email atau disimpan di dalam dokumen terpisah, tetapi pada tugas ini tanda-tangan digital disatukan di dalam email. Karena email adalah teks maka tanda-tangan digital dapat diletakkan di awal atau di akhir email, tetapi pada tugas ini tanda-tangan digital dilekatkan di akhir email. Tanda-tangan digital selanjutnya digunakan untuk membuktikan keaslian isi email dan keaslian pengirim email.

Untuk aplikasi desktop, tanda tangan dapat disimpan di dalam dokumen terpisah atau di dalam *file* yang ditandatangani (simpan tanda tangan setelah EOF dokumen). Pengguna diberi kebebasan untuk memilih dimana disimpan tanda tanga digital.

Tanda tangan digital bergantung pada isi email dan kunci. Tanda-tangan digital direpresentasikan sebagai karakter-karakter heksadesimal dan ditaruh pada akhir email. Untuk membedakan tanda-tangan digital dengan isi dokumen, maka tanda-tangan digital diawali dan diakhiri dengan *tag* `<ds>` dan `</ds>`, atau tag lain (diserahkan kepada anda)
Contoh: `<ds>4EFA7B223CF901BAA58B991DEE5B7A</ds>`.
atau

```
*** Begin of digital signature ****
     4EFA7B223CF901BAA58B991DEE5B7A
*** End of digital signature ****
```

Karena algoritma *RSA* menggunakan parameter bilangan bulat yang panjang (besar), maka program anda harus mampu menggunakan bilangan yang besar dengan membuat tipe data khusus untuk bilangan bulat besar dan primitif-primitif operasi aritmetikanya. Anda dapat membuat sendiri tipe *BigInteger* (dianjurkan) atau menggunakan fungsi-fungsi *BigInt* yang sudah disediakan oleh kakas (seperti *.NET* atau *Java*) atau diambil dari situs-situs internet. Situs web ini misalnya,

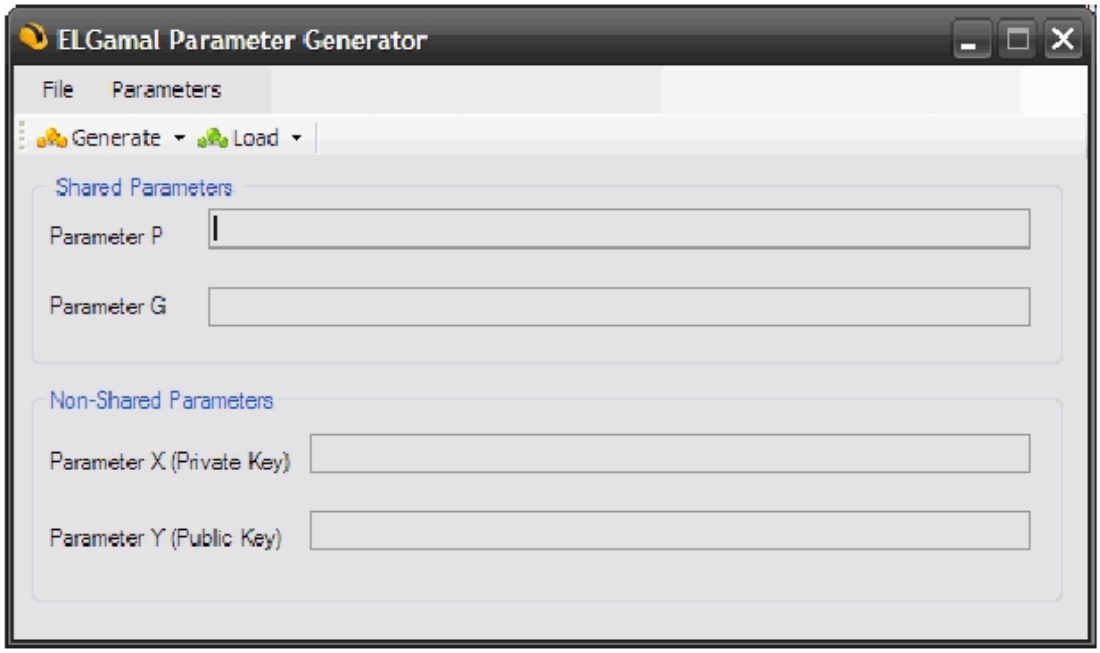
Bouncy Castle Cryptographic C# API (http://www.bouncycastle.org).

menyediakan pustaka eksternal (*dll*) khusus C# dalam bentuk *API*. Panjang bilangan prima minimal 256 bit.

Spesifikasi program:

Yang anda buat adalah:

1. Aplikasi desktop tanda-tangan digital dengan algoritma RSA dan SHA.
2. Aplikasi *desktop KeyGenerator*, adalah aplikasi yang bertujuan untuk membangkitkan parameter-parameter di dalam algoritma RSA (bilangan prima *p* dan *q*, kunci publik, kunci privat).
   Contoh program *KeyGenerator* (tapi dengan algoritma ElGamal) yang dikembangkan oleh Agus Hilman Majid:



3. Program *add-in* tanda-tangan digital pada aplikasi *e-mail*. Ikon menu program *add-in* minimal dua: penandatanganan dan verifikasi.
4. Program RSA memanfataakan program Tucil 3.
5. Program SHA memanfaatkan program Tucil 4.

Lain-lain

1. Program diberi nama yang singkat, menarik, dan memiliki makna.
2. Program harus mengandung komentar yang jelas.
3. Sertakan juga program *setup* untuk meng-instalasi dan me-*remove* (*uninstall*) progam *add-in* ke dalam aplikasi email.
3. Lampirkan di dalam disket program anda arsip contoh dan arsip parameter & kunci.

Isi laporan :

1. Deskripsi masalah.
2. Dasar teori.
3. Strategi penyelesaian masalah (lingkungan implementasi dan trik khusus).
4. Struktur data dan spesifikasi subrutin.
5. Pengujian dan analisis hasil. Pengujian menggunakaan arsip contoh dan email yang disertakan di dalam teks.
   Pengujian meliputi otentikasi dengan kasus-kasus berikut:
   - karakter di dalam pesan diubah (dihapus, ditambah)
   - karakter di dalam tanda-tangan digital diubah
   - kunci privat yang digunakan tidak berpadanan dengan pasangan kunci publiknya.
   - tanda-tangan digital dihapus dari dokumen
6. Hasil pengujian juga memasukkan eksperimen pada dua komputer *client* (pengirim dan penerima email)
7. Lampiran yang berisi:
   - antarmuka program
   - contoh dokumen/email masukan
   - contoh dokumen/email keluaran yang sudah diberi tanda-tangan digital.
   - contoh nilai-nilai paramater *RSA* yang digunakan
8. Tampilkan foto kelompok anda bertiga pada *cover* laporan.
9. Kesimpulan dan saran.