Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas Program ke-4 II4031 Kriptografi dan Koding

Implementasi Program Tanda-tangan Digital dengan Menggunakan Algoritma RSA dan Fungsi *hash* SHA-1

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-4 ini, anda diminta membuat aplikasi desktop yang mengimplementasikan algoritma RSA + SHA-1 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.

Untuk aplikasi desktop, tanda tangan dapat disimpan di dalam dokumen terpisah atau digabung di dalam *file* yang ditandatangani (tanda tangan digitak diletakkan pada akhir dokumen). Pengguna dapat memilih apakah tanda-tangan disimpan di dalam dokumen terpisah atau disatukan di dalam file pesan.

Tanda tangan digital bergantung pada isi file dan kunci. Tanda-tangan digital direpresentasikan sebagai karakter-karakter heksadesimal. 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 (lihat kembali spesifikasi tugas 3 tentang RSA)

Spesifikasi program:

1. Yang anda buat adalah aplikasi desktop yang terdiri dari menu:
   a) Menu pembangkitan kunci publik dan kunci privat RSA.
   b) Menu pembangkitan tanda-tangan digital (*signing*)
   c) Menu verifikasi tanda-tangan digital (*verivying*)
2. File dokumen yang ditanda-tangani *default*-nya adalah file teks (namun anda dapat mengembangkannya sehingga dokumen bertipe Word, Excell, audio, video, dll juga dapat ditanda-tangani).
3. Bahasa pemrograman dan kakas yang digunakan bebas (Java, C, C++, C#, Python, dll).

4. Fungsi hash SHA-1 dapat menggunakan library atau fungsi yang tersedia di dalam bahasa pemrograman yang dipilih, tetapi untuk program RSA memanfaatkan program hasil tugas 3 yang lalu.
5. Aplikasi boleh berbasis *desktop* atau *mobile*.
6. Tugas dikerjakan berkelompok, min 2 orang max 3 orang.
7. Waktu pengumpulan adalah Senin 18 April 2022 (max pukul 23.59 WIB) pada *drive* berikut:
   https://drive.google.com/drive/folders/1InCQiDPA9Y46R5HPFQBAXAXb_a_kicsk?usp=sharing
   Setiap kelompok membuat folder sendiri dan mengunggah ke dalam folder kelompoknya file berikut: file laporan dan file kode program

Isi laporan :

1. Deskripsi masalah.
2. Teori singkat.
3. Implementasi program.
4. Pengujian dan analisis hasil. 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
5. Kesimpulan dan alamat drive/github yang berisi kode program anda
6. Lampiran yang berisi:
   - antarmuka program
   - contoh dokumen masukan
   - contoh dokumen luaran yang sudah diberi tanda-tangan digital.
   - contoh nilai-nilai paramater RSA yang digunakan
   - kode program
7. Tampilkan foto kelompok anda pada *cover* laporan.