Program StudiTeknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas 5 IF4020 Kriptografi

Program Tanda-tangan Digital untuk File Teks

Pada tugas ke-5 ini anda dapat memilih salah satu dari dua buah tugas berikut:

A. Membuat aplikasi desktop untuk membuat dan memverifikasi 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 digital 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 ****

   Algoritma kriptografi kunci-publik dan fungsi hash yang dapat dipilih adalah sebagai berikut:
   a. RSA + SHA256
   b. ECC + SHA256
   c. RSA + SHA3
   d. ECC + SHA3
   e. ELGamal + SHA256
   f. ELGamal+ SHA3

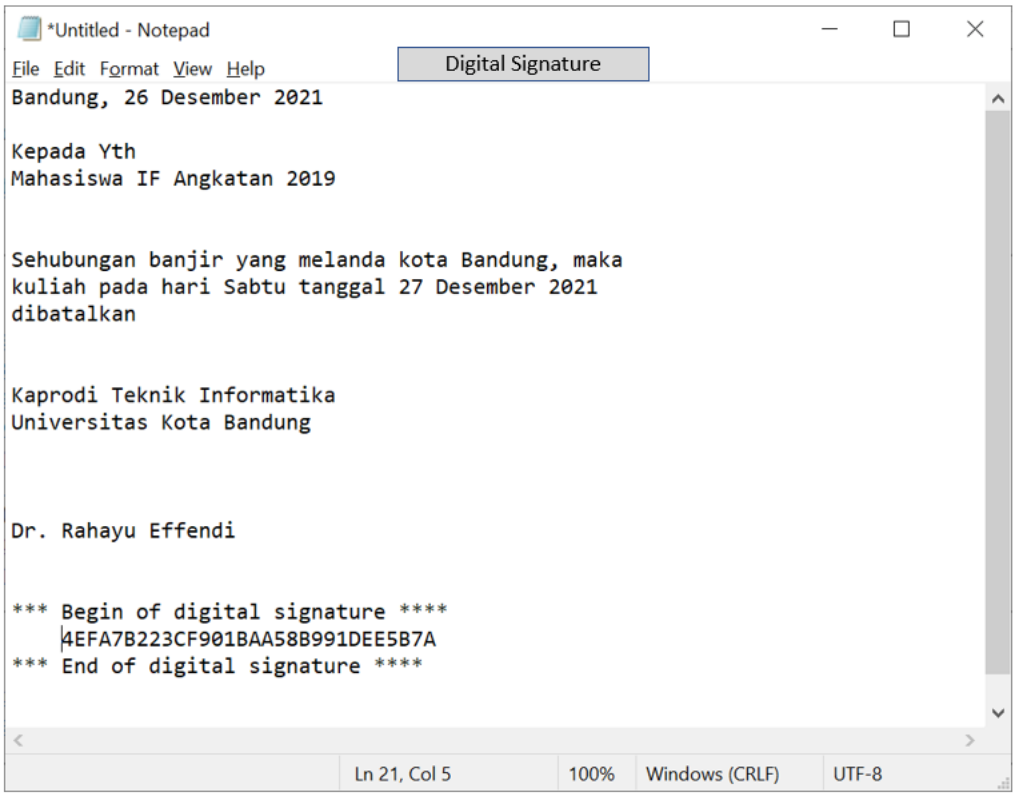
   Fungsi hash SHA256 atau SHA3 harus diimplementasikan sendiri, tidak boleh menggunakan fungsi pustaka SHA yang disediakan oleh bahasa pemrograman.
   Dokumentasi SHA256:
   https://en.wikipedia.org/wiki/SHA-2
   https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/

Spesifikasi program:

1. Yang anda buat adalah aplikasi desktop yang terdiri dari menu:
   a) Menu pembangkitan kunci publik dan kunci privat
   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. Aplikasi boleh berbasis *desktop*, web, atau *mobile*.
5. Tugas dikerjakan berkelompok, min 2 orang max 3 orang.

B. Membuat program *add-on* (plug-i add-in) tanda-tangan digital dapat dilekatkan (*embedded*) di dalam aplikasi editor teks seperti Notepad atau aplikasi e-mail.



Spesifikasi program:

Yang anda buat adalah:

1. Program add-on yang berisi menu untuk pembangkitan kunci publik dan kunci privat, menu signing, dan menu verifying.
2. Algoritma kriptografi kunci-publik dan fungsi hash yang dipilih sama seperti pada Tugas A.
3. Bahasa dan kakas yang digunakan bebas (Java, C#, C++, Phyton, dll).
4. Tugas dikerjakan berkelompok, min 2 orang max 3 orang.

Isi laporan (untuk Tugas A atau B):

1. Deskripsi masalah.
2. Teori singkat.
3. Implementasi program.
4. Pengujian dan analisis hasil. Pengujian meliputi otentikasi tanda tangan digital 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 algoritma knci-publik yang digunakan
   - kode program
7. Tampilkan foto kelompok anda pada *cover* laporan.

Laporan dalam format PDF dikumpulkan paling lambat tanggal 22 November 2021 ke alamat Google Drive yang akan diumumkan kemudian.