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

Tugas Kecil 4 (Tucil 4) IF3058 Kriptografi Sem. II Tahun 2011/2012
Implementasi fungsi hash MySHA

Batas pengumpulan	:	Rabu, 3 April 2012, pada jam kuliah Kriptografi
Tempat pengumpulan	:	Ruang Kuliah (7606), Pukul 12.00
Berkas pengumpulan	:	Kertas A4
Per kelompok	:	2 orang

Buatlah sebuah program applet Java/C# yang mengimplementasikan salah satu fungsi *hash* dari keluarga SHA (yaitu SHA-1, SHA 224, SHA 256, SHA 384, atau SHA 512) dan diberi nama *MySHA*. Spesifikasi program adalah sebagai berikut:

1. Program dapat menerima pesan berupa *file* atau pesan yang diketikkan dari papan-ketik dengan editor teks sederhana. Jika pesan tersebut diketik, maka pesan tersebut dapat disimpan ke dalam file.
2. Program dapat menghitung dan menampilkan *message digest* pesan dalam notasi heksadesimal.
3. Program dapat menyimpan *message digest* ke dalam sebuah file eksternal. File tersebut berisi informasi sbb: nama file, tanggal terakhir dimodifikasi/dibuat, dan message digestnya
4. Tes apakah program MySHA anda sensitif terhadap perubahan 1 karakter pada pesan.
5. Dapat membandingkan nilai *hash* dari dua buah file (file asli dan file yang sudah diubah) untuk memeriksa keaslian file.

Yang dikumpulkan:

1. *Source program* Java/C#
2. Tampilan antarmuka program (*print screen*).
3. Contoh file/pesan (bermacam-macam tipe seperti .doc, .jpg, .bmp, .xls, dll) dan nilai *message digest* nya.