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

Tugas Kecil 3 (Tucil 3) IF3058 Kriptografi Sem. II Tahun 2011/2012
Implementasi Algoritma RSA

Batas pengumpulan : Selasa, 28 Maret 2012, pada jam kuliah Kriptografi
Tempat pengumpulan : Ruang Kuliah (7606), Pukul 11.00
Berkas pengumpulan : Kertas A4
Per kelompok : 2 orang

Buatlah sebuah program applet Java/ C#.NET yang mengimplementasikan enkripsi/dekripsi algoritma El-Gamal dengan spesifikasi sebagai berikut:

1. Program terdiri dari:
   a. pembangkitan kunci privat dan kunci publik
      Masukan: *p*, *g*, dan *x*
      Keluaran: Kunci publik <*y*, *g*, *p*> dan kunci privat <*x*, *p*>
      Kunci publik dan kunci privat dapat disimpan dalam file terpisah (*.pub dan *.pri)
   b. Enkripsi/dekripsi file
      Masukan: nama file (*browsing*), kunci privat/pub;ik (*browing* atau diketik nilai kuncinya)
2. Program dapat menerima pesan berupa *file* bertipe sembarang.
3. Program dapat mengenkripsi plainteks dengan ElGamal.
4. Program dapat mendekripsi cipherteks dengan ElGamal.
5. Program menampilkan plainteks dan cipherteks di layar. Khusus untuk cipherteks ditampilkan dalam notasi heksadesimal.
6. Program dapat menyimpan cipherteks ke dalam *file*.
7. Program dapat menampilkan lama waktu enkripsi/dekripsid an ukuran file hasil enkripsi/dekripsi.
8. Tipe integer yang digunakan (pilih salah satu):
   a. Tipe *LongInt* yang disediakan pada setiap bahasa/kakas
   b. Tipe *BigNum* yang pustakanya dapat diunduh dari internet (atau disediakan kakas)
   c. Tipe *LongLongInteger* bentukan sendiri
9. Kode program dibuat sendiri (tidak boleh *copy/paste* dari internet, kecuali pustaka BigNum)
10. Untuk perpangkatan yang mangkus, dapat menggunakan algoritma yang dijelaskan pada pranala ini: http://en.wikipedia.org/wiki/Square-and-multiply_algorithm atau algoritma perpangkatan modulo: http://en.wikipedia.org/wiki/Modular_exponentiation

Yang dikumpulkan:

1. *Source program* lengkap
2. Tampilan antarmuka program (*print screen/screen shot*) untuk beberapa parameter ElGamal.
3. Contoh *p*, *g*, *y*, *x*, plainteks, dan cipherteks