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

Tugas Kecil 3 (Tucil 3) IF4020 Kriptografi Sem. I Tahun 2018/2019
Implementasi Algoritma ElGamal dan *Elliptic Curve Cryptography* (*ECC*)

Batas pengumpulan : Rabu, 28 Maret 2018, pada jam kuliah Kriptografi
Tempat pengumpulan : Ruang Kuliah
Berkas pengumpulan : Kertas A4
Per kelompok : 2 orang

Buatlah sebuah program applet Java/C++/ C#/Phyton yang mengimplementasikan enkripsi/dekripsi dengan algoritma ElGamal dan algoritma *Elliptic Curve Cryptography ElGamal* (*ECCEG*) dengan spesifikasi sebagai berikut:

1. Program terdiri dari:
   a. pembangkitan kunci privat dan kunci publik untuk masing-masing algoritma
   Kunci publik dan kunci privat dapat disimpan dalam file terpisah (*.pub dan *.pri)
   b. Enkripsi/dekripsi file
   Masukan: nama file (*browsing*), kunci privat/publik (*browing* atau diketik nilai kuncinya)
2. Program dapat menerima pesan berupa *file* bertipe sembarang.
3. Program dapat mengenkripsi plainteks dengan ElGamal dan ECC.
4. Program dapat mendekripsi cipherteks dengan ElGamal dan ECC.
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. Pengkodan pesan menjadi titik di kurva eliptic dapat mengikuti teknik di dalam makalah *Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method*

Yang dikumpulkan:

1. *Source program* lengkap
2. Tampilan antarmuka program (*print screen/screen shot*) untuk beberapa parameter ElGamal dan ECC.
3. Contoh kunci publik, kunci privat, plainteks, dan cipherteks