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

Tugas Kecil 3 (Tucil 3) IF4020 Kriptografi Sem. I Tahun 2020/2021
Implementasi Algoritma RSA, Elgamal, dan Diffie-Hellman

Batas pengumpulan : Senin, 2 November 2020
Tempat pengumpulan : Google Drive
Per kelompok : 2 orang

Buatlah sebuah program (sebaiknya dengan GUI) menggunakan Java/C++/ C#/Python yang mengimplementasikan enkripsi/dekripsi dengan algoritma RSA dan algoritma Elgamal, dan pembangkitan kunci sesi dengan algoritma pertukaran kunci Diffie-Hellman dengan spesifikasi sebagai berikut:

1. Program terdiri dari:
   a. pembangkitan kunci privat dan kunci publik untuk masing-masing algoritma RSA dan Elgamal
      Kunci publik dan kunci privat dapat disimpan dalam file terpisah (*.pub dan *.pri)
   b. Enkripsi/dekripsi file
      Masukan: pesan pendek yang diketik dan pesan berupa file sembarang (*browsing*), kunci privat/publik (*browing* atau diketik nilai kuncinya)
      Luaran: cipherteks (ditampilkan ke layar untuk pesan yang diketik, atau file cipherteks jika plainteks berupa file)
   c. Pembangkitan kunci sesi oleh Alice dan Bob
      Masukan: parameter-parameter di dalam algoritma Diffie-Hellman (n, g, x, y)
      Luaran: kunci sesi yang sama pada Alice dan Bob
2. Program dapat menyimpan cipherteks ke dalam *file*.
3. Program dapat menampilkan lama waktu enkripsi/dekripsi dan ukuran file hasil enkripsi/dekripsi.
4. Tipe integer yang digunakan adalah BigInteger/BigNum (pilih salah satu):
   a. Tipe *BigNum* yang pustakanya dapat diunduh dari internet (atau disediakan oleh bahasa pemrograman/kakas)
   b. Tipe *LongLongInteger* bentukan sendiri
5. Kode program dibuat sendiri (tidak boleh *copy/paste* dari internet, kecuali pustaka BigNum)

Yang dikumpulkan:

1. *Source program* lengkap
2. Tampilan antarmuka program (*print screen/screen shot*)
3. Contoh hasil enkripsi/dekripsi dan hasil pembangkitan kunci sesi