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

Tugas 4 IF4020 Kriptografi, Sem. I Tahun 2021/2022
Implementasi Algoritma RSA, ElGamal, Paillier, ECC

Batas pengumpulan : Rabu, 3 November 2021
Tempat pengumpulan : Google drive
Berkas pengumpulan : File pdf
Per kelompok : 2 orang

Buatlah sebuah program Java/C/C++/ C#/Python/Golang/dll yang mengimplementasikan kalkuator enkripsi/dekripsi dengan algoritma RSA, ElGamal, Paillier, ECC dengan spesifikasi sebagai berikut:

1. Program terdiri dari:
   a. pembangkitan kunci privat dan kunci publik
      Kunci publik dan kunci privat dapat disimpan dalam file terpisah (misalnya *.pub dan *.pri)
   b. Enkripsi/dekripsi file
      Masukan: pesan, kunci privat/publik (*browing* atau diketik nilai kuncinya)
2. Program memiliki editor tempat pengguna mengetikkan pesan atau meng-copy paste teks ke editor tersebut.
3. Program dapat mengenkripsi plainteks dengan RSA, ElGamal, Paillier, ECC
4. Program dapat mendekripsi cipherteks dengan RSA, ElGamal, Paillier, ECC
5. Program menampilkan cipherteks di layer.
6. Tipe integer yang digunakan adalah *long integer* (pilih salah satu):
   a. Tipe *Long Integer* yang disediakan pada setiap bahasa/kakas
   b. Tipe *BigNum* yang pustakanya dapat diunduh dari internet (atau disediakan kakas)
   c. Tipe *LongLongInteger* bentukan sendiri
7. 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 kunci publik, kunci privat, plainteks, dan cipherteks
4. Alamat pengumpulan akan diumumkan kemudian.