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

Tugas 3 II4031 Kriptografi dan Koding Sem. II Tahun 2020/2021
Implementasi Algoritma RSA

Batas pengumpulan : Jumat, 26 Maret 2021
Tempat pengumpulan : Googgle drive
Berkas pengumpulan : File pdf
Per kelompok : 2 orang

Buatlah sebuah program applet Java/C++/ C#/Python yang mengimplementasikan enkripsi/dekripsi dengan algoritma RSA 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 RSA.
4. Program dapat mendekripsi cipherteks dengan RSA.
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 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
9. 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*) untuk beberapa parameter RSA
3. Contoh kunci publik, kunci privat, plainteks, dan cipherteks