Program Studi Informatika
Sekolah Teknik Elektro dan Informatika ITB
==========

Tugas Kecil 1 IF4020 Kriptografi
Semester I Tahun 2016/2017

Buatlah sebuah program Java/C++ yang mengimplementasikan:

a) *Vigenere Cipher* standard (26 huruf alfabet)
b) *Vigenere Cipher extended* (256 karakter ASCII)
c) *Vigenere modifikasi (lihat contoh-contoh makalah mahasiswa di web kuliah)*
d) Playfair Cipher

dengan spesifikasi sebagai berikut:

1. Program dapat menerima pesan berupa *file* teks atau pesan yang diketikkan dari papan-ketik.
2. Program dapat mengenkripsi plainteks.
3. Program dapat mendekripsi cipherteks.
4. Program menampilkan plainteks dan cipherteks di layar.
5. Cipherteks dapat ditampikan dalam bentuk:
    (a) apa adanya (sesuai susunan plainteks)
    (b) tanpa spasi
    (c) dalam kelompok 5-huruf
6. Program dapat menyimpan cipherteks ke dalam *file*.
7. Kunci dimasukkan oleh pengguna. Panjang kunci bebas (maksimal 25 huruf).
8. Opsional (bonus): anda dapat mengenkripsi plainteks sembarang file, tidak harus file teks. Jadi, setiap file diperlakukan sama sebagai *file of byte*. Program membaca setiap *byte* di dalam file (termasuk *byte-byte header file*) dan mengenkripsinya. Hanya saja file yang sudah terenkripsi tidak bisa dibuka oleh program aplikasinya karena header file ikut terenkripsi. Namun dengan mendekripsinya kembali maka file tersbut dapat dibuka oleh aplikasinya.

Dikumpulkan minggu depan, per kelompok dua orang agau 1 orang
Yang dikumpulkan:

1. *Source program* Java/C++
2. Tampilan antarmuka program (*print screen*).
3. Contoh plainteks dan cipherteks (kecil, sedang, besar).

Catatan: Tugas ini akan terpakai untuk Tucil 2 dan Tubes 1.