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

Tugas Kecil 1 IF4020 Kriptografi
Semester II Tahun 2018/2019

Buatlah sebuah program Java/C++/Phyton/Ruby yang mengimplementasikan:
a) *Vigenere Cipher* standard (26 huruf alfabet)
b) *Tiga (3) varian Vigenere Cipher*
c) *Extended Vigenere Cipher* (256 karakter ASCII)
d) *Playfair Cipher* (26 huruf alfabet)

dengan spesifikasi sebagai berikut:

1. Program dapat menerima pesan berupa *file* sembarang atau pesan yang diketikkan dari papan-ketik. Khusus untuk a), b), dan d) hanya bisa untuk file teks. Untuk c) bisa file tipe apapun.
2. Program dapat mengenkripsi plainteks. Khusus untuk *Vigenere Cipher* dengan 26 huruf alfabet dan *Playfair Cipher* dengan 26 huruf alfabet, program hanya mengenkripsi karakter alfabet saja. Angka, spasi, dan tanda baca tidak dienkripsi, tetapi tidak ditampilkan sebagai cipherteks.
3. Program dapat mendekripsi cipherteks.
4. Program menampilkan plainteks dan cipherteks di layar.
5. Cipherteks dapat ditampilkan ke layar 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.
8. Untuk enkripsi plainteks sembarang file (dengan *Extended Vigenere Cipher*), setiap file diperlakukan sebagai *file of bytes*. 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.
Yang dikumpulkan:

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

Catatan:

1. Tugas ini akan terpakai untuk Tucil 2 dan Tubes 1.
2. Tugas perorangan