

Tugas Kecil 1 IF4020 Kriptografi
Semester II Tahun 2017/2018

Buatlah sebuah program Java/C++/Python yang mengimplementasikan:

- a) *Vigenere Cipher* standard (26 huruf alfabet)
- b) *Vigenere Cipher extended* (256 karakter ASCII)
- c) *Playfair Cipher* (26 huruf alfabet)

dengan spesifikasi sebagai berikut:

1. Program dapat menerima pesan berupa *file* teks atau pesan yang diketikkan dari papan-ketik.
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 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. Opsional (bonus): anda dapat mengenkripsi plainteks sembarang file, tidak harus file teks. Jadi, 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 tersebut dapat dibuka oleh aplikasinya.

Dikumpulkan minggu depan.

Yang dikumpulkan:

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

Catatan:

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