Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika ITB
==========

Tugas 1 II4031 Kriptografi dan Koding
Semester I Tahun 2021/2022

Buatlah sebuah program dalam Bahasa C/C++/Java/Python/Ruby/Golang (pilih salah satu) dengan antarmuka (GUI) yang mengimplementasikan:

a) *Vigenere Cipher* standard (26 huruf alfabet)
b) *Extended Vigenere Cipher* (256 karakter ASCII)
c) *Playfair Cipher* (26 huruf alfabet)
d) *Enigma Cipher* dengan 3-rotor (26 huruf alfabet)
e) Bonus: *One-time pad* (26 huruf alfabet)

dengan spesifikasi sebagai berikut:

1. Program dapat menerima pesan berupa *file* sembarang (file text maupun file biner) atau pesan yang diketikkan dari papan-ketik.
2. Program dapat mengenkripsi plainteks. Khusus untuk *Vigenere Cipher* dengan 26 huruf alfabet, *Playfair Cipher* dengan 26 huruf alfabet, dan *One-time pad* dengan 26 huruf alfabet, program hanya mengenkripsi karakter alfabet saja. Angka, spasi, dan tanda baca lainnya diabaikan dan dibuang saat cipherteks ditampilkan atau disimpan.
3. Untuk *One-time pad*, kunci dibaca dari file teks yang berisi huruf-huruf yang dibangkitkan secara acak. Jumlah huruf di dalam file kunci sebaiknya banyak (misalnya puluhan ribu huruf). Huruf-huruf kunci yang digunakan adalah sepanjang karakter di dalam pesan, sisa huruf yang tidak terpakai dibiarkan begitu saja.
4. Program dapat mendekripsi cipherteks menjadi plainteks semula.
5. Untuk pesan berupa text, program dapat menampilkan plainteks dan cipherteks di layar. Cipherteks dapat ditampilkan dalam dua cara: (a) tanpa spasi, (b) 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 (khusus untuk 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.

Laporan tugas dikumpulkan Jumat minggu depan (4 Februari 2022) sebelum jam kuliah. Tugas sebaiknya dibuat berpasangan (2 orang), namun diperkenankan per orang. Laporan yang dikumpulkan adalah file format PDF yang berisi:

1. *Source program* Java/C++/Python/Ruby/Golang
2. Tampilan antarmuka program (*print screen*).

3. Contoh plainteks dan cipherteks (text, gambar, file database, audio, video)
4. Link ke *github* atau *google drive* yang berisi kode program

File PDF diunggah ke alamat berikut:
https://drive.google.com/drive/folders/1fniCOJLqg11MaFliPT0OjWniUObxFdVX?usp=sharing
(satu jam setelah kuliah pranala tsb ditutup)

Jika program tidak selesai/tidak bisa run/masih ada yang salah, maka tuliskan di dalam laporan.

Program harus dibuat sendiri, DILARANG KERAS mengambil kode program dari teman, kakak tingkat, internet, dan dari sumber-sumber lainnya.

Lengkapi tabel berikut di dalam laporan dengan mencentang kolom):

No	Spek	Berhasil (√)	Kurang berhasil (√)	Keterangan
1	Vigenere standard			
4	Extended Vigenere Cipher			
5	Playfair cipher			
6	Enigma Cipher			
7	Bonus: One-time pad			

Keterangan:

1) Berhasil artinya program sesuai spek, benar, bisa melakukan enkripsi dan dekripsi dengan benar (baik pesan diketik maupun file)
2) Kurang berhasil artinya i) program tidak selesai, atau ii) program masih ada kesalahan, atau iii) program hanya bisa melakukan enkripsi tetapi dekripsi salah, atau iv) hanya bisa enkripsi file text tidak bisa file sembarang, atau v) hanya bisa enkripsi pesan diketik langsung tidak bisa untuk file, vi) dll. Tuliskan pada bagian keterangan aspek apa yang kurang berhasil