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

Tugas Kecil 1 IF4020 Kriptografi
Semester II Tahun 2020/2021

Buatlah sebuah program Java/C++/Python/Ruby/Golang dengan antarmuka (GUI) yang mengimplementasikan:

a) *Vigenere Cipher* standard (26 huruf alfabet)
b) *Varian Vigenere Cipher* (26 huruf alfabet): Full Vigenere Cipher dan Auto-key Vigenere Cipher)
c) *Extended Vigenere Cipher* (256 karakter ASCII)
d) *Playfair Cipher* (26 huruf alfabet)
e) Super enkripsi: Vigenere Cipher standard + *cipher* transposisi (bebas). Jelaskan cipher transposisi yang dibuat.
f) Affine cipher (26 huruf alfabet)
g) Hill cipher (26 huruf alfabet)
h) Bonus: Enigma cipher (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 dan *Playfair Cipher* dengan 26 huruf alfabet, program hanya mengenkripsi karakter alfabet saja. Angka, spasi, dan tanda baca dibuang.
3. Program dapat mendekripsi cipherteks menjadi plainteks semula.
4. Untuk pesan berupa text, program dapat menampilkan plainteks dan cipherteks di layar.
5. Untuk plainteks berupa text, cipherteks dapat ditampilkan ke layar dalam bentuk:
    (a) tanpa spasi
    (b) 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 (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 Rabu minggu depan (9 September 2020) sebelum jam kuliah. Tugas perorangan atau pasangan (2 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 Google Drive (Drive dibuka 2 jam sebelum kuliah dimulai dan ditutup setelah kuliah selesai):
https://drive.google.com/drive/u/0/folders/1mvzu1jUwPy5vUO_-R-nstzvuDJrgPDPu

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

Program harus dibuat sendiri, tidak dibenarkan mengambil program dari tempat lain atau dari orang lain.

Lengkapi tabel berikut di dalam laporan dengan mencentang kolom):

No	Spek	Berhasil (√)	Kurang berhasil (√)	Keterangan
1	Vigenere standard			
2	Full Vigenere Cipher			
3	Running-Key Vigenere Cipher			
4	Extended Vigenere Cipher			
5	Playfair cipher			
6	Super enkripsi			
7	Affine cipher			
8	Hill cipher (matriks 3 x 3)			
9	Bonus: Enigma cipher			

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