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

Tugas 2 II4031 Kriptografi dan Koding
Modified RC4
Semester II Tahun 2023/2024

Buatlah sebuah program modifikasi RC4 (*modified RC4*) dengan menggabungkannya dengan konsep *Extended Vigenere Cipher/Play Cipher/Affine Cipher*. Memodifikasi RC4 dan menggabungkannya dengan *Extended Vigenere Cipher/Play Cipher/Affine Cipher* berarti memodifikasi prosedur KSA atau PRGA di dalam RC4 dan menggabungkannya dengan konsep *Extended Vigenere Cipher/Playfair Cipher/Affine Cipher*. Anda dapat membuat fungsi permutasi yang lebih kompleks. Program ditulis berbasis web atau program desktop atau aplikasi mobile (pilih salah satu, bonus jika aplikasi mobile) dalam Bahasa C/C++/Java/C++/C#/Python/Golang/Perl/dll (pilih salah satu) dengan antarmuka (GUI).

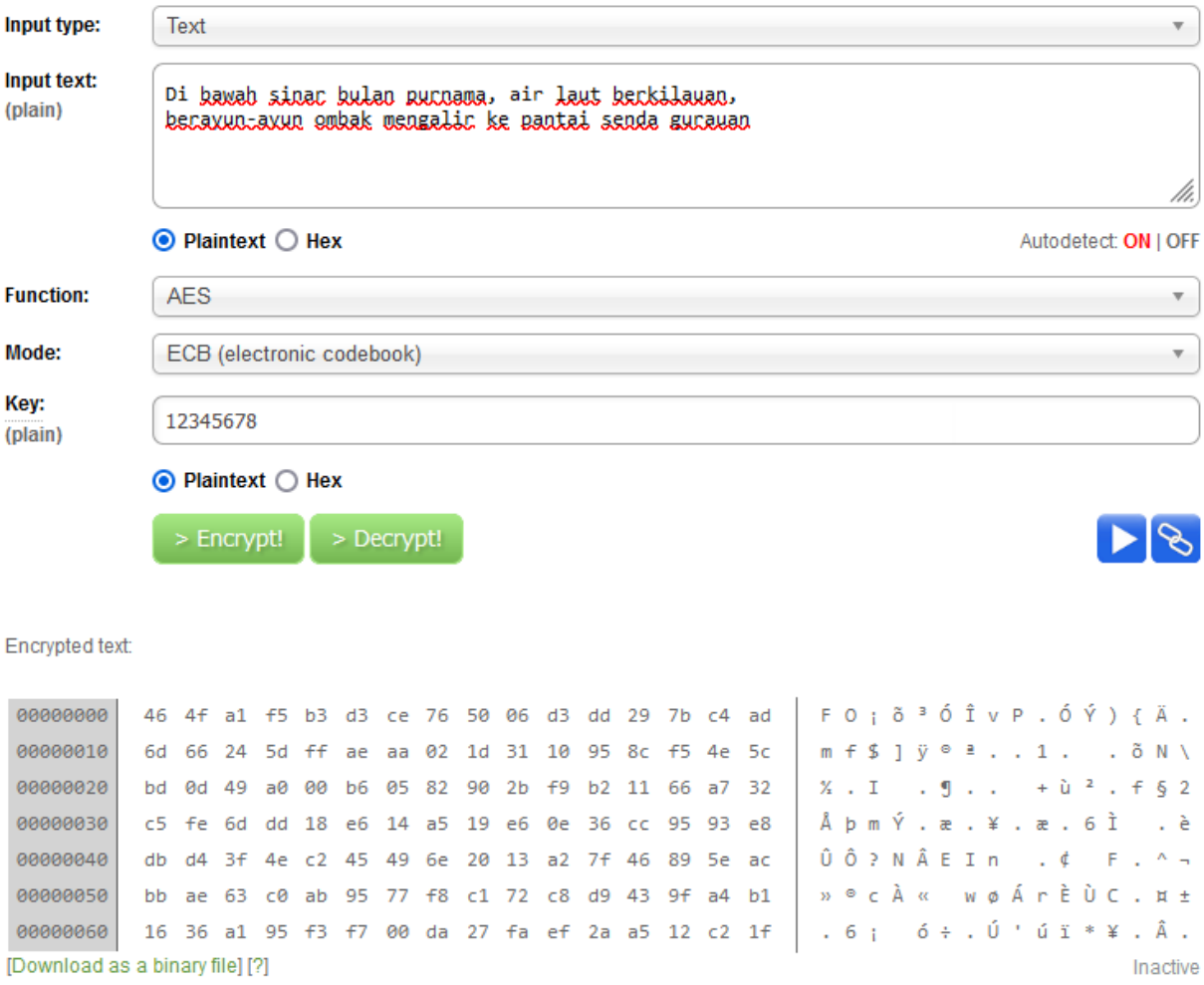
Spesifikasi program adalah sebagai berikut:

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 dan mendekripsi cipherteks menjadi plainteks semula.
3. Untuk pesan berupa text, program dapat menampilkan plainteks dan cipherteks di layer (format string atau base64).
4. Program dapat menyimpan cipherteks ke dalam *file*.
5. Kunci dimasukkan oleh pengguna. Panjang kunci bebas.

Laporan tugas dikumpulkan hari Jumat (15 Maret 2024) paling lambat pukul 23.59. 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/dll
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. Cantumkan file Readme.txt di dalam *github* yang menjelaskan cara menjalankan program

Contoh inspirasi antarmuka program (diambil dari http://aes.online-domain-tools.com/ (Function dapat diganti dengan Cipher):



File PDF diunggah ke alamat berikut:
https://drive.google.com/drive/u/1/folders/1bp8zDfpozFdzIpy2YixYdnB2ypxgCvSs

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.