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

Tugas 2 II4031 Kriptografi dan Koding
MyOwnStreamCipher
Semester II Tahun 2022/2023

Buatlah sebuah program *stream cipher* yang akan menjadi *MyOwnStreamCipher*. Program *stream cipher* dapat memodifikasi RC4 (*modified RC4*) dan menggabungkannya dengan konsep Extended Vigenere Cipher/Play Cipher. Memodifikasi RC4 dan menggabungkannya dengan Extended Vigenere Cipher/Play Cipher berarti memodifikasi prosedur KSA atau PRGA di dalam RC4 dan mengabungkannya dengan konsep Extended Vgenere Cipher. Anda dapat membuat fungsi permutasi yang lebih kompleks, menambahkan LFSR, dll. Program ditulis dalam Bahasa C/C++/Java/C++/C#/Python/Golang (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 Jumat minggu depan (17 Februari 2023) sebelum pukul 23.59 WIB. Tugas boleh perorangan atau pasangan (2 orang). Laporan yang dikumpulkan adalah file format PDF yang berisi:

1. Deskripsi algoritma stream cipher yang yang anda rancang
2. *Source program*
3. Tampilan antarmuka program (*print screen*).
4. Contoh plainteks dan cipherteks (text, gambar, file database, audio, video)
5. Link ke *github* atau *google drive* yang berisi kode program

File PDF diunggah ke alamat Google Drive:

https://drive.google.com/drive/folders/11LypGLxXd1ea_enO6ojIZUP9H1O21zXh?usp=sharing

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 sumber lain, dari kakak tingkat, atau dari orang lain.