

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

=====

**Tugas 2 II4031 Kriptografi dan Koding  
*MyOwnCipher*  
Semester II Tahun 2021/2022**

Buatlah sebuah program *stream cipher* yang akan menjadi *MyOwnCipher*. Program *stream cipher* dapat memodifikasi RC4 (*modified RC4*) atau membuat *stream cipher* dengan ide sendiri. Memodifikasi RC4 dapat berarti memodifikasi prosedur KSA atau PRGA di dalam RC4, membuat fungsi permutasi yang lebih kompleks, menambahkan LFSR, dll. Membuat *stream cipher* sendiri artinya membuat *stream cipher* yang berbeda dari yang sudah ada. *Stream cipher* dapat beroperasi dalam mode bit atau *byte*. Program ditulis dalam Bahasa C/C++/Java/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 layar.
4. Program dapat menyimpan cipherteks ke dalam *file*.
5. Kunci dimasukkan oleh pengguna. Panjang kunci bebas.

Laporan tugas dikumpulkan Jumat minggu depan (18 Februari 2022) sebelum jam kuliah. Tugas perorangan atau pasangan (2 orang). Laporan yang dikumpulkan adalah file format PDF yang berisi:

1. Deskripsi algoritma stream cipher 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 (Drive dibuka 2 jam sebelum kuliah dimulai dan ditutup setelah kuliah selesai):

<https://drive.google.com/drive/folders/1EQITDCFJfvEV8vlyg46IbHQ765Wya2Ud?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.**