

**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):

Input type: Text

Input text: (plain)
 Di bawah sinar bulan purnama, air laut berkilauan,
 berayun-ayun ombak mengalir ke pantai senda surauan

Plaintext Hex Autodetect: **ON** | OFF

Function: AES

Mode: ECB (electronic codebook)

Key: (plain)
12345678

Plaintext Hex

> Encrypt! > Decrypt!

Encrypted text:

00000000	46 4f a1 f5 b3 d3 ce 76 50 06 d3 dd 29 7b c4 ad	F O ; ð ¸ Ó Î v P . Ó Ý) { Ä .
00000010	6d 66 24 5d ff ae aa 02 1d 31 10 95 8c f5 4e 5c	m f \$] ý ° ¢ . . 1 . . ð N \
00000020	bd 0d 49 a0 00 b6 05 82 90 2b f9 b2 11 66 a7 32	% . I . ¶ . . + ù º . f § 2
00000030	c5 fe 6d dd 18 e6 14 a5 19 e6 0e 36 cc 95 93 e8	Å þ m Ý . æ . ¥ . æ . 6 Ì . è
00000040	db d4 3f 4e c2 45 49 6e 20 13 a2 7f 46 89 5e ac	Û Ô ? N Â E I n . ¢ F . ^ ~
00000050	bb ae 63 c0 ab 95 77 f8 c1 72 c8 d9 43 9f a4 b1	» ° c À « w ø Á r È Ù C . ¤ ±
00000060	16 36 a1 95 f3 f7 00 da 27 fa ef 2a a5 12 c2 1f	. 6 ; ó ÷ . Ú ' ú ï * ¥ . Ä .

[\[Download as a binary file\] \[?\]](#) Inactive

File PDF diunggah ke alamat berikut:

<https://drive.google.com/drive/u/1/folders/1bp8zDfpozFdZlpy2YixYdnB2ypxgCvSs>

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.