

**Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung**

=====

**Tugas 1 II4031 Kriptografi dan Koding
Semester II Tahun 2023/2024**

Buatlah sebuah program berbasis web atau program desktop (pilih salah satu) dalam Bahasa C/C++/Java/Python/Ruby/Golang/dll (pilih salah satu) dengan antarmuka (GUI) yang mengimplementasikan:

- a) *Vigenere Cipher* standard (26 huruf alfabet)
 - b) *Extended Vigenere Cipher* (256 karakter ASCII)
 - c) *Playfair Cipher* (26 huruf alfabet)
 - d) *Product cipher: kombinasi Vigenere Cipher (26 huruf alfabet) dan cipher transposisi berbasis kolom (26 huruf alfabet)*
- Bonus: *Affine Cipher (26 huruf alfabet) dan Autokey Vigenere Cipher*

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, *Playfair Cipher* dengan 26 huruf alfabet, dan *Affine Cipher* dengan 26 huruf alfabet, program hanya mengenkripsi karakter alfabet saja. Angka, spasi, dan tanda baca lainnya diabaikan dan dibuang saat cipherteks ditampilkan atau disimpan.
3. Program dapat mendekripsi cipherteks menjadi plainteks semula.
4. Untuk pesan berupa text, program dapat menampilkan plainteks dan cipherteks di layar. Cipherteks sebaiknya ditampilkan dalam kode Base64.
5. Program dapat menyimpan cipherteks ke dalam *file*.
6. Kunci dimasukkan oleh pengguna. Panjang kunci bebas.
7. Untuk enkripsi plainteks sembarang file (khusus untuk *extended Vigenere Cipher* saja), 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 tersebut dapat dibuka oleh aplikasinya.

Laporan tugas dikumpulkan Rabu minggu depan (28 Februari 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:

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

Plaintext Hex Autodetect: **ON** | OFF

Function:

Mode:

Key: (plain)

Plaintext Hex

Encrypted text:

00000000	46 4f a1 f5 b3 d3 ce 76 50 06 d3 dd 29 7b c4 ad	F O ; ð ³ 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 \$] ŷ ° ð . . 1 . . ð N \
00000020	bd 0d 49 a0 00 b6 05 82 90 2b f9 b2 11 66 a7 32	% . I . ¶ . . + ù ² . f § 2
00000030	c5 fe 6d dd 18 e6 14 a5 19 e6 0e 36 cc 95 93 e8	Ä 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 Û C . ¨ ±
00000060	16 36 a1 95 f3 f7 00 da 27 fa ef 2a a5 12 c2 1f	. 6 ; ó ÷ . Ú ' ú i * ¥ . Ä .

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

File PDF diunggah ke alamat berikut:
https://drive.google.com/drive/folders/1n2tRMfcpOs13inUSJOLITE8WADMxtagk?usp=drive_link

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.

Lengkapi tabel berikut di dalam laporan dengan mencentang kolom):

No	Spek	Berhasil (√)	Kurang berhasil (√)	Keterangan
1	Vigenere standard			
2	Extended Vigenere Cipher			
3	Playfair cipher			
4	Product cipher			
5	Bonus 1: Affine Cipher			
6	Bonus 2: Autokey Vigenere 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