

Tugas 1 IF4020 Kriptografi
Semester II Tahun 2023 / 2024

Buatlah sebuah program dengan antarmuka (GUI) berbasis web. Pemilihan bahasa pemrograman yang digunakan dibebaskan kepada mahasiswa (Javascript / Typescript / PHP / Python / Golang pilih salah satu). Program mengimplementasikan:

- a) *Vigenere Cipher* standard (26 huruf alfabet)
- b) Varian *Vigenere Cipher* standard (26 huruf alfabet): *Auto-Key Vigenere Cipher*
- c) *Extended Vigenere Cipher* (256 karakter ASCII)
- d) *Playfair Cipher* (26 huruf alfabet)
- e) *Affine Cipher* (26 huruf alfabet)
- f) *Hill Cipher* (26 huruf alfabet)
- g) Super enkripsi: gabungan *Extended Vigenere Cipher* dan *cipher transposisi* (metode kolom)
- h) Bonus 1: Enigma cipher
- i) Bonus 2: Menggunakan bahasa Ruby

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 *cipher* dengan keterangan 26 huruf alfabet, program hanya mengenkripsi karakter alfabet saja. Angka, spasi, dan tanda baca dibuang dari plainteks dan cipherteks.
3. Program dapat mendekripsi cipherteks menjadi plainteks semula.
4. Program dapat menampilkan pesan (plainteks maupun cipherteks) di layar dalam kode *base64*.
5. Cipherteks di layar ditampilkan tanpa spasi dan semuanya huruf kecil (atau huruf kapital) dalam kode *base64*.
6. Program dapat menyimpan cipherteks ke dalam *file* (*save as* atau *download as a binary file*).
7. Kunci dimasukkan oleh pengguna. Panjang kunci bebas.
8. Untuk enkripsi pesan berupa *file*, 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 digunakan kembali.

9. Untuk enkripsi plainteks *file* dengan ekstensi sembarang, format file cipherteks bebas (misalnya sebagai file dengan ekstensi .dat, lihat contoh gambar di bawah). Ketika didekripsi, maka jenis filenya harus disimpan dengan jenis yang sama seperti file plainteks, misalnya jika file plainteks bertipe docx maka pada saat didekripsi pengguna harus menyimpan dengan ekstensi docx juga agar bisa dibaca kembali oleh program Microsoft Word, jika file plainteks bertipe .jpg maka pada waktu dekripsi harus disimpan dengan ekstensi .jpg juga, dst. Anda boleh menyimpan ekstensi file atau nama file plainteks di dalam file cipherteks agar pada saat dekripsi pengguna tidak perlu memikirkan jenis file apa yang dienkripsi sebelumnya.
10. Beberapa pustaka untuk menghitung balikan modulo, matriks balikan, aljabar linier, diperbolehkan.
11. Boleh menggunakan *framework* pemrograman apapun seperti ReactJs, Flask, Ruby on Rails, dan lain sebagainya.

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 surauan

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 i ð 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 ° ð . . 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 p 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 i ó ÷ . Ú ' ú i * ¥ . Â .

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

Inactive

Laporan tugas dikumpulkan **Kamis minggu depan (22 September 2024)** sebelum jam kuliah.

Tugas sebaiknya dibuat berpasangan (2 orang), tetapi juga diperkenankan per orang. Laporan yang dikumpulkan adalah *file* format PDF yang berisi:

1. Tampilan antarmuka program (*print screen*).
2. Contoh plainteks dan cipherteks (text, gambar, *file database*, audio, video)
3. *Link* ke github (*repo* di publik setelah pengumpulan) yang berisi kode program. Lengkapi dengan README berisi cara menjalankan program.

File PDF diunggah ke alamat berikut:

https://drive.google.com/drive/folders/1jtq0U_K2SFUoK9QT62GmlcW1B0miMHpB?usp=drive_link (satu jam setelah kuliah akses drive tsb ditutup)

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 tempat lain atau dari orang lain.

Jika ada pertanyaan, silakan disampaikan melalui sheets berikut:

<https://docs.google.com/spreadsheets/d/1csV5V3yBy5a8KoUETKMduP8B0gwJEff7vt31KtqzbBk/edit#gid=0>

Lengkapi tabel berikut di dalam laporan dengan mencentang kolom:

No	Spek	Berhasil (✓)	Kurang Berhasil (✓)	Keterangan
1.	<i>Vigenere Cipher</i> standard (26 huruf alfabet)			
2.	Varian <i>Vigenere Cipher</i> standard (26 huruf alfabet): <i>Auto-Key Vigenere Cipher</i>			
3.	<i>Extended Vigenere Cipher</i> (256 karakter ASCII)			
4.	<i>Playfair Cipher</i> (26 huruf alfabet)			
5.	<i>Affine Cipher</i> (26 huruf alfabet)			

6.	<i>Hill Cipher</i> (26 huruf alfabet)			
7.	Super enkripsi			
8.	(Bonus) Enigma cipher			
9.	(Bonus) Bahasa Ruby			

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.