**Program Studi Teknik Informatika**

**Sekolah Teknik Elektro dan Informatika**

**Institut Teknologi Bandung**

**===============================**

# **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:

1. *Vigenere Cipher* standard (26 huruf alfabet)
2. Varian *Vigenere Cipher* standard (26 huruf alfabet): *Auto-Key Vigenere Cipher*
3. *Extended Vigenere Cipher* (256 karakter ASCII)
4. *Playfair Cipher* (26 huruf alfabet)
5. *Affine Cipher* (26 huruf alfabet)
6. *Hill Cipher* (26 huruf alfabet)
7. Super enkripsi: gabungan *Extended Vigenere Cipher* dan *cipher transposisi* (metode kolom)
8. Bonus 1: Enigma cipher
9. 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 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 Microsof 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):



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 dipublic setelah pengumpulan) yang berisi kode program. Lengkap 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.

Lengkapi tabel berikut di dalam laporan dengan mencentang kolom:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Spek | Berhasil (✓) | Kurang Berhasil (✓) | Keterangan |
| 1. | *Vigenere Cipher* standard (26 huruf alfabet) |  |  |  |
| 2. | Varian *Vigenere Cipher* standard (26 huruf alfabet): *Auto-Key Vigenere Cipher* |  |  |  |
| 3. | *Extended Vigenere Cipher* (256 karakter ASCII) |  |  |  |
| 4. | *Playfair Cipher* (26 huruf alfabet) |  |  |  |
| 5. | *Affine Cipher* (26 huruf alfabet) |  |  |  |
| 6. | *Hill Cipher* (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.