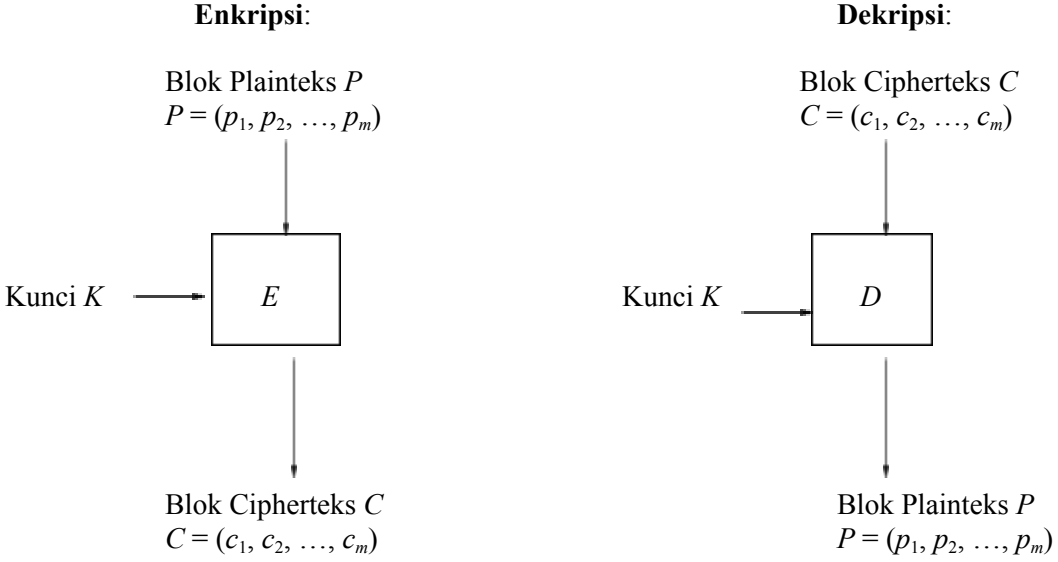
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
==========

Tugas 3 IF4020 Kriptografi
Semester II Tahun 2023/2024

Merancang dan Mengimplementasikan Cipher Blok "Baru"

Sebagaimana yang sudah dijelaskan di dalam kuliah, pada tugas 3 ini anda mengembangkan *block cipher* 'baru'. Skema algoritma blok *cipher* adalah Gambar 1.



Gambar 1 Skema enkripsi dan dekripsi pada *cipher* blok

Anda harus merancang fungsi *E* dan *D* yang sekompleks mungkin sehingga algoritma enkripsi menjadi sangat sukar dipecahkan. Spesifikasi fungsi *E* dan *D* (keduanya identik) adalah sebagai berikut:

1. Menerapkan prinsip ***diffusion*** dan ***confusion*** dari **Shannon**
2. Mendefinisikan fungsi putaran (*f*) yang berisi jaringan **substitusi-permutasi**.
3. Operasi substitusi dan transposisi (keduanya beroperasi dalam bit atau byte). Aturan substitusi dan transposisi diserahkan kepada anda untuk mendefinisikannya (dapat menggunakan tabel substitusi S-box dan matriks permutasi, atau menggunakan pergeseran bit atau byte untuk permutasi). Rancangan fungsi *E* dan *D* harus dijelaskan di dalam laporan.
4. Menerapkan ***cipher* berulang**, yaitu melakukan *enciphering* terhadap blok pesan berulang kali sejumlah putaran. Setiap putaran menggunakan kunci putaran yang berbeda-beda. Kunci putaran dibangkitkan dari kunci eksternal.
5. Ukuran blok pesan yang dienkripsi adalah **128 bit**
6. Panjang kunci antara **128-256 bit**.
7. Jumlah putaran **10-16 kali.**

8. Dianjurkan menggunakan jaringan Feistel untuk iterated cipher, namun tidak diharuskan.
9. Beri nama *block cipher* anda tersebut, misalnya MyCRYPT, CrytpMania, FastChip, ChipMunk, WhisPher, dll.

Setelah rancangan *block cipher* selesai diimplementasi, selanjutnya buatlah sebuah aplikasi **desktop/web-based** untuk mengenkripsi dan dekripsi pesan (**teks yang diketik** atau **file biner**) dengan menggunakan **pilihan mode ECB, CBC, OFB, CFB, dan Counter**.

Tugas sebaiknya dibuat berkelompok (minimal 2 maksimal 3 orang). Laporan yang dikumpulkan adalah *file* format PDF yang berisi:

1. Desain *Block Cipher* (*Proposed Method*)
   Berisi rincian algoritma enkripsi dan dekripsi, termasuk skema, diagram, tabel, dll.
2. Tampilan antarmuka program
3. Eksperimen dan pembahasan hasil
   Berisi hasil uji enkripsi dan dekripsi dan menganalisis hasil-hasilnya, meliputi:
   - Waktu enkripsi dan dekripsi untuk pesan dengan berbagai macam pesan (teks, file)
   - Analisis efek longsoran (*avalanche effect*), yaitu bagaimana perubahan cipherteks jika satu bit atau satu *byte* plainteks atau kunci diubah
   - Analisis ruang kunci (*key space*)
   - Analisis keamanan lainnya
4. Kesimpulan dan Saran
   Berisi konklusi dari hasil-hasil yang sudah diperoleh dan saran pengembangan (*future works*).
5. Daftar referensi
   Berisi semua referensi yang digunakan di dalam pembuatan tugas
6. Link ke github (repo disetel publik setelah pengumpulan) yang berisi kode program. Lengkap dengan README berisi cara menjalankan program.

Ada 2 artefak yang harus dikumpulkan:

1. Link kode program, dengan mengisi sheets
   https://docs.google.com/spreadsheets/d/1tOEjA8HoFxEo-PgVfcPrBeeeiYyHiDRW-n4OJKZrLRM/edit?usp=sharing
2. Laporan, upload laporan ke
   https://drive.google.com/drive/folders/1nffDaXTamKkV42howuK3QcwIFkd9tbi7?usp=sharing

   Kumpulkan laporan dengan format nama Tugas3_<Nomor Kelompok>.pdf

   <Nomor Kelompok> disesuaikan dengan nomor di sheets pengumpulan link kode program. Contoh: Tugas3_00.pdf

Waktu pengerjaan tugas adalah sampai sebelum UTS, yaitu selambatnya Sabtu 23 Maret 2024 pukul 23.59 WIB.