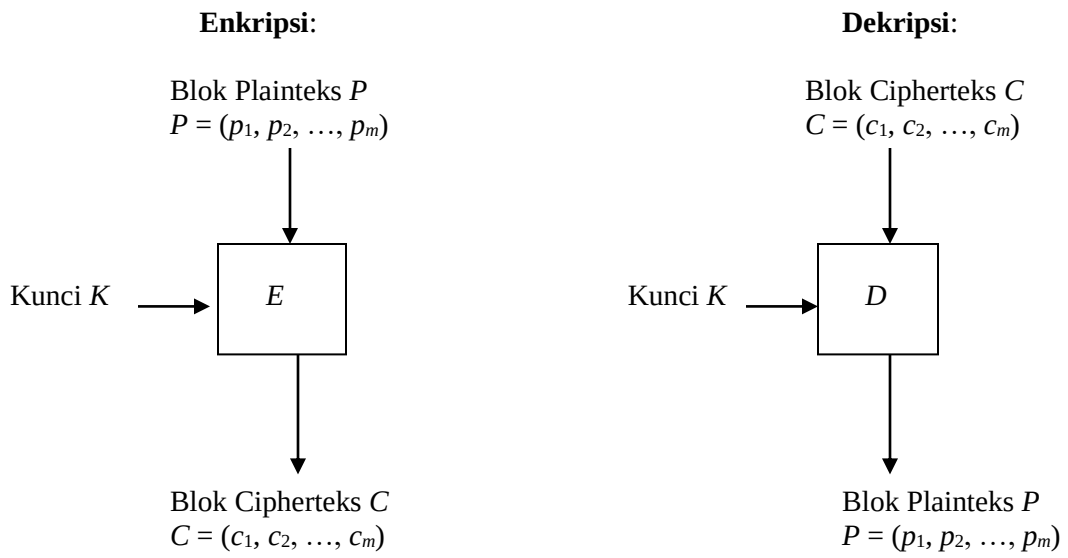
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
==========

Tugas 2 IF4020 Kriptografi
Semester II Tahun 2022/2023

Merancang dan Mengimplementasikan Cipher Blok "Baru"

Sebagaimana yang sudah dijelaskan di dalam kuliah, pada tugas 2 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 tabel permutasi, atau meggunakan pergeseran bit atau byte untuk permutasi). Rancangan fungsi *E* dan *D* harus dijelaskan di dalam makalah
4. Menerapkan *cipher* berulang, yaitu melakukan *enciphering* terhadap blok pesan berulangkalis ejumlah 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 128 bit.
7. Jumlah putaran 16 kali
8. Boleh menggunakan jaringan Feistel
9. Beri nama block cipher anda tyersebut, misalnya INDOCRYPT, CrypMania, dll.

Setelah rancangan *block cipher* selesai diimplementasi dan diujicoba, selanjutnya anda sebarkan algoritma *block cipher* tersebut dalam bentuk makalah. Makalah ditulis dalam Bahasa Indonesia atau Bahasa Inggris. Isi makalah adalah sebagai berikut:

1. Pendahuluan
   Berisi latar belakang, masalah, dan *related works* (mengacu pada referensi/paper)
2. Studi Pustaka/Dasar Teori
   Berisi konsep/teori yang digunakan di dalam *block cipher* yang anda buat. Tidak usah berpanjang-panjang dan menyita banyak halaman
3. Rancangan *Block Cipher* (*Proposed Method*)
   Berisi rincian algoritma enkripsi dan dekripsi, termasuk skema, diagram, tabel, dll.
4. Eksperimen dan Pembahasan Hasil
   Berisi hasil uji enkripsi dan dekripsi dan menganalisis hasil-hasilnya, meliputi:
   - Waktu enkripsi dan dekripsi untuk pesan dengan ukuran beragam (small, medium, large, very large)
   - 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
5. Kesimpulan dan Saran
   Berisi konklusi dari hasil-hasil yang sudah diperoleh dan saran pengembangan (*future works*).
6. Daftar referensi
   Berisi semua referensi yang digunakan di dalam makalah

Jumlah halaman makalah tidak dibatasi, namun jangan terlalu singkat karena tidak menggambarkan keseluruhan hasil penelitian.

Tugas dibuat berkelompok, sedikitnya 2 orang dan sebanyaknya 3 orang. Makalah ditulis dengan format IEEE (lihat lampiran). Unduh *template* makalah pada laman web berikut:

Makalah dikumpulkan paling lambat hari Minggu tanggal 5 Maret 2023 pukul 23.59 WIB pada google drive berikut:
https://drive.google.com/drive/folders/1L92-dwx3joV8OZ8qNJ_-a24ULNbIaa0Y?usp=share_link

Link kode program (untuk dicoba leh asisten) diberikan pada laman Google Sheet berikut:
https://docs.google.com/spreadsheets/d/1p1byvK7XhQaArLZEaOOfXVSODfOmwFamPKCctBwDzFw/edit?usp=sharing

Makalah ditulis dengan format IEEE (unduh dari halaman website).

Silakan mengunduh beberapa comntoh makalah yang melaporkan hasil penghembangan block cipher baru.

Lain-lain

a. Jangan menjadikan Wikipedia sebagai salah satu daftar referensi. Boleh menjadikan Wikepedia sebagai bahan bacaan awal, tetapi gunakan referensi yang terdapat di laman Wikipedia tersebut sebagai daftar referensi.
b. Semua gambar, tabel, diagram, dan lain-lain yang diambil dari karya orang lain dan dipakai di dalam makalah harus disebutakn sumbernya.
c. Jangan sekali-kali melakukan *copas* meskipun terjemahan, tulislah kembali dalam gaya bahasa anda sendiri dan sebutkan sumbernya (jika dikutip seluruhnya).
d. Jangan mengakali jumlah halaman dengan memuat banyak gambar.

e. Jangan menuliskan dasar teori secara panjang lebar, cukup yang penting-penting saja. Makalah harus lebih banyak membahas substansi. Kalau ingin memaparkan dasar teori lebih jelas, cukup dituliskan acuan ke referensi saja.