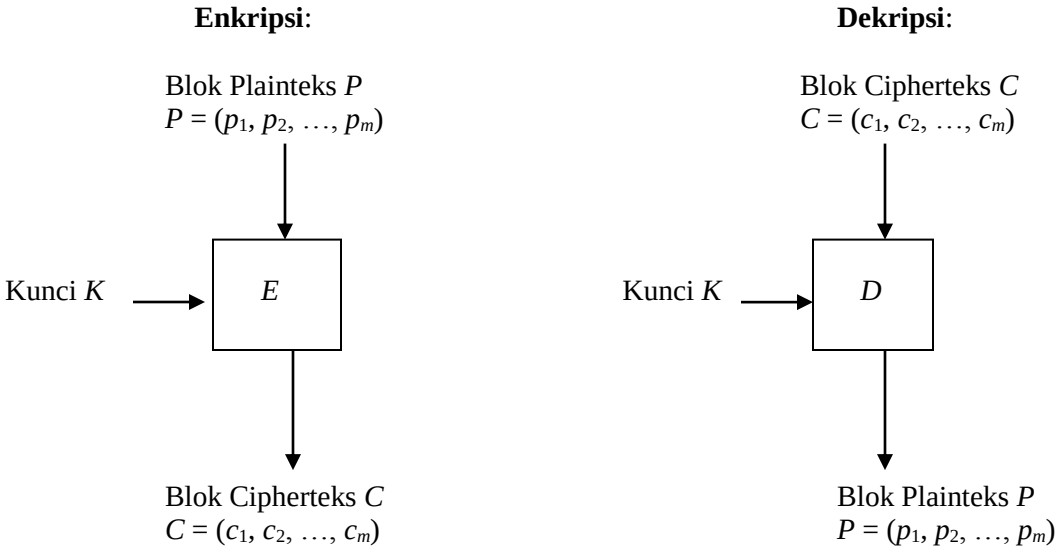
Tugas Makalah I (Pengganti UTS)
Rancangan dan Implementasi Algoritma *Block Cipher* 'Baru'

IF4020 Kriptografi, Semester II Tahun 2014/2015

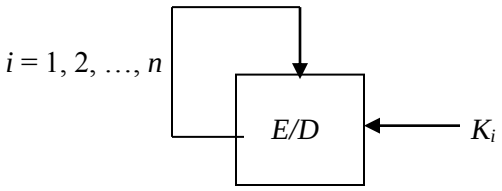
Sebagaimana yang sudah dijelaskan di dalam kuliah, makalah I berisi hasil penelitian mengembangkan sebuah *block cipher* 'baru' seperti *block cipher* yang sudah dipublikasikan (DES, RC5, *Rijndael*, *GOST*, *Blowfish*, dll). Skema algoritma blok *cipher* adalah Gambar 1.



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 (mengacu kepada prinsip *diffusion* dan *confusion* dari Shannon). Fungsi *E* dan *D* (keduanya identik) harus melibatkan:

1. Operasi substitusi dan transposisi (keduanya beroperasi dalam bit, byte, atau dalam hexadesimal). Aturan substitusi dan transposisi diserahkan kepada anda untuk mendefinisikannya (dapat menggunakan tabel substitusi dan tabel permutasi). Rancangan fungsi *E* dan *D* harus dijelaskan di dalam laporan tugas
2. Untuk menambah kerumitan, maka gunakan struktur Jaringan Feistel.
3. Untuk memberikan efek diffusion, terapkan *cipher* berulang, yaitu untuk setiap blok bit, fungsi *E* atau *D* dikerjakan sejumlah kali (*round*), seperti pada Gambar 2. Algoritma blok *cipher* anda yang "baru" harus dapat dioperasikan dalam mode *ECB*, *CBC*, dan *CFB* 8-bit untuk blok data *n*-bit (misalnya, untuk *CFB* 8-bit, panjang blok 64 bit). Jaringan Feistel digunakan di dalam pengulangan ini.



Gambar 2 Skema *cipher* berulang untuk setiap blok bit yang dienkripsi/dekripsi

Hal-hal lain yang perlu diperhatikan adalah sebagai berikut:

1. Algoritma kriptografi simetri *block cipher* yang diimplementasikan dapat melakukan proses enkripsi/dekripsi terhadap blok-blok data. Ukuran blok data minimal 64-bit (setara dengan 8 karakter). Panjang blok otomatis diketahui dari panjang kunci yang diberikan oleh pengguna program.
2. Panjang kunci (*K*) harus sama dengan panjang blok yang dispesifikasikan.
3. Khusus untuk mode *CBC*, *initialiazation vector* (*IV*) dibangkitkan secara acak oleh program (pengguna tidak perlu memasukkan *IV*, pengguna cukup memasukkan mode blok *cipher* dan kunci saja).
4. 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
5. Analisis Keamanan
   Berisi analisis keamanan *block cipher* yang anda kembangkan
6. Kesimpulan dan Saran
   Berisi konklusi dari hasil-hasil yang sudah diperoleh dan saran pengembangan (*future works*).
7. 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.

Makalah dikumpulkan tepat satu minggu setelah UTS Kriptografi (sesuai jadwal) yaitu pada jam kuliah. Makalah dikumpulkan dalam bentuk *hard-copy*, sedangkan *soft copy*-nya dalam bentuk file *pdf* dikirim ke rinaldi@informatika.org

Makalah ditulis dengan format IEEE (lihat lampiran). Unduh *template* makalah pada laman web berikut: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/kripto14-15.htm

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.