

**Tugas II IF5054 Kriptografi**  
**Sem. I Tahun 2007/2008**

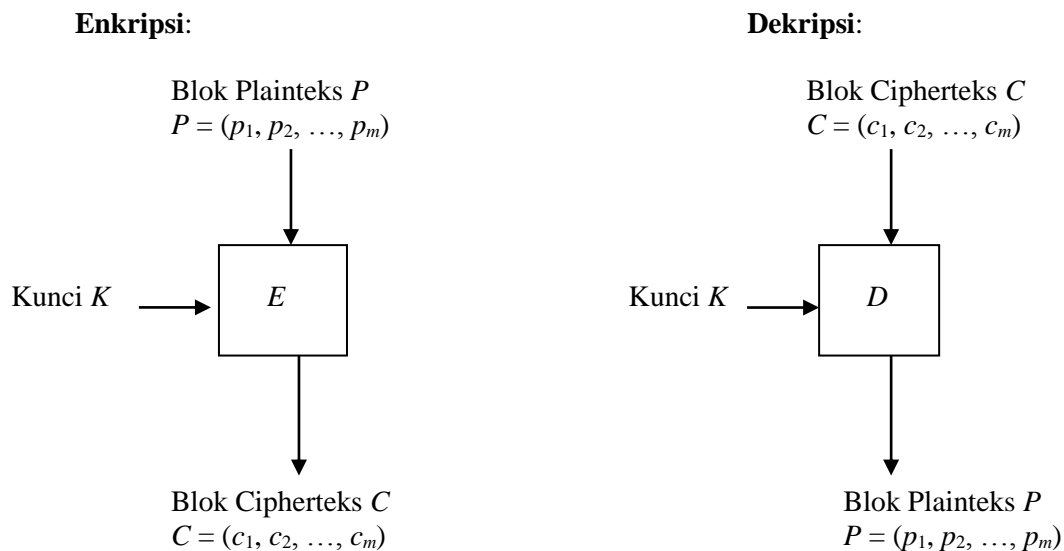
**Perancangan dan Implementasi Algoritma Kriptografi**  
**“Baru” dengan Mode *ECB*, *CBC*, dan *CFB***

**Tujuan:**

Mengimplementasikan algoritma kriptografi simetri *block cipher* dengan mode *ECB* (*Electronic Code Book*), *CBC* (*Cipher Block Chaining*), dan *CFB* (*Cipher Feedback*)  $n$ -bit untuk blok data  $n$ -bit.

**Deskripsi tugas:**

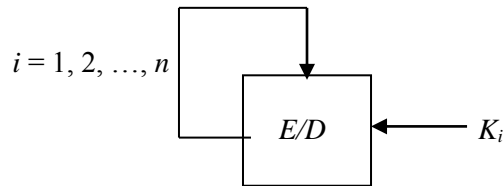
Pada Tugas ke-2 ini anda berlaku sebagai seorang kriptografer, yaitu orang yang merancang sebuah algoritma kriptografi. Skema algoritma blok *cipher* adalah Gambar 1.



**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 (menggunakan prinsip *diffusion* dan *confusion* dari Shannon). Fungsi  $E$  dan  $D$  harus melibatkan:

1. Operasi substitusi dan transposisi (keduanya beroperasi dalam bit 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 memperkuat *cipher*, 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*  $n$ -bit untuk blok data  $n$ -bit (misalnya, untuk *CFB* 64-bit, panjang blok juga 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). Ukuran blok adalah kelipatan 8-bit. 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. Bahasa pemrograman yang digunakan diharapkan menekankan antarmuka yang memudahkan pengguna (*user friendly*) sehingga diharapkan memilih perangkat (*tools*) pemrograman yang mendukung grafis. Lingkungan pemrograman dapat berada pada lingkungan *windows* atau *linux*. Kakas pemrograman yang digunakan bebas.
5. Program yang dibuat mampu menangani:
  - a. Proses enkripsi menerima nama arsip plainteks, kunci ( $K$ ). Kunci  $K$  merupakan *string* alfanumerik yang dibaca dari papan ketik.
  - b. Proses dekripsi menerima nama arsip cipherteks dan kunci ( $K$ ). Ukuran blok, mode, dan  $IV$  seharusnya tidak perlu menjadi masukan untuk proses dekripsi (dengan kata lain, ukuran blok, mode, dan  $IV$  sebaiknya disimpan di dalam *header* arsip cipherteks. **Jangan menyimpan kunci di dalam arsip cipherteks!**).
  - c. Arsip yang dienkripsi adalah sembarang arsip dengan format apa pun (arsip *text*, arsip *word*, arsip *spread sheet*, arsip gambar, arsip *database*, *executable file*, dan sebagainya).
  - d. Menampilkan dan menyimpan arsip hasil enkripsi dan hasil dekripsi. Jadi, anda harus juga membuat *editor* sederhana yang hanya berfungsi menampilkan karakter-karakter hasil enkripsi/dekripsi (tidak dapat melakukan *editing*). Perhatikan bahwa jika arsip yang dienkripsi bukan arsip *text*, maka hasil enkripsinya tidak dapat dibuka oleh program aplikasi yang bersesuaian karena *header file* juga ikut terenkripsi. Namun karakter-karakter hasil enkripsinya masih dapat ditampilkan ke editor sederhana di atas. Khusus arsip *text* (tanpa format), hasil enkripsi maupun dekripsinya dapat dibuka oleh editor sederhana ini tanpa masalah. Contoh program dari angkatan sebelumnya dapat dijadikan acuan (*download* berkas *exe*-nya di [http://mail.informatika.org/~rinaldi](mailto:mail.informatika.org/~rinaldi)).

6. Berkas *executable* yang didekripsikan harus dapat di-*run* kembali, berkas gambar (*image*) hasil dekripsi harus dapat dibuka kembali oleh aplikasi gambar, berkas musik/video hasil dekripsi harus dapat dimainkan kembali oleh *media player*.

### Prosedur Pengerjaan

1. Tugas dikerjakan secara berkelompok (1 kelompok @ 3 orang).
2. Waktu pengumpulan tugas: paling lambat 5 Oktober 2007 sebelum pukul 17.00 di Lab IRK).
3. Yang diserahkan pada saat pengumpulan antara lain:
  - a. Disket atau CD yang berisi program sumber (*source code*), arsip siap eksekusi (*executable file*) (termasuk semua *.dll* jika ada), dan arsip-arsip contoh untuk enkripsi/dekripsi.
  - b. Laporan yang memiliki sistematika sebagai berikut :
    - i. Teori singkat (kriptografi, terutama blok cipher, mode *ECB*, *CBC*, dan *CFB*).
    - ii. Perancangan dan Implementasi, termasuk : rancangan fungsi *E* dan *D* yang anda usulkan, modularisasi program, struktur data, keterangan tentang *header* arsip cipherteks, antarmuka, lingkungan pengembangan, dll. Cantumkan juga pembagian tugas antar anggota kelompok dalam bab ini.
    - iii. Pengujian program dan analisis hasil. Uji program dengan bermacam-macam arsip. Lakukan juga pengujian untuk mengukur tingkat keamanan algoritma (misal: pengubahan 1 bit plainteks/cipherteks, penambahan blok cipherteks semu, penghilangan satu/lebih blok cipherteks, dsb. Anda boleh menggunakan aplikasi lain untuk melakukan pengubahan tersebut, seperti Edit Plus, Ultra Edit, Norton Utilities, dsb)
    - iv. Kesimpulan dari hasil implementasi.

Laporan dikumpulkan dalam bentuk *hard copy* dan *soft copy* dengan format \*.pdf .

4. Penilaian tugas dilakukan pada saat demo.