Tugas Pengganti UTS IF4020 Kriptografi

Semester Genap Tahun 2017/2018

Rancanglah sebuah *block cipher* "baru" dengan spesifikasi *minimal* sebagai berikut:

1. Ukuran blok bebas, minimal 64 bit
2. Beroperasi dalam bit, *byte*, atau hexadecimal.
3. Panjang kunci minimal sepanjang blok
4. Menerapkan struktur Feistel di dalam algoritmanya sehingga tidak diperlukan algoritma dekripsi yang berbeda dengan enkripsi.
5. Menerapkan prinsip *diffusion* dan *confusion* dari Shannon.
6. Menerapkan operasi dasar: substitusi dan transposisi (permutasi). Substitusi boleh menggunakan tabel (kotak-S).
7. Operasi selain substitusi dan transposisi dianjurkan, misalnya pergeseran, rotasi, penjumlahan modulo, dan lain-lain.
8. Menerapkan sejumlah putaran (*iterated cipher*) sebanyak *n k*ali. Setiap putaran menggunakan kunci putaran (*round key*). Kunci putaran dibangkitkan dari kunci eksternal.
9. Selain delapan poin di atas, silakan menambahkan kreatifitas lainnya.
10. Buatlah algoritma anda sekompleks/serumit mungkin. Beri nama block cipher anda tersebut dengan nama yang bagus.

Setelah rancangan anda selesai, coding-lah menjadi program enkripsi dan dekripsi dalam pemrograman yang dipilih (bebas), minimal Bahasa C. *Block cipher* harus dapat dioperasikan dalam mode ECB, CBC, CFB, OFB, dan mode *counter*.

Materi yang dikumpulkan di dalam tugas pengganti UTS ini hanyalah laporan berupa makalah standard format IEEE (format 2 kolom), silakan unduh template makalah di www.ieee.org.

Makalah berisi poin-poin sebagai berikut:

1. Judul, nama penulis dan afiliasi serta email
2. Abstraksi dan kata-kata kunci (minimal 6 kata/frase kata)
3. Pendahuluan: latar belakang, review beberapa *block cipher* sejenis (misalnya DES, AES, dll), gagasan/pendekatan yang digunakan di dalam *block cipher* "baru" anda.
4. *Proposed block cipher*: berisi rancangan detil *block cipher* anda. Jelaskan secara rinci algoritma enkripsi anda. Tuliskan juga skema dekripsinya. Penggambaran menggunakan diagram, bagan, tabel, dll sangat membantu pembaca memahaminya.

5. Simulasi dan pembahasan hasil. Jelaskan hasil-hasil implementasi *block cipher* anda (yang sudah dikode ke dalam Bahasa pemrograman), serta hasil-hasil enkripsi dan dekripsi. Lakukan pengujian *block cipher*, misalnya pengubahan satu bit kunci, satu bit plainteks, satu bit cipherteks, perhatikan bagaimana hasilnya. Analisis hasil-hasil pengujian tersebut. Anaisis juga keamanannya.
6. Kesimpulan dan saran pengembangan (future works)

Makalah dikumpulkan pada hari Rabu setelah UTS. Soft copy makalah berupa file PDF dikirim ke alamat email saya: rinaldi.munir@itb.ac.id

Tugas ini dibuat per kelompok, @2 orang

Minggu depan dikumpulkan proposal *block cipher* anda yang berisi *extended abstract* rancangan *block cipher* secara garis besar (max 2 halaman).