Tugas Pengganti UTS IF4020 Kriptografi

Semester Genap Tahun 2020/2021

(Per kelompok @2 orang)

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 menggunakan tabel (kotak-S). Definisikan sendiri 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 Bahasa pemrograman yang dipilih (bebas), minimal Bahasa C. *Block cipher* harus dapat dioperasikan minimal dalam tiga mode ECB, CBC, dan mode *counter*.

Materi yang dikumpulkan sebagai tugas pengganti UTS ini adalah jurnal (dalam Bahasa Indonesia atau Bahasa Inggris) dengan format yang standard (diunduh dari situs kuliah).

Jurnal 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. Bagian 1: Pendahuluan, berisi latar belakang, review beberapa *block cipher* sejenis (misalnya DES, AES, dll), gagasan/pendekatan yang digunakan dalam merancang *block cipher* "baru" anda. Sitat (*cite*) di dalam tulisan referensi yang digunakan.

4. Bagian 2: Studi Pustaka, berisi teori singkat yang penting-penting saja seperti yang terkait dengan block cipher, teori pendukung lain seperti konsep matematika yang digunakan, dll
5. Bagian 3: *Proposed block cipher*, berisi rancangan detil *block cipher* anda. Jelaskan secara rinci algoritma enkripsi dan dekripsi anda, strukturnya seperti apa, berepa kali putaran, pembangkitan kunci putaran, fungsi f, kotak-S, operasi permutasi, pergeseran, dan transformasi lainnya. Penggambaran menggunakan diagram, bagan, tabel, dll sangat membantu pembaca memahaminya.
6. Bagian 4: Eksperimen dan Analisis Hasil, berisi eksperimen enkripsi/dekripsi pesan, contoh skrinsut program, dan hasil-hasil pengujian lain seperti ukuran pesan, waktu enkripsi/dekripsi, kunci, dan-lain-lain. Analisis hasil-hasil implementasi *block cipher* anda (yang sudah dikode ke dalam Bahasa pemrograman). Lakukan pengujian *block cipher*, misalnya pengubahan satu bit kunci, satu bit plainteks, satu bit cipherteks, perhatikan bagaimana hasilnya. Analisis hasil-hasil pengujian tersebut. Analisis juga keamanannya (cari referensi yang menjelaskan cara mengukur aspek keamanan block cipher).
7. Bagian 5: Ksimpulan dan saran pengembangan (future works)

Makalah dikumpulkan pada hari Jumat 23 Oktober paling lambat pukul 15.00. Soft copy makalah dalam format PDF diunggah ke alamat Google Drive (akan diumumkan via grup WA).