Tugas Makalah I (Pengganti UTS)
IF3058 Kriptografi, Semester II Tahun 2010/2011

Buatlah makalah yang berisi *technical report* yang berkaitan dengan hasil riset skala kecil tentang salah satu dari topik kriptografi di bawah ini (boleh dipilih satu):

1. Jenis-jenis serangan (*attack*) pada kriptografi
2. Algoritma kriptografi klasik (misal *Caesar cipher*, Vigenere *cipher*, Playfair *cipher*, dll)
3. Kriptanalisis (analisis frekuensi, *differential analysis*, dll)
4. Algoritma kriptografi modern (*stream cipher* dan *block cipher*)
5. Steganografi dan *watermarking*

Kata kunci untuk makalah tersebut adalah kontribusi. Makalah harus berisi kontribusi anda (usulan/analisis/perancangan/pengujian), bukan studi literatur atau kompilasi bahan berbagai sumber.
Makalah dapat berupa:

- Hasil analisis terhadap algoritma kriptografi kunci-simetri tertentu, termasuk perbandinganya dengan algoritma yang sejenis. Sebaiknya ada program tes yang menguji performansi dan keamanannya.
- Menganalisis sistem keamanan menggunakan kriptografi pada suatu *platform*/*tools*/aplikasi, dsb
- Mengivestigasi aplikasi sistem kriptografi kunci-simetri di bidang tertentu
- Rancangan algoritma kriptografi kunci-simetri yang diusulkan sendiri, lengkap dengan konsep, implementasi, dan pengujiannya.
- Dll

Contoh-contoh judul makalah:

1. Perbandingan algoritma simetri Camellia dengan *DES*
2. Aplikasi *Identity-based Encryption* pada Keamanan Jaringan Komputer
3. Keamanan pada jaringan VoIP
4. Aplikasi *spread spectrum steganography* pada data audio
5. Eksplorasi Keamanan pada *Windows 7 Encryption File System*
6. dll

Sebelum membuat makalah, anda diharuskan menyusun proposal (format bebas) makalah yang akan anda buat. Proposal setidaknya berisi *extended abstract* yang berisi latar belakang, rumusan masalah, batasan masalah, dll, termasuk daftar pustaka. Proposal maksimum 2 halaman.

Proposal diserahkan kepada dosen IF5054 untuk diperiksa dan disetujui. Penyerahan proposal adalah pada tanggal 2 Maret 2010. Proposal akan diperiksa dan hasilnya ada dua kemungkina: disetujui atau ditolak. Jika ditolak, maka proposal harus ditulis lagi dengan topik yang berbeda. Makalah dikumpulkan tepat satu minggu setelah UTS Kriptografi (sesuai jadwal) yaitu pada jam kuliah.

Makalah ditulis dengan ketentuan berikut:

1. *Font* = *Times New Roman*, Ukuran *font* = 10
2. Lebar spasi = 1
3. Format 2 kolom (lihat *template*)
4. Jumlah halaman minimal = 6 halaman, maksimal = 10 halaman.

Makalah tidak boleh sama dengan makalah yang sudah dibuat pada tahun-tahun sebelumnya, selain itu belum pernah diberikan di dalam kuliah.