Tugas Makalah I (Pengganti UTS)
IF4020 Kriptografi, Semester II Tahun 2013/2014

Buatlah makalah yang berisi *technical report* dari riset kriptografi skala kecil hingga sedang yang berkaitan dengan 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, dilengkapi hasil uji dari program/kakas.
- Menganalisis sistem keamanan menggunakan kriptografi pada suatu *platform*/*tools*/aplikasi, dsb, didalamnya ada eksperimen menggunakan aplikasi/kakas.
- Rancangan algoritma kriptografi kunci-simetri/steganografi/watermarking yang diusulkan sendiri, lengkap dengan konsep, implementasi, dan pengujiannya.
- Hasl kriptanalisis terhadap sebuah algoritma kriptografi (lengkap dengan eksperimen)
- 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 5 Maret 2014. 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 dikumpulkan dalam bentuk *hard-copy*, sedangkan *soft copy*-nya dalam bentuk file *pdf* dikirim ke rinaldi@informatika.org

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.

Unduh *template* makalah pada laman web berikut:
http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2013-2014/kripto13-14.htm

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

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. Setiap makalah diberi tanda tangan (*digitized signature*) pada akhir makalah (setelah pernyataan).
e. Jangan mengakali jumlah halaman dengan memuat banyak gambar.
f. 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.