Tugas Makalah II (Pengganti UAS)
IF5054 Kriptografi, Sem. I Tahun 2007/2008

Buatlah makalah yang berisi *technical report* yang berkaitan dengan salah satu dari topik kriptografi di bawah ini:

1. Sistem kriptografi kunci-publik
2. Fungsi *hash*
3. Tanda-tangan digital
4. *MAC*
5. Pembangkit bilangan acak
6. Infrastruktur kunci-publik
7. Protokol kriptografi
8. Manajemen kunci
9. Kriptografi dalam kehidupan sehari-hari

Kata kunci untuk tugas makalah ini adalah: **kontribusi**. Makalah anda harus mengandung kontribusi (usulan, saran, perbandingan, konsep baru, dsb) yang anda lakukan, tidak sekadar menyalin dan mengkompilasi berbagai sumber rujukan.

Makalah dapat berupa:

- Menganalisis algoritma kriptografi kunci-publik tertentu, termasuk perbandinganya dengan algoritma yang sejenis (kalau ada).
- Menganalisis keamanan data dan informasi pada suatu *platform*/*tools*/aplikasi yang berbasis pada sistem kriptografi kunci-publik, dsb
- Rancangan algoritma kriptografi kunci-publik yang diusulkan sendiri, lengkap dengan konsep, implementasi, dan pengujiannya.
- Dll

Sebelum membuat makalah, anda diharuskan menyusun proposal (format bebas) makalah yang akan anda buat. Proposal cukup selembar berisikan anstraksi makalah yang akan anda buat, lalu daftar referensi yang digunakan (sementara).

Proposal harus diserahkan kepada dosen IF5054 untuk diperiksa dan disetujui. Penyerahan proposal paling lambat 2 minggu sebelum UTS. Makalah dikumpulkan tepat pada saat UTS Kriptografi (sesuai jadwal).

Makalah ditulis dengan ketentuan berikut:

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

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