

**Tugas Makalah II (Pengganti UATS)
IF5054 Kriptografi, Sem. I Tahun 2006/2007**

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

Sebelum membuat makalah, anda diharuskan menyusun proposal (format bebas) makalah yang akan anda buat. Proposal hanya 1 halaman saja dan cukup berisi ringkasan (gambaran umum) makalah yang akan dibuatkannya berisi abstraksi, termasuk daftar pustaka.

Proposal diserahkan kepada dosen IF5054 untuk diperiksa dan disetujui. Penyerahan proposal paling lambat 2 minggu sebelum UAS. Makalah dikumpulkan tepat pada saat UATS 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)
4. Jumlah halaman minimal = 15 halaman

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