Tugas Makalah II (Pengganti UAS)
IF4020 Kriptografi, Sem. II Tahun 2020/2021

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

1. Algoritma kriptografi kunci-publik
2. *Elliptic Curve Cryptography*
3. Fungsi *hash*
4. Tanda-tangan digital
5. *MAC*
6. Pembangkit bilangan acak
7. Infrastruktur kunci-publik
8. Protokol kriptografi
9. Manajemen kunci
10. Kriptografi Visual
11. Skema pembagian kunci rahasia
12. 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.
- Aplikasi kriptografi kunci-publik
- Dll

Makalah ditulis peroranganan, boleh dalam Bahasa Indonesia atau Bahasa Inggris. Makalah ditulis dengan ketentuan berikut:

1. *Font* = *Times New Roman*, Ukuran *font* = 10
2. Lebar spasi = 1
3. Format 2 kolom (seperti makalah I)
4. Jumlah halaman minimal 6 halaman, maksimal tidak dibatasi

Format makalah dapat diunduh dari web kuliah.

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

Makalah dikumpulkan paling lambat tanggal 21 Desember 2020 dalam format PDF ke Google Drive berikut:
https://drive.google.com/drive/folders/1osBDBfEYNeG_kmWrDC7FkzcYgDDsQTDR?usp=sharing