Tugas Makalah
IF4020 Kriptografi, Sem. II Tahun 2022/2023

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. Sertifikat digital
8. Infrastruktur kunci-publik (PKI)
9. Protokol kriptografi
10. Kriptografi Visual
11. Skema pembagian data rahasia
12. Kriptografi dalam kehidupan sehari-hari

Kata kunci untuk tugas makalah ini adalah: **kontribusi**. Makalah membahas sebuah persoalan keamanan riil yang membutuhkan solusi kriptografi. Solusi kriptografi tersebut diimplementasikan (diprogram), dilakukan eksperimen/pengujian, dianalisis hasilnya, lalu ditarik kesimpulan.

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
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. Kode program tidak perlu dilampirkan. Daftar pustaka harus jelas dan dapat ditemukan di dalam mesin pencari.

Makalah dikumpulkan paling lambat tanggal 22 Mei 2023 dalam format PDF ke Google Drive berikut:
https://drive.google.com/drive/folders/1O_7h9xw0tb1Nyw5GqszjaLlIEnx2mraK?usp=share_link