Tugas Makalah
IF4020 Kriptografi, Semester I Tahun 2025/2026

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

1. Algoritma kriptografi kunci-simetri (stream cipher dan block cipher)
2. Steganografi dan watermarking
3. Kriptanalisis
4. Algoritma kriptografi kunci-publik
5. *Elliptic Curve Cryptography*
6. Fungsi *hash*
7. Tanda-tangan digital
8. *MAC*
9. Pembangkit bilangan acak
10. Sertifikat digital
11. Infrastruktur kunci-publik (PKI)
12. Protokol kriptografi SSL/TLS
13. Kriptografi Visual
14. Skema pembagian data rahasia
15. Lightweight cryptography
16. Post-quantum cryptography
17. Blockchain
18. 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 dengan Word atau LateX dengan ketentuan berikut:

a) Makalah dapat ditulis dalam Bahasa Indonesia atau Bahasa Inggris
b) *Font* = *Times New Roman*, Ukuran *font* = 10
c) Lebar spasi = 1
d) Format 2 kolom, unduh template makalah format IEEE dalam Word dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/kripto25-26.htm
e) Gambar yang besar (jika ada) tidak harus diletakkan dalam satu kolom tertentu), tetapi boleh penuh (memakai 2 kolom).
f) Referensi harus ditulis lengkap dengan cara penulisan referensi seperti contoh. Referensi dari internet harus mencantumkan URL dan tanggal/waktu akses.
g) Jumlah halaman minimal = 6 halaman dan maksimal = 10 halaman. Jangan mengakali jumlah halaman dengan memuat banyak gambar/tabel.
h) Alamat email di dalam makalah harus ditulis dua buah: @std.stei.itb.ac.id dan @gmail.com (gmail ditulis agar setelah mahasiswa lulus dari ITB, pembaca makalah anda bila ingin menghubungi anda maka alamat gmail masih aktif)
i) Jika menggunakan LateX, silakan menggunakan template conference IEEE yang dapat diunduh dari laman berikut: https://www.ieee.org/conferences/publishing/templates

Nilai bonus 5 jika membuat video makalah di Youtube

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.

Supaya memastikan tidak ada 1 judul diambil oleh lebih dari 1 mahasiswa, mahasiswa diharuskan menuliskan dulu usulan judul/topiknya ke sebuah *spreadsheet* yang bisa diakses semua sebagai berikut:
https://docs.google.com/spreadsheets/d/15qczQSBEgiicGLTu7bux5ytdzIKPEXfUcUJYpdiH2Dg/edit?usp=sharing

Batas waktu pengisian judul/topik makalah adalah 20 Desember 2025 pukul 23.59 WIB

Makalah dikumpulkan paling lambat tanggal 24 Desember 2025 dalam format PDF ke Google Drive berikut:

https://drive.google.com/drive/folders/1KwSS7gbko3Lz1z8FUK7O12jKUBDFdbim?usp=drive_link