Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas Makalah
II4021 Kriptografi, Semester II Tahun 2025/2026

Mahasiswa tidak hanya mampu membangun program aplikasi kriptografi, tetapi juga diharapkan mampu menulis karya ilmiah. Dengan membuat tulisan, maka berbagai pemikiran, karya, maupun, penelitian dalam bidang kriptogafi dapat dikomunikasikan ke tengah masyarakat. Salah satu mata kuliah pilihan pada Program Studi Sistem dan Teknologi Informasi adalah **II4021 Kriptografi.** Mahasiswa yang mengambil mata kuliah II4021 diwajibkan menulis sebuah makalah ilmiah dan video makalah dengan memilih salah satu topik di dalam kriptografi (lihat penjelasan tugas di bawah ini). Dengan menulis makalah maka kita telah ikut mendokumentasikan pengetahuan dan berbagi ilmu dengan orang lain.

Bonus: Video makalah. Video memberikan gambarkan tentang persoalan yang diangkat dan solusinya. Video diunggah ke YouTube.

Tujuan penulisan makalah:
1. Memotivasi mahasiswa agar memiliki kemampuan menulis untuk menuangkan ide-ide atau hasil risetnya;
2. Melakukan eksplorasi terhadap isu, metode, dan masalah yang dipelajari dalam pengembangan serta menyebarkan aplikasi yang mendukung teknologi informasi;
3. Sebagai media untuk berbagi informasi hasil-hasil pemikiran dan penelitian. Semua makalah mahasiswa akan dimuat di dalam *website* dosen, sehingga siapa pun dapat melihat dan membaca karya ilmiah tersebut.

Tujuan membuat video (bonus):
1. Memotivasi mahasiswa agar dapat menyajikan hasil riset mandirinya dalam bentuk multimedia (audio visual) yang menarik dan mudah dimengerti oleh pembelajar lainnya.
2. Berbagi pengetahuan lewat video publik.

Buatlah makalah yang berisi *technical report* yang berkaitan dengan salah satu dari topik kriptografi dan koding yang sudah anda pelajari, namun tidak dibatasi pada topik tsb itu saja, yaitu.

1. Kriptografi klasik
2. Kriptografi modern
3. Block cipher dan stream cipher
4. Steganografi dan watermarking
5. Kriptografi nirsimetri (kunci-publik)
6. *Elliptic Curve Cryptography*
7. Fungsi *hash*
8. Tanda-tangan digital
9. *MAC*
10. Sertifikat digital

11. Infrastruktur kunci-publik (PKI)
12. Protokol kriptografi dan SSL
13. Blockchain
14. Enkripsi homomorfik
15. Kriptografi visual
16. Pembangkit bilangan acak
17. Skema pembagian data rahasia

Kata penting di dalam makalah ini adalah: **kontribusi**. Makalah anda harus mengandung kontribusi yang merupakan rancangan, implementasi dan eksperimen terkait topik masalah kriptografi yang anda pilih. Makalah bukan suatu studi literatur atau kompilasi berbagai referensi.

Makalah dapat berupa:

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

Naskah ditulis dalam Bahasa Indonesia atau bahasa Inggris dengan susunan penulisan yang terdiri dari: judul, nama penulis dan instansi, abstrak (maksimal 200 kata), kata kunci, isi makalah, apendiks (jika ada), dan daftar pustaka.

Naskah ditulis pada kertas berukuran A4 dengan format terlampir. *Template* makalah 2025 dan tugas makalah ini dapat diunduh dari laman website Kriptografi.

Ketentuan teknis makalah adalah mengikuti format IEEE sebagai 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

Makalah tidak boleh sama dengan makalah yang sudah dibuat pada tahun-tahun sebelumnya pada kelas Kriptografi. Makalah tidak boleh berupa saduran, terjemahan, atau plagiasi dari makalah orang lain. Pada bagian akhir makalah (setelah daftar referensi harus ada pernyataan bahwa makalah bukan plagiasi dan ditandatangani dengan Microsoft Paint).

Pranala video di Youtube harus dituliskan di dalam makalah (lihat template).

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/1U997w6dNvyu4tKlUB_EJxgfXlvlQpkSNe-XV5TlfR_Y/edit?gid=0#gid=0

Batas waktu pengisian judul/topik makalah adalah 13 Juni 2026 pukul 23.59 WIB

Makalah dikumpulkan paling lambat tanggal 19 Juni 2026 pukul 23.59 dalam format PDF ke Google Drive berikut:
https://drive.google.com/drive/u/1/folders/1umyqejWGaFnqXsnsM4hzxMFHXsQwou71

Lain-lain

a. Jangan menjadikan Wikipedia sebagai salah satu daftar referensi . Boleh menjadikan Wikipedia sebagai bahan bacaan awal, tetapi gunakan referensi yang terdapat di laman Wikipedia tersebut sebagai daftar referensi.
b. Semua gambar, tabel, diagram, dan lain-lain yang diambil dari karya orang lain dan dipakai di dalam makalah harus disebutakn sumbernya.
c. Jangan sekali-kali melakukan *copas* meskipun terjemahan, tulislah kembali dalam gaya bahasa anda sendiri dan sebutkan sumbernya (jika dikutip seluruhnya).
d. Setiap makalah diberi tanda tangan (*digitized signature*) pada akhir makalah (setelah pernyataan).
e. Jangan mengakali jumlah halaman dengan memuat banyak gambar.