

SILABUS MATA KULIAH

MATA KULIAH	Nama MK : Kriptografi
	Kode MK : ET234501
	Kredit : 3 SKS
	Semester : 5

DESKRIPSI MATA KULIAH

Pada mata kuliah ini, mahasiswa mempelajari dan mengimplementasikan cara mengamankan dan menyembunyikan pesan (dalam bentuk data digital) melalui cabang ilmu kriptografi dan steganografi.

CAPAIAN PEMBELAJARAN LULUSAN YANG DIBEBANKAN MATA KULIAH

- CPL-4 : Mampu mengimplementasikan, mengelola, dan mengamankan informasi yang didistribusikan melalui jaringan komputer untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi.
- CPL-6 : Mampu merancang, mengintegrasikan, dan mengelola platform atau komponen perangkat keras maupun perangkat lunak menggunakan pemrograman integratif dan *big data* untuk mendukung aplikasi dan basis data berbasis jaringan.

CAPAIAN PEMBELAJARAN MATA KULIAH

- CPMK-1 : Mahasiswa mampu memahami cabang ilmu kriptografi dan kriptanalisis, serangan terhadap layanan kriptografi serta kriptografi klasik.
- CPMK-2 : Mahasiswa mampu memahami dan mengimplementasikan kriptografi modern, *stream-chiper* dan *block-chiper*, serta kriptografi kunci publik.
- CPMK-3 : Mahasiswa mampu memahami dan mengimplementasikan pembangkit bilangan acak, Fungsi *Hash* satu arah dan digital *signature*.
- CPMK-4 : Mahasiswa mampu memahami dan mengimplementasikan protokol komunikasi kriptografi, *key management* dan steganografi.

POKOK BAHASAN

1. Pengantar Kriptografi
2. Serangan dan Keamanan Algoritma
3. Metode Enkripsi Sederhana
4. Algoritma *Stream-Chiper* dan *Block-Chiper*

5. Kriptografi Kunci Publik
6. Pembangkit Bilangan Acak
7. Fungsi Hash dan Penandatanganan (*Digital Signature*)
8. Protokol Komunikasi Aman
9. *Key Management*
10. Steganografi

PRASYARAT

-

PUSTAKA

- J. P. Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*, San Francisco: No Starch Press, Inc., 2017.