Departemen Matematika
Institut Teknologi Sepuluh Nopember
email : matematika@its.ac.id – web : https://www.its.ac.id/matematika

Mata Kuliah	**Nama Mata Kuliah**	**: Kriptografi**
	Kode Mata Kuliah	**: KM184830**
	Kredit	**: 2**
	Semester	**: 8**

Deskripsi Mata Kuliah	
Pada mata kuliah ini diberikan dasar-dasar yang terkait dengan kriptografi dan tanda tangan digital untuk pengaman data. Topik-topik yang akan dibahas meliputi dasar-dasar ilmu matematika, algoritma kriptografi klasik dan modern, teknik-teknik kritografi dan aplikasi dari kriptografi. Sistem pengajaran yang dilakukan meliputi tutorial, responsi dan praktikum yang terjadwal	
Capaian Pembelajaran Lulusan yang Dibebankan Mata Kuliah	
CPL 3	[C4] Mahasiswa mampu menganalisis permasalahan sederhana dan praktis pada salah satu bidang analisis, aljabar, pemodelan, optimasi sistem dan ilmu komputasi
CPL 4	[C5] Mahasiswa mampu mengerjakan tugas ilmiah yang terdefinisi secara jelas dan mampu menjelaskan hasilnya secara lisan dan tulisan, pada bidang matematika murni atau terapan atau ilmu komputasi
CPL 7	Mahasiswa mampu menunjukkan sikap bertanggung jawab dan berkomitmen terhadap penegakan hukum, etika, norma untuk kehidupan bermasyarakat dan kelestarian lingkungan
Capaian Pembelajaran Mata Kuliah	
Mahasiswa mampu mengembangkan pemahaman konsep dan prosedur dari teknik – teknik pengamanan pada komputer, khususnya pengamanan data dan	

informasi, baik dengan kinerja individu maupun secara berkelompok dalam kerjasama tim.
Pokok Bahasan
PENGENALAN KRIPTOGRAFI : pengenalan dasar kriptografi, data sekuriti, teori informasi, kompleksitas dan bilangan BEBERAPA ALGORITMA ENKRIPSI : algorithma enkripsi klasik dan modern (DES dan algoritma kunci public) TEKNIK KRIPTOGRAFI : beberapa teknik kriptografi, manajemen kunci
Prasyarat
Pustaka
1. William.Stallings, Cryptography and Network Security, Principle and Practise. 2nd ed., Prentice Hall, 1999 2. Douglas R. Stinson, "Cryptography Theory and Practice", 3rd Edition, Chapman & Hall/CRC, 2006
Pustaka Pendukung
1. Serge Vaudenay, "A Classical Introduction to Modern Cryptography', Springer, 2006 2. Rinaldi Munir "Kriptografi", Informatika Bandung