	Universitas Negeri Surabaya **S1 Matematika**	**Kode Dokumen**

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)	SEMESTER	Tgl Penyusunan
Pengantar Kriptografi	4420102097		**2**		25 Agustus 2026

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
			RADEN SULAIMAN

Deskripsi Singkat MK	Matakuliah ini mengkaji tentang sejarah dan konsep dasar kriptografi, sistemkripto simetris dan asimetris. Sistemkripto simetris yang dibahas adalah: Caesar chipper, Monoalphabetic, Vigenere, One Time Pad, Palyfair, ADFGVX, dan cipher Affine. Sedangkan Sistemkripto asimetris yang dibahas adalah RSA.

Capaian Pembelajaran (CP)

CPL-PRODI yang dibebankan pada MK

CPL	Mengembangkan pemikiran logis, kritis, sistematis, dan kreatif dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan
CPL	Mampu bekerja sama dan memiliki kepekaan sosial serta mampu membawa perubahan terhadap masyarakat yang techno- ecopreneurship;
CPL	Mampu merumuskan dan menyelesaikan masalah matematika fundamental;
CPL	Mampu menerapkan prinsip dasar matematika untuk menyelesaikan masalah matematika sederhana*

Capaian Pembelajaran Mata Kuliah (CPMK)

CPMK-1	Bertanggung jawab dalam menyelesaikan tugas sesuai waktu yang ditentukan
CPMK-2	Mengembangkan chiper baru dengan menggunakan konsep matematika
CPMK-3	Menyampaikan ide secara tertulis dan oral terkait inovasi penyusunan chiper
CPMK-4	Menerapkan konsep bilangan dalam pemecahan masalah
CPMK-5	Memahami konsep matematika terkait dengan teori bilangan

Matrik CPL - CPMK

CPMK	CPL	CPL	CPL	CPL
CPMK-1	✔			
CPMK-2	✔			
CPMK-3		✔		
CPMK-4			✔	
CPMK-5				✔

Matrik CPMK pada Kemampuan akhir tiap tahapan belajar (Sub-CPMK)

CPMK	Minggu Ke															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CPMK-1				✔												
CPMK-2																✔
CPMK-3		✔						✔				✔				
CPMK-4	✔															
CPMK-5					✔											

Pustaka

Utama :

1. Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag
2. Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag
3. Paul Garret. 2001. An introduction to Cryptology. New York: Printice Hall
4. Simon Singh. 2004. Code Book

Pendukung :

Mg Ke-	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [Estimasi Waktu]		Materi Pembelajaran	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk	Luring (*offline*)	*Daring (online)*		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Memahami konsep matematika terkait dengan teori bilangan	1. • Menjelaskan pengertian kriptosistem 2. Melakukan enkripsi dan dekripsi pada contoh sederhana		Pendekatan Pembelajaran Kolaboratif (Ceramah, diskusi, dan tanya jawab)			5%
2	• Menentukan cipher text	1. • Menentukan cipher text 2. • Melakukan dekripsi dengan Caesar wheel					20%
4	Mengaplikasikan konsep teori bilangan dalam mendekripsi pesan	• Mendekeripsi pesan dengan menggunakan: Caesar cipher dan Mono Alphabetic					10%
5	Mengaplikasikan konsep teori bilangan dalam melakukan encripsi dan decripsi pesan	1. • Mengenkrisi pesan dengan Vigenere cipher 2. Mengenkrisi pesan dengan One Time Pad cipher					20%
8							10%
12	Berbagi ide dan gagasan dalam kelompok	Mampu mengembangkan chiper baru					5%
16		Melaporkan hasil kerja projek					30%
3							
6							
7							
9							
10							

11							
13							
14							
15							

Catatan

1. **Capaian Pembelajaran Lulusan Program Studi (CPL-Prodi)** adalah rumusan kemampuan yang harus dimiliki oleh lulusan program studi yang mencakup sikap, penguasaan pengetahuan, keterampilan umum, dan keterampilan khusus sesuai dengan jenjang kualifikasi, yang diperoleh melalui proses pembelajaran.
2. **CPL-Prodi yang dibebankan pada Mata Kuliah** adalah bagian dari CPL-Prodi yang dipilih dan relevan untuk dikembangkan melalui suatu mata kuliah, sebagai dasar perumusan capaian pembelajaran mata kuliah.
3. **Capaian Pembelajaran Mata Kuliah (CPMK)** adalah kemampuan yang dirumuskan secara spesifik dan diturunkan dari CPL-Prodi yang dibebankan pada mata kuliah, serta menggambarkan kompetensi yang harus dicapai mahasiswa setelah menyelesaikan mata kuliah.
4. **Sub-CPMK** adalah kemampuan akhir yang direncanakan pada setiap tahap pembelajaran, sebagai penjabaran lebih rinci dari CPMK, bersifat terukur dan dapat diamati sesuai dengan materi pembelajaran.
5. **Indikator Penilaian** adalah pernyataan spesifik dan terukur yang digunakan untuk menilai ketercapaian Sub-CPMK, baik dari proses maupun hasil belajar mahasiswa, yang didukung dengan bukti penilaian.
6. **Kriteria Penilaian** adalah tolok ukur yang digunakan untuk menentukan tingkat ketercapaian hasil belajar mahasiswa berdasarkan indikator penilaian, guna menjamin penilaian yang objektif, konsisten, dan adil. Kriteria penilaian dapat bersifat kuantitatif dan/atau kualitatif.
7. **Bentuk Penilaian** meliputi penilaian tes dan non-tes sesuai dengan karakteristik capaian pembelajaran.
8. **Bentuk Pembelajaran** meliputi kuliah, responsi, tutorial, seminar atau bentuk lain yang setara, praktikum, praktik studio, praktik bengkel, praktik lapangan, penelitian, dan pengabdian kepada masyarakat.
9. **Metode Pembelajaran** merupakan cara penyampaian pembelajaran yang digunakan untuk mencapai capaian pembelajaran, antara lain Small Group Discussion, Project Based Learning, Case Based Learning, Collaborative Learning, Discovery Learning, Self-Directed Learning, serta metode lain yang relevan.
10. **Materi Pembelajaran** adalah bahan kajian yang disusun secara sistematis dalam bentuk pokok dan sub-pokok bahasan untuk mendukung pencapaian Sub-CPMK.
11. **Bobot Penilaian** adalah persentase kontribusi setiap komponen penilaian terhadap nilai akhir mata kuliah, yang ditetapkan secara proporsional sesuai tingkat kompleksitas dan ketercapaian Sub-CPMK, dengan total keseluruhan sebesar 100%.
12. TM = Tatap Muka, PT = Penugasan Terstruktur, BM = Belajar Mandiri.