	Universitas Negeri Surabaya Fakultas Matematika dan Ilmu Pengetahuan Alam Program Studi S1 Matematika	Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)			SEMESTER	Tgl Penyusunan
Pengantar Kriptografi	4420102097	Aljabar	T=2	P=0	ECTS=3.18	5	26 April 2023

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
	R. Sulaiman	.....	Prof. Dr. Raden Sulaiman, M.Si.

Model Pembelajaran	**Project Based Learning**	
Capaian Pembelajaran (CP)	**CPL-PRODI yang dibebankan pada MK**	
	CPL-3	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-5	Mampu bekerja sama dan memiliki kepekaan sosial serta mampu membawa perubahan terhadap masyarakat yang techno- ecopreneurship;
	CPL-6	Mampu merumuskan dan menyelesaikan masalah matematika fundamental;
	CPL-7	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	Menerapkan konsep bilangan dalam pemecahan masalah
	CPMK - 3	Menyampaikan ide secara tertulis dan oral terkait inovasi penyusunan chiper
	CPMK - 4	Memahami konsep matematika terkait dengan teori bilangan
	Matrik CPL - CPMK	

CPMK	CPL-3	CPL-5	CPL-6	CPL-7
CPMK-1	✔	✔		
CPMK-2			✔	
CPMK-3		✔		
CPMK-4				✔

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																

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.	
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 :	
Dosen Pengampu	Prof. Dr. Raden Sulaiman, M.Si.	

Mg Ke-	**Kemampuan akhir tiap tahapan belajar (Sub-CPMK)**	**Penilaian**		**Bantuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [Estimasi Waktu]**		**Materi Pembelajaran [Pustaka]**	**Bobot Penilaian (%)**
		Indikator	**Kriteria & Bentuk**	**Luring (*offline*)**	**Daring (*online*)**		
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
1	1.Memahami konsep matematika terkait dengan teori bilangan 2.1. Menjelaskan pengertian kriptosistem 3.2. Menjelaskan pengertian enkripsi 4.3. Menjelaskan pengertian dekripsi 5.4. Menjelaskan pengertian plaintext 6.5. Menjelaskan pengertian ciphertext	1.• Menjelaskan pengertian kriptosistem 2.Melakukan enkripsi dan dekripsi pada contoh sederhana	**Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan Pembelajaran Kolaboratif (Ceramah, diskusi, dan tanya jawab) 100	Secara daring mahasiswa melakukan enkripsi dan dekripsi sederhana		10%
2	1.• Menentukan cipher text 2.• Melakukan dekripsi dengan Caesar wheel	1.• Menentukan cipher text 2.• Melakukan dekripsi dengan Caesar wheel			Secara daring, Membuat Caesar Wheel dan menggunakannya; Menggunakan software	**Materi:** Caesar Cipher **Pustaka:**	10%
3	Memahmi matematika terkait dengan keterbagian bilangan	1.• Mendekripsi pesan teks bahasa inggris 2.• Mendekripsi pesan bahasa Indonesia			Pembelajaran dilaksanakan secara daring; Mahasiswa melakukan survey penggunaan abjad dalam teks Bahasa Inggris dan Bahasa Indonesia	**Materi:** Mono Alphabetic **Pustaka:** *Simon Singh. 2004. Code Book*	0%
4	Mengaplikasikan konsep teori bilangan dalam mendekripsi pesan	• Mendekeripsi pesan dengan menggunakan: Caesar cipher dan Mono Alphabetic			Pembelajaran dilakaukan secara daring; melakukan Praktek “Crack code” dengan Caesar Ciper dan Mono Alphabetic	**Materi:** Caesar dan Mono Alphabetic **Pustaka:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%
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			Pembelajaran dilakukan secara daring . Mahasiswa melakukan enkripsi dan dekripsi.	**Materi:** 3. Vigenere 4. One Time Pad **Pustaka:** *Simon Singh. 2004. Code Book*	0%
6	Mengaplikasikan konsep teori bilangan dalam melakukan encripsi dan decripsi pesan	1.• Mengenkrisi pesan dengan Vigenere cipher 2.Mengenkrisi pesan dengan One Time Pad cipher	**Bentuk Penilaian** : Aktifitas Partisipasif		Pembelajaran dilakukan secara daring. Mahasiswa melakukan enkripsi dan dekripsi	**Materi:** One Time Pad **Pustaka:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%

7	Mengaplikasikan konsep teori bilangan dalam melakukan encripsi dan decripsi pesan	1.• Mendekripsi pesan dengan menggunakan Caesar Cipher 2.Mendekripsi pesan dengan menggunakan Mono Alphabetic 3.Mendekripsi pesan dengan menggunakan Vigenere dan One Time pad	**Bentuk Penilaian** : Aktifitas Partisipasif		Pembelajaran dlaksanakan secara daring. Mendiskusikan dan mempraktekkan "Crack code" dengan Caesar Ciper, Mono Alphabetic, Vigenere dan One Time pad	**Materi:** Caesar Cipher, Mono Alphabetic, Vigenere dan One Time pad **Pustaka:**	0%
8					UTS		0%
9	Mampu mengkomunikasikan ide secara oral	• Mengenkrisi dan mendekripsi pesan dengan ADFGVX cipher	**Bentuk Penilaian** : Aktifitas Partisipasif		Pembelajaran dilaksanakan secara daring. Mendiskusikan ADFGVX cipher	**Materi:** ADFGVX cipher **Pustaka:** *Paul Garret. 2001. An introduction to Cryptology. New York: Printice Hall*	0%
10	Bekerja sama dalam kelompok untuk berbagi ide dan gagasan baru membuat chiper		**Bentuk Penilaian** : Aktifitas Partisipasif		Pembelajaran secara daring. Mendiskusikan : • ECB mode • CBC mode • CFB mode • OFB mode	**Materi:** • ECB mode • CBC mode • CFB mode • OFB mode **Pustaka:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%
11	Bekerja sama dalam kelompok untuk berbagi ide dan gagasan baru membuat chiper	Mampu mengembangkan chiper baru	**Bentuk Penilaian** : Aktifitas Partisipasif		Pembelajaran secara daring. Mendiskusikan : • ECB mode • CBC mode • CFB mode • OFB mode	**Materi:** • ECB mode • CBC mode • CFB mode • OFB mode **Pustaka:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%
12	Berbagi ide dan gagasan dalam kelompok	Mampu mengembangkan chiper baru	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk		mendiskusikan secara kelompok tugas Projek, mengembangngkan Cipher baru berdasarkan beberapa Chiper yang sudah dikenal mahasiswa. Tugas projek ini diselesaikan dalam waktu 3 pekan (pekan ke 10-12). Pekan ke 13-15 Mahasiswa mempresentasikan hasil projeknya secara bergantian.	**Materi:** KOnstruksi chiper baru **Pustaka:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%

13	Mendiskusikan dise dan berkomunikasi dalam kelompok	Mampu mengembangkan chiper baru	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk		mendiskusikan secara kelompok tugas Projek, mengembangngkan Cipher baru berdasarkan beberapa Chiper yang sudah dikenal mahasiswa. Tugas projek ini diselesaikan dalam waktu 3 pekan (pekan ke 10-12). Pekan ke 13-15 Mahasiswa mempresentasikan hasil projeknya secara bergantian.	**Materi:** Konstruksi chiper baru **Pustaka:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%
14	Berdiskusi dalm mengembangkan chiper baru	Mampu mengkomunikasikan ide dan gagasan	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk, Praktik / Unjuk Kerja		Secara daring mahasiswa mempresentasika hasil projek mengembangngkan Cipher baru berdasarkan beberapa Chiper yang sudah dikenal mahasiswa.	**Materi:** Presentasi **Pustaka:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%
15	Mengkomunikasikan secara tulis dan oral tentang chiper `baru	Mampu mengkomunikasikan ide dan gagasan	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk		Secara daring mahasiswa mempresentasika hasil projek mengembangngkan Cipher baru berdasarkan beberapa Chiper yang sudah dikenal mahasiswa.	**Materi:** Presentasi **Pustaka:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%
16		Melaporkan hasil kerja projek	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk		Finalisasi hasil laporan Projek	**Materi:** Penyusunan laporan **Pustaka:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%

Rekap Persentase Evaluasi : Project Based Learning

No	Evaluasi	Persentase
1.	Aktifitas Partisipasif	10%
		10%

Catatan

1. **Capaian Pembelajaran Lulusan Prodi (CPL - Prodi)** adalah kemampuan yang dimiliki oleh setiap lulusan prodi yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. **CPL yang dibebankan pada mata kuliah** adalah beberapa capaian pembelajaran lulusan program studi (CPL-Prodi) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampulan umum, ketrampilan khusus dan pengetahuan.
3. **CP Mata kuliah (CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. **Sub-CPMK Mata kuliah (Sub-CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
5. **Indikator penilaian** kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
6. **Kreteria Penilaian** adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
7. **Bentuk penilaian:** tes dan non-tes.
8. **Bentuk pembelajaran:** Kuliah, Responsi, Tutorial, Seminar atau yang setara, Praktikum, Praktik Studio, Praktik Bengkel, Praktik Lapangan, Penelitian, Pengabdian Kepada Masyarakat dan/atau bentuk pembelajaran lain yang setara.

9. **Metode Pembelajaran:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, dan metode lainnya yg setara.
10. **Materi Pembelajaran** adalah rincian atau uraian dari bahan kajian yg dapat disajikan dalam bentuk beberapa pokok dan sub-pokok bahasan.
11. **Bobot penilaian** adalah prosentasi penilaian terhadap setiap pencapaian sub-CPMK yang besarnya proposional dengan tingkat kesulitan pencapaian sub-CPMK tsb., dan totalnya 100%.
12. TM=Tatap Muka, PT=Penugasan terstruktur, BM=Belajar mandiri.