



UNIVERSITAS ISLAM NEGERI SUNAN GUNUNG DJATI BANDUNG

FAKULTAS SAINS DAN TEKNOLOGI

JURUSAN KIMIA

RPS-  
MA215A06

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH	KODE	Rumpun MK	Bobot (sks)		Semester	Tgl Penyusunan
Kriptografi		Pilihan	T = 3 SKS	P = 0 SKS	7	06 Desember 2022
OTORISASI/PENGESAHAN	Dosen Pengembang RPS		Koordinator RMK		Ketua Jurusan	
	Salwa Nursyahida, S.Pd.,M.Si.				Asep Sholih Awalluddin, M.Si.	

Capaian Pembelajaran	CPL Prodi yang dibebankan pada MK	
	CPL 1 (S4)	Memiliki semangat kemandirian dan gotong-royong, bertanggung jawab dan jujur, serta memiliki daya juang dan kewirausahaan dalam menekuni keahlian dan berkontribusi di masyarakat.
	CPL 2 (KU-1)	Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi yang sesuai dengan bidang matematika dan penerapannya.
	CPL 3 (KU-3)	Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah berdasarkan literatur dan hasil analisis data secara ilmiah.
	CPL 4 (KK-1)	Mampu menggunakan serta mengembangkan pemikiran matematis untuk mempelajari, mengidentifikasi, mengeksplorasi dan menganalisis permasalahan matematika dan penerapannya secara objektif dan logis.
	CPL 5 (KK-4)	Mampu memanfaatkan berbagai alternatif pemecahan masalah matematis yang telah tersedia baik secara mandiri maupun kelompok untuk pengambilan keputusan yang tepat
	CPL 6 (P-4)	Menguasai secara teoretis atau penerapan matematika sesuai dengan peminatan bidang keahlian meliputi matematika murni, pemodelan matematika, matematika keuangan dan industri, statistika dan aktuaria, dan matematika komputasi.
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK 1	Mahasiswa mampu menggunakan landasan matematika yang diperlukan untuk kriptografi
	CPMK 2	Mahasiswa mampu menjelaskan prinsip kriptografi klasik beserta beberapa algoritma-algoritmanya
	CPMK 3	Mahasiswa mampu menjelaskan jenis-jenis serangan terhadap kriptografi dan kriptanalisis sederhana
	CPMK 4	Mahasiswa mampu menjelaskan prinsip kriptografi kunci modern beserta beberapa algoritma-algoritmanya
	CPMK 5	Mahasiswa mampu menjelaskan prinsip kriptografi kunci public beserta beberapa algoritma-algoritmanya
	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)	

	Sub-CPMK1	Mahasiswa mampu menjelaskan pengertian kriptografi, sejarah kriptografi, prinsip-prinsip kerahasiaan dalam kriptografi
	Sub-CPMK2	Mahasiswa mampu menggunakan konsep-konsep teori bilangan: modulo, inversi modulo; kombinatorika, aljabar linier: matriks, invers matriks.
	Sub-CPMK3	Mahasiswa mampu menjelaskan prinsip-prinsip dan metode dalam kriptografi klasik
	Sub-CPMK4	Mahasiswa mampu menggunakan algoritma-algoritma dalam kriptografi klasik untuk mengenkripsi dan dekripsi pesan
	Sub-CPMK5	Mahasiswa mampu menjelaskan prinsip-prinsip serangan terhadap kriptografi
	Sub-CPMK6	Mahasiswa mampu melakukan kriptanalisis sederhana
	Sub-CPMK7	Mahasiswa mampu menjelaskan prinsip-prinsip dan metode dalam kriptografi modern
	Sub-CPMK8	Mahasiswa mampu menjelaskan skema dan prinsip yang digunakan dalam stream cipher
	Sub-CPMK9	Mahasiswa mampu menjelaskan skema dan prinsip yang digunakan dalam block cipher
	Sub-CPMK10	Mahasiswa mampu menggunakan algoritma-algoritma dalam blok cipher untuk mengenkripsi dan dekripsi pesan
	Sub-CPMK11	Mahasiswa mampu menghitung eksponen modulo dengan berbagai teknik matematika
	Sub-CPMK12	Mahasiswa mampu menjelaskan prinsip-prinsip dan metode dalam kriptografi kunci publik
	Sub-CPMK13	Mahasiswa mampu menggunakan algoritma-algoritma dalam kriptografi kunci publik untuk mengenkripsi dan dekripsi pesan
<b>Deskripsi Singkat</b>	Mata kuliah ini membahas tentang pengantar kriptografi dan matematika kriptografi. Kriptografi digunakan untuk merahasiakan sebuah pesan baik berupa teks, gambar, audio, dan lain sebagainya. Mata kuliah ini mempelajari prinsip-prinsip yang digunakan dalam kriptografi seperti kriptografi klasik, modern dan kunci public, juga membahas tentang konsep matematika yang dibutuhkan untuk menggunakan sebuah algoritma kriptografi.	
<b>Bahan Kajian :</b> Materi Pembelajaran	<ol style="list-style-type: none"> <li>1 Landasan Matematika</li> <li>2 Kriptografi Klasik</li> <li>3 Serangan terhadap Kriptografi dan Kriptanalisis Sederhana</li> <li>4 Kriptografi Modern</li> <li>5 Kriptografi Kunci Publik</li> </ol>	
<b>Pustaka</b>	<b>Utama :</b>	<ol style="list-style-type: none"> <li>1 Rinaldi Munir. 2019. Kriptografi. Bandung: Penerbit Informatika.</li> </ol>

**Pendukung :**

2 Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. 2008. An Introduction to Mathematical Cryptography. Springer.

**Dosen Pengampu****Mata Kuliah Syarat** Matematika Diskrit, Aljabar Linear Elementer

Minggu Ke -	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; [estimasi waktu]		Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
		Indikator	Kriteria & Teknik	Luring (5)	Daring (6)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Mahasiswa mampu menjelaskan pengertian kriptografi, sejarah kriptografi, prinsip-prinsip kerahasiaan dalam kriptografi	Ketepatan dalam menjelaskan pengertian kriptografi, sejarah kriptografi, prinsip-prinsip kerahasiaan dalam kriptografi	Rubrik holistik	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Pengantar Kriptografi [1]	7%
2	Mahasiswa mampu menggunakan konsep-konsep teori bilangan: modulo, inversi modulo; kombinatorika, aljabar linier: matriks, invers matriks.	-Ketepatan dalam menggunakan konsep-konsep teori bilangan: modulo, inversi modulo; kombinatorika, aljabar linier: matriks, invers matriks	Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Landasan Matematika untuk Kriptografi[1] [2]	8%
3	Mahasiswa mampu menggunakan konsep-konsep teori bilangan: modulo, inversi modulo; kombinatorika, aljabar linier: matriks, invers matriks.	Ketepatan dalam menggunakan konsep-konsep teori bilangan: modulo, inversi modulo; kombinatorika, aljabar linier: matriks, invers matriks	Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Landasan Matematika untuk Kriptografi[1] [2]	7%
4	Mahasiswa mampu menjelaskan prinsip-prinsip dan metode dalam kriptografi klasik	Ketepatan dalam menjelaskan prinsip-prinsip dan metode dalam kriptografi klasik	Rubrik Holistik	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Klasik[1]	8%

5	Mahasiswa mampu menggunakan algoritma-algoritma dalam kriptografi klasik untuk mengenkripsi dan dekripsi pesan	Ketepatan dalam menggunakan algoritma-algoritma dalam kriptografi klasik untuk mengenkripsi dan dekripsi pesan	Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Klasik [1]	7%
6	Mahasiswa mampu menggunakan algoritma-algoritma dalam kriptografi klasik untuk mengenkripsi dan dekripsi pesan	Ketepatan dalam menggunakan algoritma-algoritma dalam kriptografi klasik untuk mengenkripsi dan dekripsi pesan	Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Klasik	8%
7	Mahasiswa mampu menjelaskan prinsip-prinsip serangan terhadap kriptografi  Mahasiswa mampu melakukan kriptanalisis sederhana	Ketepatan dalam menjelaskan prinsip-prinsip serangan terhadap kriptografi  Ketepatan dalam melakukan kriptanalisis sederhana	Rubrik Holistik  Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Serangan terhadap Kriptografi [1]	5%
8	<b>UTS</b>						
9	Mahasiswa mampu menjelaskan prinsip-prinsip dan metode dalam kriptografi modern	Ketepatan dalam menjelaskan prinsip-prinsip dan metode dalam kriptografi modern	Rubrik Holistik	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Modern [1]	7%
10	Mahasiswa mampu menjelaskan skema dan prinsip yang digunakan dalam stream cipher	- Ketepatan dalam menjelaskan skema dan prinsip yang digunakan dalam stream cipher	Rubrik Holistik	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Modern[1]	8%
11	Mahasiswa mampu menjelaskan skema dan prinsip yang digunakan	Ketepatan dalam menjelaskan skema dan prinsip yang digunakan	Rubrik Holistik	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Modern[1]	7%

	dalam block cipher	dalam block cipher					
<b>12</b>	Mahasiswa mampu menggunakan algoritma-algoritma dalam blok cipher untuk mengenkripsi dan dekripsi pesan	Ketepatan dalam menggunakan algoritma-algoritma dalam blok cipher untuk mengenkripsi dan dekripsi pesan	Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Modern[1]	8%
<b>13</b>	Mahasiswa mampu menghitung eksponen modulo dengan berbagai teknik matematika	Ketepatan dalam menghitung eksponen modulo dengan berbagai teknik matematika	Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Landasan Matematika[1] [2]	7%
<b>14</b>	Mahasiswa mampu menjelaskan prinsip-prinsip dan metode dalam kriptografi kunci publik	Ketepatan dalam menjelaskan prinsip-prinsip dan metode dalam kriptografi kunci publik	Rubrik Holistik	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Kunci Publik[1]	8%
<b>15</b>	Mahasiswa mampu menggunakan algoritma-algoritma dalam kriptografi kunci public untuk mengenkripsi dan dekripsi pesan	- Ketepatan dalam menggunakan algoritma-algoritma dalam kriptografi kunci public untuk mengenkripsi dan dekripsi pesan	Latihan Soal	Ceramah, diskusi 3 x 50'	Kuliah online, video youtube 3x50'	Kriptografi Kunci Publik[1]	5%
<b>16</b>	<b>UAS</b>						