



Universitas Negeri Surabaya
S2 Informatika

Kode
Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)		KODE	Rumpun MK		BOBOT (sks)		SEMESTER	Tgl Penyusunan
Keamanan Jaringan dan Kriptografi		5510003013			3			25 Agustus 2026
OTORISASI		Pengembang RPS		Koordinator RMK		Koordinator Program Studi		
				Dr. Ir. Ricky Eka Putra, S.Kom., M.Kom.		RICKY EKA PUTRA		
Deskripsi Singkat MK		Matakuliah Keamanan Jaringan dan Kriptografi pada jenjang S2 program studi Informatika bertujuan untuk memberikan pemahaman mendalam dan terintegrasi tentang konsep, teknik, dan implementasi keamanan jaringan serta kriptografi. Mahasiswa akan mempelajari teknik-teknik perlindungan jaringan komputer, analisis risiko, protokol keamanan, serta implementasi enkripsi dan dekripsi untuk melindungi informasi dalam sistem komputer. Selain itu, mata kuliah ini juga mencakup pembahasan tentang pengembangan strategi keamanan berbasis teknologi terbaru dan penerapan kriptografi dalam berbagai konteks industri dan penelitian. Dengan memadukan teori dan praktik, mata kuliah ini mendukung pengembangan kemampuan analitis dan inovatif mahasiswa dalam menyelesaikan tantangan keamanan di era transformasi digital.						
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 mengembangkan solusi informatika yang inovatif, efektif, efisien, aman, adaptif, dan berkelanjutan untuk meningkatkan kinerja organisasi, industri, pendidikan, atau masyarakat.					
		CPL	Mampu mengevaluasi kinerja sistem, teknologi, atau solusi informatika berdasarkan data, metrik, eksperimen, dan kebutuhan pengguna/organisasi untuk menghasilkan perbaikan berkelanjutan.					
		Capaian Pembelajaran Mata Kuliah (CPMK)						
		CPMK-1	Menerapkan dan mengintegrasikan solusi keamanan berlapis untuk melindungi infrastruktur TI dari serangan siber					
		CPMK-2	Mengembangkan solusi kriptografi yang inovatif untuk meningkatkan keamanan data dan transaksi dalam jaringan					
		CPMK-3	Menciptakan metode baru dalam deteksi dan pencegahan intrusi menggunakan teknologi terkini					
		CPMK-4	Menganalisis kebutuhan keamanan informasi organisasi dan merancang arsitektur jaringan yang sesuai untuk memenuhi kebutuhan tersebut					
		CPMK-5	Menganalisis dan mengevaluasi protokol keamanan untuk menentukan kekuatan dan kelemahan dalam konteks keamanan sistem informasi					
		CPMK-6	Mengevaluasi implementasi keamanan jaringan dalam studi kasus nyata untuk mengidentifikasi area perbaikan dan penerapan strategi keamanan yang lebih efektif					
		CPMK-7	Mengevaluasi efektivitas berbagai algoritma kriptografi dalam konteks kebutuhan spesifik organisasi dan membuat rekomendasi berdasarkan analisis tersebut					
		CPMK-8	Menganalisis dan merespon secara efektif terhadap insiden keamanan dengan menggunakan prinsip forensik digital					
		Matrik CPL - CPMK						

		<table><tr><td>CPMK</td><td colspan="4">CPL</td><td colspan="4">CPL</td><td colspan="4">CPL</td></tr><tr><td>CPMK-1</td><td colspan="4">✓</td><td colspan="4"></td><td colspan="4"></td></tr><tr><td>CPMK-2</td><td colspan="4"></td><td colspan="4">✓</td><td colspan="4"></td></tr><tr><td>CPMK-3</td><td colspan="4"></td><td colspan="4">✓</td><td colspan="4"></td></tr><tr><td>CPMK-4</td><td colspan="4"></td><td colspan="4">✓</td><td colspan="4"></td></tr><tr><td>CPMK-5</td><td colspan="4"></td><td colspan="4"></td><td colspan="4">✓</td></tr><tr><td>CPMK-6</td><td colspan="4"></td><td colspan="4"></td><td colspan="4">✓</td></tr><tr><td>CPMK-7</td><td colspan="4"></td><td colspan="4"></td><td colspan="4">✓</td></tr><tr><td>CPMK-8</td><td colspan="4"></td><td colspan="4"></td><td colspan="4">✓</td></tr></table>																CPMK	CPL				CPL				CPL				CPMK-1	✓												CPMK-2					✓								CPMK-3					✓								CPMK-4					✓								CPMK-5									✓				CPMK-6									✓				CPMK-7									✓				CPMK-8									✓																																																							
CPMK	CPL				CPL				CPL																																																																																																																																																																																	
CPMK-1	✓																																																																																																																																																																																									
CPMK-2					✓																																																																																																																																																																																					
CPMK-3					✓																																																																																																																																																																																					
CPMK-4					✓																																																																																																																																																																																					
CPMK-5									✓																																																																																																																																																																																	
CPMK-6									✓																																																																																																																																																																																	
CPMK-7									✓																																																																																																																																																																																	
CPMK-8									✓																																																																																																																																																																																	
Matrik CPMK pada Kemampuan akhir tiap tahapan belajar (Sub-CPMK)																																																																																																																																																																																										
		<table><tr><td rowspan="2">CPMK</td><td colspan="16">Minggu Ke</td></tr><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td></tr><tr><td>CPMK-1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>CPMK-2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>✓</td><td></td><td></td><td></td><td></td></tr><tr><td>CPMK-3</td><td></td><td></td><td></td><td></td><td></td><td></td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>CPMK-4</td><td></td><td></td><td></td><td></td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>CPMK-5</td><td></td><td></td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>CPMK-6</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>CPMK-7</td><td></td><td></td><td></td><td></td><td></td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>CPMK-8</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr></table>																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			✓														CPMK-6													✓	✓	✓	✓	CPMK-7						✓											CPMK-8											✓					
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			✓																																																																																																																																																																																							
CPMK-6													✓	✓	✓	✓																																																																																																																																																																										
CPMK-7						✓																																																																																																																																																																																				
CPMK-8											✓																																																																																																																																																																															
Pustaka	Utama :																																																																																																																																																																																									
			1. Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson. 2. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.																																																																																																																																																																																							
	Pendukung :																																																																																																																																																																																									
			1. As-sajid, A. B. N., dan Putra, R. E. (2023). Analisis Dan Pengujian Dictionary Attack Terhadap WPA3 Berbasis Script. Journal of Informatics and Computer. 2. Suartana, I. M., Putra, R. E., Bisma, R., dan Prapanca, A. (2022). Pengenalan pentingnya cyber security awareness pada UMKM. Jurnal Abadimas Adi. 3. Adlani, M. A., dan Putra, R. E. (2022). Pengamanan Mnemonic Phrase Menggunakan Modified Advanced Encryption Standard. Journal of Informatics and Computer. 4. Rakhmawati, L., Tjahyaningtijas, H. P. A., dan Yustanti, W. (2023). Double-encrypted Watermark Image in Dual Domain for Authentication and Recovery. Conference on Internet. 5. Putra, R. E., Suartana, I. M., dan Nerisafitra, P. (2024). Implementation of shallow neural network to intrusion detection system. AIP Conference Proceedings. 6. Rakhmawati, L., Tjahyaningtijas, H. P. A., dan Yustanti, W. (2022). Block-Based Image Reversible Data Hiding Based on Visual Feature and Edge Entropy. IEEE Conference on Electrical.																																																																																																																																																																																							
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)																																																																																																																																																																																			
3	Mahasiswa mampu mengevaluasi protokol keamanan jaringan untuk menentukan kelemahan dan kekuatannya	1. Ketepatan analisis protokol keamanan dilakukan dengan mendalam 2. Mampu mengidentifikasi kekuatan dan kelemahan protokol 3. Rekomendasi perbaikan disusun secara jelas	Kelengkapan evaluasi kelemahan dan kekuatan	Pembelajaran aktif melalui diskusi kelompok dan proyek serta Diskusi dan presentasi			5%																																																																																																																																																																																			
5	Mahasiswa mampu merancang arsitektur jaringan yang aman berdasarkan analisis kebutuhan keamanan informasi	1. Analisis implementasi keamanan jaringan 2. Identifikasi area perbaikan 3. Ketepatan perancangan strategi keamanan efektif 4. Ketepatan rancangan arsitektur jaringan.	Relevansi rancangan dengan kebutuhan keamanan	Pembelajaran Berbasis Proyek dan Diskusi tentang implementasi keamanan jaringan dalam kehidupan nyata			5%																																																																																																																																																																																			

6	Mahasiswa mampu mengevaluasi algoritma kriptografi modern untuk aplikasi tertentu	1. Penerapan teknik kriptografi modern dalam pengembangan aplikasi 2. Kemampuan memilih teknik kriptografi yang sesuai dengan standar keamanan 3. Kemampuan mengimplementasikan teknik kriptografi dalam aplikasi 4. Kelengkapan evaluasi algoritma kriptografi	Ketepatan analisis relevansi algoritma dengan aplikasinya	Pembelajaran berbasis proyek dan Penugasan proyek pengembangan aplikasi dengan menerapkan teknik kriptografi modern			5%
7	Mahasiswa mampu mengembangkan teknologi deteksi intrusi dengan menggunakan perangkat lunak terkini	1. Penerapan teknik kriptografi modern dalam pengembangan aplikasi 2. Kemampuan memilih teknik kriptografi yang sesuai 3. Kemampuan mengimplementasikan standar keamanan 4. Ketepatan implementasi teknologi deteksi intrusi	Efektivitas solusi deteksi intrusi yang diusulkan	Pembelajaran berbasis proyek dan Pengembangan aplikasi keamanan dengan teknik kriptografi			5%
8	Mampu menjelaskan dengan lebih baik materi-materi dari minggu ke-1 s.d. ke-7	1. Menerapkan konsep yang telah dipelajari 2. Mengalisis dan memecahkan masalah 3. Menjawab soal esai dan studi kasus	Kedalaman jawaban	Menyelesaikan soal ujian Sub-Sumatif			15%
9	Mahasiswa mampu menyusun strategi keamanan jaringan berbasis proyek tertentu	1. Analisis kebutuhan keamanan informasi organisasi 2. Rancangan arsitektur jaringan yang sesuai 3. Ketepatan strategi yang disusun	Relevansi strategi dengan permasalahan di proyek	Pembelajaran berbasis proyek dan penugasan			5%
11	Mahasiswa mampu menganalisis dan merespon insiden keamanan menggunakan prinsip forensik digital	1. Kemampuan menciptakan metode baru dalam deteksi dan pencegahan intrusi 2. Penerapan teknologi terkini dalam keamanan jaringan 3. Ketepatan analisis insiden	Kelengkapan respons terhadap insiden keamanan	Pembelajaran Berbasis Proyek, diskusi dan penugasan			5%
12	Mahasiswa mampu mengembangkan solusi kriptografi inovatif untuk meningkatkan keamanan data dalam jaringan	1. Kemampuan menganalisis kebutuhan organisasi 2. Kemampuan mengevaluasi efektivitas algoritma kriptografi 3. Kemampuan memberikan rekomendasi berdasarkan analisis 4. Kreativitas solusi yang dikembangkan	Relevansi solusi terhadap kebutuhan keamanan data	Pembelajaran berbasis proyek, Forum diskusi dan penugasan penilaian hasil proyek			5%
13	Mahasiswa mampu membuat laporan evaluasi keamanan jaringan yang terstruktur dan informatif	1. Integrasi lapisan keamanan 2. Pemahaman solusi keamanan berlapis 3. Kemampuan menerapkan solusi keamanan 4. Kelengkapan laporan evaluasi	Kejelasan penyajian data dan rekomendasi	Pembelajaran Berbasis Proyek, Diskusi tentang implementasi solusi keamanan berlapis, Analisis kasus keamanan berlapis, dan Tugas daring			5%
14	Mahasiswa mampu merevisi rancangan keamanan berdasarkan umpan balik	1. Pemahaman konsep keamanan berlapis 2. Kemampuan mengidentifikasi potensi serangan siber 3. Kemampuan merancang solusi keamanan yang efektif 4. Ketepatan revisi rancangan	Perbaikan yang relevan dengan umpan balik	Pembelajaran Berbasis Proyek, Forum Diskusi dan Penugasan Proyek			5%

15	Mahasiswa mampu menyusun laporan akhir proyek keamanan jaringan dan kriptografi	1. Mampu mengidentifikasi jejak digital yang relevan 2. Mampu menerapkan prinsip forensik digital dalam analisis insiden keamanan 3. Mampu menyusun laporan forensik digital yang komprehensif 4. Kelengkapan laporan akhir	Kesesuaian dengan standar penulisan akademik	Pembelajaran berbasis proyek dan Penugasan Analisis Kasus Forensik Digital			5%
16	Mampu menjelaskan dengan lebih baik materi-materi dari minggu ke-9 s.d. ke-15	Mengintegrasikan seluruh materi Keamanan Jaringan dan Kriptografi yang telah dipelajari dalam mata kuliah	Kemampuan menyelesaikan soal terkait semua CPMK	Menyelesaikan soal Ujian Sumatif			15%
1							
2							
4							
10							

SDGS (Sustainable Development Goals)



Catatan

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- Bentuk Penilaian** meliputi penilaian tes dan non-tes sesuai dengan karakteristik capaian pembelajaran.
- Bentuk Pembelajaran** meliputi kuliah, responsi, tutorial, seminar atau bentuk lain yang setara, praktikum, praktik studio, praktik bengkel, praktik lapangan, penelitian, dan pengabdian kepada masyarakat.
- 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.
- Materi Pembelajaran** adalah bahan kajian yang disusun secara sistematis dalam bentuk pokok dan sub-pokok bahasan untuk mendukung pencapaian Sub-CPMK.
- 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%.
- TM = Tatap Muka, PT = Penugasan Terstruktur, BM = Belajar Mandiri.