UNESA	**Universitas Negeri Surabaya** **Fakultas Teknik** **Program Studi S1 Teknik Informatika**	**Kode Dokumen**

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)			SEMESTER	Tgl Penyusunan
Keamanan Data dan Informasi	5520203140		T=3	P=0	ECTS=4.77	4	6 Desember 2025

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
	I Made Suartana	.....	PARAMITHA NERISAFITRA

Model Pembelajaran: Project Based Learning

Capaian Pembelajaran (CP)

CPL-PRODI yang dibebankan pada MK

CPL-1	Mampu menunjukkan nilai-nilai agama, kebangsaan dan budaya nasional, serta etika akademik dalam melaksanakan tugasnya
CPL-8	Mampu mengimplementasikan kebutuhan computing dengan mempertimbangkan berbagai metode/algoritma yang sesuai (COM-03)
CPL-11	Mampu menganalisis persoalan computing yang kompleks untuk mengidentifikasi solusi pengelolaan proyek teknologi bidang informatika/ilmu komputer dengan mempertimbangkan wawasan perkembangan ilmu trandisiplin (KNO-01)

Capaian Pembelajaran Mata Kuliah (CPMK)

CPMK - 1	Mampu menganalisis (C4) prinsip-prinsip fundamental keamanan informasi—mencakup kerahasiaan (confidentiality), integritas (integrity), ketersediaan (availability), otentikasi, dan non-repudiasi—dalam berbagai konteks sistem teknologi informasi.
CPMK - 2	Mampu merancang (C6) dan menerapkan (C3) mekanisme kriptografi simetris dan asimetris untuk proteksi data at-rest dan in-transit menggunakan algoritma standar.
CPMK - 3	Mampu mengevaluasi (C5) postur keamanan jaringan dan sistem menggunakan perangkat standar industri serta merekomendasikan kontrol teknis untuk mitigasi kerentanan yang teridentifikasi.
CPMK - 4	Mampu menganalisis (C4) risiko keamanan informasi dan menyusun elemen-elemen kebijakan keamanan berdasarkan kerangka kerja internasional seperti ISO/IEC 27001 dan NIST Cybersecurity Framework.
CPMK - 5	Mampu menunjukkan (A3) sikap profesional dan etis dalam praktik keamanan informasi, serta bertanggung jawab atas hasil analisis dan rekomendasi yang diberikan.

Matrik CPL - CPMK

CPMK	CPL-1	CPL-8	CPL-11
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															✔	✔

Deskripsi Singkat MK: Mata kuliah ini membahas konsep fundamental, prinsip, dan praktik dalam keamanan data dan informasi. Mahasiswa akan mempelajari pilar-pilar keamanan (Kerahasiaan, Integritas, Ketersediaan), kriptografi modern, keamanan jaringan, keamanan sistem, serta manajemen risiko dan tata kelola keamanan. Pembelajaran ditekankan pada pendekatan analitis dan praktis melalui studi kasus dan sesi praktikum menggunakan perangkat lunak standar industri (seperti Nmap, Wireshark, Metasploit) untuk mempersiapkan mahasiswa dalam mengidentifikasi, menganalisis, dan memitigasi ancaman keamanan siber di dunia nyata

Pustaka

Utama :

1. Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.
2. William Stallings. 2017. Network Security Essentials : Applications and Standards Sixth edition Global edition. Pearson
3. Joseph Migga Kizza. 2020. Guide to Computer Network Security Fifth Edition. Springer.
4. Forouzan, Behrouz A., & Mukhopadhyay, Debdeep. (2015). Cryptography and Network Security (3rd Edition). McGraw-Hill.
5. International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
6. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce

Pendukung :

Dosen Pengampu	Agus Prihanto, S.T., M.Kom. I Made Suartana, S.Kom., M.Kom. Rifqi Abdillah, M.Kom.

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	Mahasiswa mampu menjelaskan konsep fundamental keamanan informasi, arsitektur keamanan OSI, dan prinsip-prinsip desain keamanan.	Ketepatan dalam mendefinisikan CIA, ancaman, serangan, dan mekanisme keamanan.	**Kriteria:** Pemahaman konseptual yang benar. Bentuk: Partisipasi kelas, kuis formatif (tidak dinilai).	Ceramah Interaktif, Diskusi Kelompok. Membaca Stallings Bab 1. 3x50		**Materi:** Pengantar Keamanan Informasi & Jaringan. Konsep CIA, Arsitektur Keamanan OSI, Prinsip Desain Keamanan. **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	0%
2	Mahasiswa mampu menjelaskan dan menerapkan algoritma kriptografi klasik (substitusi dan transposisi) untuk enkripsi/dekripsi pesan sederhana	Ketepatan dalam menerapkan Caesar Cipher, Vigenère Cipher, dan Rail Fence Cipher; Kemampuan menganalisis frekuensi huruf.	**Kriteria:** Logika penerapan algoritma benar, hasil enkripsi/dekripsi akurat. Bentuk: Kuis, Latihan Terstruktur. **Bentuk Penilaian** : Aktifitas Partisipasif, Tes	Ceramah, Latihan Terbimbing. Mengerjakan soal latihan, membaca Stallings Bab 2-3. 2x50		**Materi:** Kriptografi Klasik: Teknik Substitusi (Caesar, Monoalphabetic, Polyalphabetic/Vigenère), Teknik Transposisi. **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	5%
3	Mahasiswa mampu menjelaskan struktur block cipher modern dan prinsip kerja Data Encryption Standard (DES) dan Advanced Encryption Standard	Kemampuan menjelaskan struktur Feistel, putaran (rounds) pada DES, dan struktur SPN pada AES.	**Kriteria:** Pemahaman alur proses enkripsi DES dan AES. Bentuk: Kuis. **Bentuk Penilaian** : Tes	Ceramah, Studi Kasus (Evolusi dari DES ke AES). Membaca Stallings Bab 4, 6. 2x50		**Materi:** Block Ciphers dan DES. Struktur Block Cipher Tradisional, DES, The Strength of DES, AES (pengenalan). **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	5%
4	Mahasiswa mampu menerapkan mode operasi block cipher (ECB, CBC, CFB, OFB, CTR) sesuai dengan kebutuhan aplikasi	Ketepatan dalam memilih mode operasi untuk skenario tertentu (misal, enkripsi file vs. streaming data).	**Kriteria:** Justifikasi pemilihan mode operasi logis dan benar. Bentuk: Latihan Terstruktur, bagian dari Laporan Praktikum. **Bentuk Penilaian** : Penilaian Praktikum, Praktik / Unjuk Kerja	Praktikum Terbimbing 1: Enkripsi File dengan AES		**Materi:** Mode Operasi Block Cipher. ECB, CBC, CFB, OFB, CTR. Penggunaan library kriptografi (misal, Python cryptography) **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	5%
5	Mahasiswa mampu menjelaskan konsep matematika dasar (Teori Bilangan dan Finite Fields) yang mendasari kriptografi kunci publik.	Kemampuan menghitung invers modular menggunakan Extended Euclidean Algorithm; Memahami Teorema Euler dan Fermat.	**Kriteria:** Ketepatan perhitungan matematis. Bentuk: Kuis, Latihan Terstruktur. **Bentuk Penilaian** : Tes	Ceramah, Latihan Soal. Mengerjakan soal latihan, membaca Stallings Bab 2, 5. 2x50		**Materi:** Teori Bilangan dan Finite Fields. Aritmetika Modular, Teorema Fermat & Euler, Primality Testing, Algoritma Euklides. **Pustaka:** **Materi:** Teori Bilangan dan Finite Fields. Aritmetika Modular, Teorema Fermat & Euler, Primality Testing, Algoritma Euklides. **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	5%

6	Mahasiswa mampu menjelaskan dan menerapkan algoritma kriptografi kunci publik RSA dan skema pertukaran kunci Diffie-Hellman	1. Ketepatan dalam melakukan proses pembangkitan kunci, enkripsi, dan dekripsi menggunakan RSA 2. Menghitung kunci sesi bersama dengan Diffie-Hellman.	**Kriteria:** Alur perhitungan benar, hasil akurat. Bentuk: Kuis, Latihan Terstruktur. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Praktik / Unjuk Kerja, Tes	Ceramah, Demonstrasi Perhitungan. Membaca Stallings Bab 9. 2x50		**Materi:** Kriptografi Kunci Publik. Prinsip, RSA, Pertukaran Kunci Diffie-Hellman. **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	5%
7	Mahasiswa mampu menjelaskan fungsi dan aplikasi digital signature, fungsi hash, dan MAC untuk menjamin integritas dan otentikasi data.	Kemampuan membedakan antara enkripsi, hash, dan signature; Menjelaskan cara kerja HMAC.	**Kriteria:** Pemahaman konseptual yang jelas dan mampu memberikan contoh. Bentuk: Partisipasi Diskusi, Studi Kasus. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Tes	Ceramah Interaktif, Studi Kasus (Proses validasi update software). Membaca Stallings Bab 11, 12, 13. 2x50		**Materi:** Integritas Data dan Otentikasi. Fungsi Hash (SHA), MAC, HMAC, Digital Signatures (DSA). **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	5%
8	Mengukur penguasaan materi dari pertemuan 1 hingga 7.	Sesuai dengan kunci jawaban dan rubrik penilaian soal. Bentuk: Ujian Tulis (Esai, Studi Kasus Pendek).	**Kriteria:** Sesuai dengan kunci jawaban dan rubrik penilaian soal. Bentuk: Ujian Tulis (Esai, Studi Kasus Pendek). **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Project Penugasan Kelompok		**Materi:** Seluruh materi dari Mg. 1-7. **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	15%
9	Mahasiswa mampu menggunakan Nmap untuk melakukan pemindaian port, identifikasi layanan, dan deteksi sistem operasi pada jaringan target	1. Kemampuan menggunakan sintaks Nmap yang tepat (SYN scan, version scan, OS detection); Ketepatan interpretasi output Nmap. 2. Ketepatan interpretasi output Nmap.	**Kriteria:** Laporan praktikum menunjukkan pemahaman prosedur dan analisis hasil. Bentuk: Laporan Praktikum. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Penilaian Praktikum	Praktikum Terbimbing 2: Network Discovery & Scanning. 2x50		**Materi:** Network Reconnaissance & Scanning. Penggunaan Nmap (scan types, NSE scripts). **Pustaka:** *Joseph Migga Kizza. 2020. Guide to Computer Network Security Fifth Edition. Springer.*	5%
10	Mahasiswa mampu menggunakan Wireshark untuk menangkap dan menganalisis lalu lintas jaringan untuk mengidentifikasi protokol dan potensi anomali keamanan	1. Kemampuan menggunakan filter display 2. Mengidentifikasi kredensial tidak terenkripsi (HTTP, FTP) 3. Menganalisis three-way handshake TCP	**Kriteria:** Laporan praktikum berisi temuan yang relevan dan analisis yang tajam. Bentuk: Laporan Praktikum. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Praktikum Terbimbing : Analisis Protokol Jaringan. 2x50		**Materi:** Analisis Lalu Lintas Jaringan. Penggunaan Wireshark, filter, dan protocol dissection. **Pustaka:** *Joseph Migga Kizza. 2020. Guide to Computer Network Security Fifth Edition. Springer.*	5%
11	Mahasiswa mampu menjelaskan konsep dan arsitektur Firewall dan Intrusion Detection/Prevention Systems (IDS/IPS)	1. Kemampuan membedakan antara packet filtering, stateful inspection, dan proxy firewall 2. Menjelaskan perbedaan antara IDS dan IPS.	**Kriteria:** Pemahaman arsitektur dan fungsi masing-masing teknologi. Bentuk: Studi Kasus, Diskusi. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio	Case-based Learning, Diskusi. Membaca Stallings Bab 20. 2x50		**Materi:** Keamanan Perimeter Jaringan. Firewalls (Jenis dan Konfigurasi), IDS/IPS. **Pustaka:** *Forouzan, Behrouz A., & Mukhopadhyay, Debdeep. (2015). Cryptography and Network Security (3rd Edition). McGraw-Hill.*	5%
12	Mahasiswa mampu mengidentifikasi dan menjelaskan jenis-jenis kerentanan perangkat lunak umum (buffer overflow, SQL injection) dan malicious software	1. Kemampuan menjelaskan cara kerja serangan buffer overflow dan SQL injection 2. Mengklasifikasikan malware.	**Kriteria:** Pemahaman mekanisme serangan dan dampaknya. Bentuk: Kuis, Presentasi Kelompok. **Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk	Ceramah, Video Demonstrasi Serangan. Membaca Stallings Bab 21, Proyek Akhir 2x50		**Materi:** Keamanan Perangkat Lunak & Sistem. Malicious Software, Buffer Overflow, SQL Injection. **Pustaka:** *Forouzan, Behrouz A., & Mukhopadhyay, Debdeep. (2015). Cryptography and Network Security (3rd Edition). McGraw-Hill.*	5%

13	Mahasiswa mampu menjelaskan proses manajemen risiko keamanan informasi dan komponen utama dari sebuah kebijakan keamanan	1. Kemampuan menjelaskan siklus manajemen risiko (identify, assess, treat, monitor) 2. Mengidentifikasi elemen-elemen penting dalam dokumen kebijakan.	**Kriteria:** Pemahaman proses dan struktur dokumen. Bentuk: Diskusi, Pengerjaan Proyek Akhir. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Problem-based Learning. Membaca materi ISO 27001 & NIST CSF, Proyek Akhir 2x50		**Materi:** Manajemen Risiko dan Kebijakan Keamanan. Proses Manajemen Risiko, Standar Kebijakan Keamanan. **Pustaka:** *International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*	5%
14	Mahasiswa mampu menjelaskan kerangka kerja keamanan ISO/IEC 27001 dan NIST CSF serta aspek etika dan hukum dalam keamanan siber	1. Kemampuan menjelaskan tujuan dan struktur ISO 27001 Annex A dan 5 fungsi NIST CSF 2. Membedakan antara tindakan etis dan ilegal.	**Kriteria:** Pemahaman tujuan dan struktur kerangka kerja. Bentuk: Presentasi Proyek Akhir, Diskusi. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Presentasi Proyek Akhir. Finalisasi Laporan Proyek Akhir. 2x50		**Materi:** Kerangka Kerja Keamanan dan Etika. ISO/IEC 27001, NIST CSF, Etika Profesional, UU PDP. **Pustaka:** *National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce*	10%
15	Presentasi Proyek Akhir dan Ulasan	1. Kemampuan mempresentasikan hasil analisis secara jelas, logis, dan persuasif 2. Kemampuan menjawab pertanyaan dari dosen dan audiens.	**Kriteria:** Sesuai dengan rubrik penilaian presentasi. Bentuk: Presentasi Kelompok. **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio, Praktik / Unjuk Kerja	simulasi, diskusi			10%
16	Capstone Project Akhir Semester	Mengukur penguasaan materi dari pertemuan 9 hingga 14 dan kemampuan integratif.	**Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Praktik / Unjuk Kerja	simulasi, diskusi		**Materi:** Seluruh materi dari Mg. 9-14 dan konsep integratif. **Pustaka:** *Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.*	10%

Rekap Persentase Evaluasi : Project Based Learning

No	Evaluasi	Persentase
1.	Aktifitas Partisipasif	5%
2.	Penilaian Hasil Project / Penilaian Produk	55%
3.	Penilaian Portofolio	5.83%
4.	Penilaian Praktikum	5%
5.	Praktik / Unjuk Kerja	12.5%
6.	Tes	16.67%
		100%

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.

RPS ini telah divalidasi pada tanggal 23 Agustus 2025

Koordinator Program Studi S1 Teknik Informatika

PARAMITHA NERISAFITRA
NIDN 0729058902

UPM Program Studi S1 Teknik Informatika

NIDN 0707039601

File PDF ini digenerate pada tanggal 6 Desember 2025 Jam 13:38 menggunakan aplikasi RPS-OBE SiDia Unesa