	UNIVERSITAS SUMATERA UTARA FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM PROGRAM STUDI SARJANA MATEMATIKA	Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER (RPS)

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (SKS)		SEMESTER	Tanggal Penyusunan
PENGANTAR KRIPTOGRAFI	MAT3247	Mata Kuliah Pilihan	Teori = 2	Praktik = 0	V	10 Agustus 2026

OTORISASI	Pengembang RPS	Ketua Program Studi	Ketua LINKUP USU
	Dr. Mohammad Andri Budiman S.T., M.Comp.Sc., M.E.M. Dr. Sawaluddin, M.IT Dra. Normalina Napitupulu, M.Sc	Dr. Mimmy Sari Syah Putri, M.Si	DirPPUSU

Capaian Pembelajaran

CPL-PRODI yang dibebankan pada MK

CPL04	Menguasai konsep teoritis dasar dalam kriptografi, termasuk enkripsi dan dekripsi, algoritma kunci simetris dan asimetris.
CPL05	Mampu berpikir kritis dan analitis dalam menyelesaikan masalah keamanan data menggunakan teknik kriptografi.
CPL07	Mampu mengkomunikasikan hasil analisis kriptografi dalam konteks keamanan data.
CPL11	Mampu berkolaborasi dan belajar sepanjang hayat.

Capaian Pembelajaran Mata Kuliah (CPMK)

Kode CPMK	Deskripsi CPMK	Bobot CPMK (%)
CPMK1	Mahasiswa mampu menjelaskan konsep dasar kriptografi, sejarah perkembangannya, tujuan keamanan informasi, serta prinsip kerja enkripsi dan dekripsi secara tepat (C2-C3).	**20%**
CPMK2	Mahasiswa mampu menerapkan dan menganalisis algoritma kriptografi kunci simetris dan asimetris, termasuk DES, AES, RSA, dan ECC, berdasarkan karakteristik, penggunaan kunci, serta kebutuhan keamanan (C3-C4).	**30%**
CPMK3	Mahasiswa mampu menerapkan dan menganalisis fungsi hashing, tanda tangan digital, infrastruktur kunci publik, serta protokol keamanan untuk menjaga kerahasiaan, integritas, autentikasi, dan non-repudiasi data (C3-C5).	**30%**
CPMK4	Mahasiswa mampu mengevaluasi solusi kriptografi pada kasus keamanan data dan mengomunikasikan hasilnya melalui Case Method dan Project Based Learning secara kolaboratif, dengan penggunaan AI generatif secara kritis, transparan, etis, aman, dan terverifikasi (C5-C6).	**20%**

Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)

	Sub-CPMK	Deskripsi
	Sub-CPMK 1	Mampu menjelaskan pengertian, tujuan, sejarah perkembangan kriptografi, konsep keamanan informasi, jenis ancaman, serta prinsip dasar enkripsi dan dekripsi (C2-C3).
	Sub-CPMK 2	Mampu menerapkan dan menganalisis algoritma kriptografi kunci simetris, khususnya DES dan AES, serta membandingkan karakteristik dan penggunaannya (C3-C4).
	Sub-CPMK 3	Mampu menerapkan dan menganalisis algoritma kriptografi kunci asimetris, khususnya RSA dan ECC, termasuk konsep pasangan kunci dan pengelolaan kunci (C3-C4).
	Sub-CPMK 4	Mampu menerapkan dan mengevaluasi fungsi hashing, verifikasi integritas, message authentication, dan tanda tangan digital berdasarkan tujuan keamanan yang relevan (C3-C5).
	Sub-CPMK 5	Mampu menjelaskan dan menganalisis Infrastruktur Kunci Publik (PKI), sertifikat digital, PGP, serta SSL/TLS dalam membangun komunikasi digital yang aman (C3-C5).
	Sub-CPMK 6	Mampu menganalisis penerapan kriptografi pada e-commerce, keuangan, dan layanan digital serta mengevaluasi ancaman, asumsi keamanan, dan pilihan mekanisme kriptografi melalui studi kasus (C4-C5).
	Sub-CPMK 7	Mampu mengevaluasi perkembangan kriptografi modern dan kuantum serta merancang solusi konseptual keamanan data dalam proyek kelompok, kemudian mendokumentasikan dan mempresentasikan hasil secara ilmiah, kolaboratif, dan bertanggung jawab dengan penggunaan AI yang transparan dan terverifikasi (C4-C6).

Korelasi CPMK dan Sub CPMK

	Sub-1	Sub-2	Sub-3	Sub-4	Sub-5	Sub-6	Sub-7
CPMK 1	✓	✓					
CPMK 2		✓	✓				
CPMK 3		✓	✓	✓	✓		
CPMK 4				✓	✓	✓	✓

Deskripsi Singkat Mata Kuliah

Mata kuliah Pengantar Kriptografi merupakan mata kuliah pilihan pada Program Studi Sarjana Matematika yang membekali mahasiswa dengan landasan teoritis untuk memahami pengamanan informasi melalui teknik kriptografi. Materi mencakup sejarah dan konsep keamanan informasi, enkripsi-dekripsi, algoritma kunci simetris DES dan AES, algoritma kunci asimetris RSA dan ECC, fungsi hashing, tanda tangan digital, Infrastruktur Kunci Publik (PKI), PGP, SSL/TLS, perkembangan kriptografi kuantum, serta aplikasi kriptografi pada e-commerce dan keuangan. Seluruh beban 2 SKS dilaksanakan sebagai teori melalui kuliah, diskusi, latihan analitis, Case Method (CM), dan Project Based Learning (PBL). AI generatif dapat digunakan secara terbatas untuk eksplorasi penjelasan, penyusunan alternatif skenario ancaman, pemeriksaan konsistensi argumentasi, atau bantuan menyusun pseudocode. Setiap keluaran AI wajib diverifikasi dengan konsep kriptografi, perhitungan, sumber pembelajaran yang ditetapkan, atau penalaran pembanding; penggunaan AI harus dinyatakan secara transparan dan tidak boleh melibatkan data sensitif, kunci rahasia, atau informasi rahasia lainnya.

Bahan Kajian / Materi Pembelajaran

1. Pengantar Kriptografi dan Keamanan Informasi
- Sejarah perkembangan kriptografi
- Tujuan keamanan: kerahasiaan, integritas, autentikasi, dan non-repudiasi
- Ancaman, serangan, enkripsi, dan dekripsi

2. Kriptografi Kunci Simetris
- Konsep cipher kunci simetris
- DES dan AES
- Perbandingan karakteristik dan penggunaan
- Penerapan enkripsi-dekripsi pada data sederhana

3. Kriptografi Kunci Asimetris
- Konsep kunci publik dan kunci privat
- RSA dan ECC
- Pengelolaan dan distribusi kunci
- Penerapan enkripsi-dekripsi pada data sederhana

4. Hashing dan Tanda Tangan Digital
- Fungsi hash dan verifikasi integritas
- Message authentication
- Tanda tangan digital dan sifat keamanannya

5. Infrastruktur Kunci Publik dan Protokol Keamanan
- PKI dan sertifikat digital

	- PGP - SSL/TLS 6. Aplikasi Kriptografi - E-commerce dan transaksi digital - Keuangan dan layanan digital - Analisis ancaman dan pemilihan mekanisme kriptografi 7. Kriptografi Modern dan Masa Depan - Kriptografi kuantum dan tantangan terhadap algoritma klasik - Arah perkembangan kriptografi dan kesiapan migrasi algoritma 8. Penggunaan Solusi Kriptografi dalam Analisis Keamanan - Analisis keamanan berdasarkan konsep kriptografi - Evaluasi alternatif mekanisme keamanan data - Penyusunan argumentasi, dokumentasi, dan komunikasi ilmiah
PUSTAKA	UTAMA: 1. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson. 2. Schneier, B. Applied Cryptography. Wiley.
	PENDUKUNG: 1. Stinson, D. R. Cryptography: Theory and Practice. CRC Press. 2. Ferguson, N., & Schneier, B. Practical Cryptography. Wiley. 3. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography. CRC Press.
Dosen Pengampu	Dr. Mohammad Andri Budiman S.T., M.Comp.Sc., M.E.M.; Dr. Sawaluddin, M.IT; Dra. Normalina Napitupulu, M.Sc
Matakuliah syarat	Tidak ada

Minggu ke-	**Kemampuan Akhir yang Diharapkan (Sub-CPMK)**	**Penilaian**		**Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa** [Estimasi Waktu]		**Bahan Kajian (Materi Pembelajaran)**	**SDGS**	**Bobot Penilaian (%)**
		Indikator	**Kriteria dan Bentuk**	**Asinkronus**	**Sinkrons**			
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**8**	**(9)**
1	Sub-CPMK 1: Mampu menjelaskan pengertian, tujuan, sejarah perkembangan kriptografi, konsep keamanan informasi, jenis ancaman, serta prinsip dasar enkripsi dan dekripsi (C2-C3).	1. Ketepatan menjelaskan tujuan dan terminologi dasar kriptografi. 2. Ketepatan membedakan kerahasiaan, integritas, autentikasi, dan non-repudiasi. 3. Ketepatan mengidentifikasi ancaman dan kebutuhan keamanan.	Kriteria: Rubrik Penilaian Tugas Bentuk: Tugas 1 individu (non-tes).	BM [(1 x (2 x 60 menit))]: membaca RPS, bahan ajar, dan sejarah kriptografi. PT [(1 x (2 x 60 menit))]: Tugas 1 - menganalisis kebutuhan keamanan pada contoh komunikasi digital sederhana. AI boleh digunakan untuk memperoleh penjelasan alternatif, tetapi hasil wajib diverifikasi dan penggunaannya dicatat. Moda: LMS USU.	TM Teori [(1 x (2 x 50 menit))]: orientasi perkuliahan, pengantar kriptografi, tujuan keamanan, ancaman, dan diskusi. Media: PPT, papan tulis, LMS. Metode: Discovery Learning & Discussion.	1. Pengantar Kriptografi dan Keamanan Informasi: - Sejarah perkembangan - Enkripsi dan dekripsi - Tujuan keamanan informasi - Ancaman dan serangan	SDG 4, SDG 16	**Tugas: 5%**

Minggu ke-	Kemampuan Akhir yang Diharapkan (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa [Estimasi Waktu]		Bahan Kajian (Materi Pembelajaran)	SDGS	Bobot Penilaian (%)
		Indikator	Kriteria dan Bentuk	Asinkronus	Sinkrons			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	8	(9)
2-3	Sub-CPMK 2: Mampu menerapkan dan menganalisis algoritma kriptografi kunci simetris, khususnya DES dan AES, serta membandingkan karakteristik dan penggunaannya (C3-C4).	1. Ketepatan menjelaskan prinsip kerja cipher simetris. 2. Ketepatan menjelaskan struktur DES dan AES. 3. Kemampuan membandingkan karakteristik, kekuatan, dan konteks penggunaan.	Kriteria: Rubrik Penilaian Quiz Bentuk: Kuis 1 (tes) dan latihan formatif.	BM [(2 x (2 x 60 menit))]: membaca materi DES/AES dan latihan konsep. PT [(2 x (2 x 60 menit))]: latihan enkripsi-dekripsi sederhana dan perbandingan DES/AES. Kuis dilaksanakan tanpa AI kecuali dosen menetapkan lain. Moda: LMS USU.	TM Teori [(2 x (2 x 50 menit))]: prinsip cipher simetris, DES, AES, contoh perhitungan/transformasi, dan diskusi keamanan. Media: PPT, papan tulis, LMS. Metode: Guided Discovery & Problem Solving.	2. Kriptografi Kunci Simetris: - DES - AES - Proses enkripsi-dekripsi - Perbandingan karakteristik dan penggunaan	SDG 4, SDG 9	**Kuis: 5%**
4-5	Sub-CPMK 3: Mampu menerapkan dan menganalisis algoritma kriptografi kunci asimetris, khususnya RSA dan ECC, termasuk konsep pasangan kunci dan pengelolaan kunci (C3-C4).	1. Ketepatan menjelaskan perbedaan kunci publik dan kunci privat. 2. Ketepatan menerapkan konsep dasar RSA dan ECC pada contoh sederhana. 3. Ketepatan menganalisis kelebihan, keterbatasan, dan penggunaan algoritma asimetris.	Kriteria: Rubrik Penilaian Tugas Bentuk: Tugas 2 individu (non-tes).	BM [(2 x (2 x 60 menit))]: kajian RSA/ECC dan latihan konsep kunci publik. PT [(2 x (2 x 60 menit))]: Tugas 2 - analisis alur pembentukan kunci, enkripsi-dekripsi, dan perbandingan RSA/ECC. AI boleh membantu membuat pertanyaan pembanding atau memeriksa kejelasan penjelasan; seluruh isi teknis wajib diverifikasi. Moda: LMS USU.	TM Teori [(2 x (2 x 50 menit))]: konsep kunci publik, RSA, ECC, distribusi/pengelolaan kunci, dan latihan analitis. Media: PPT, papan tulis, LMS. Metode: Collaborative Learning & Problem Solving.	3. Kriptografi Kunci Asimetris: - Kunci publik dan privat - RSA - ECC - Pengelolaan dan distribusi kunci	SDG 4, SDG 9	**Tugas: 5%**
6-7	Sub-CPMK 4: Mampu menerapkan dan mengevaluasi fungsi hashing, verifikasi integritas, message authentication, dan tanda tangan digital berdasarkan tujuan keamanan yang relevan (C3-C5).	1. Ketepatan menjelaskan sifat fungsi hash dan integritas data. 2. Ketepatan membedakan hashing, message authentication, dan tanda tangan digital. 3. Kualitas analisis pemilihan mekanisme untuk kasus keamanan tertentu.	Kriteria: Rubrik Penilaian CM/PBL Bentuk: Case Method 1 - studi kasus kelompok (non-tes).	BM [(2 x (2 x 60 menit))]: kajian hashing, autentikasi, dan tanda tangan digital. PT [(2 x (2 x 60 menit))]: CM 1 - menganalisis kasus perubahan data/pemalsuan pesan, menentukan mekanisme yang sesuai, dan mempertanggungjawabkan pilihan. AI boleh digunakan untuk brainstorming skenario serangan, tetapi kelompok wajib memeriksa kebenaran setiap asumsi dan mencatat penggunaan AI. Moda: LMS USU.	TM Teori [(2 x (2 x 50 menit))]: fungsi hash, verifikasi integritas, message authentication, tanda tangan digital, dan diskusi kasus. Media: PPT, papan tulis, LMS. Metode: Case Method.	4. Hashing dan Tanda Tangan Digital: - Fungsi hash - Verifikasi integritas - Message authentication - Tanda tangan digital	SDG 4, SDG 16	**CM: 10%**
8	**UJIAN TENGAH SEMESTER (UTS)**							**15%**

Minggu ke-	Kemampuan Akhir yang Diharapkan (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa [Estimasi Waktu]		Bahan Kajian (Materi Pembelajaran)	SDGS	Bobot Penilaian (%)
		Indikator	Kriteria dan Bentuk	Asinkronus	Sinkrons			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	8	(9)
9-10	Sub-CPMK 5: Mampu menjelaskan dan menganalisis PKI, sertifikat digital, PGP, serta SSL/TLS dalam membangun komunikasi digital yang aman (C3-C5).	1. Ketepatan menjelaskan komponen dan peran PKI/sertifikat digital. 2. Ketepatan menjelaskan fungsi PGP dan SSL/TLS. 3. Kemampuan menganalisis alur kepercayaan dan autentikasi pada komunikasi aman.	Kriteria: Rubrik Penilaian CM/PBL Bentuk: Case Method 2 - laporan dan presentasi kelompok (non-tes).	BM [(2 x (2 x 60 menit))]: kajian PKI, PGP, SSL/TLS, dan model kepercayaan. PT [(2 x (2 x 60 menit))]: CM 2 - menganalisis skenario komunikasi digital, memetakan sertifikat/kunci/protokol, mengidentifikasi potensi kegagalan, dan memberi rekomendasi. AI dapat membantu menyusun alternatif diagram atau pertanyaan uji, tetapi analisis akhir wajib berasal dari mahasiswa dan terverifikasi. Moda: LMS USU.	TM Teori [(2 x (2 x 50 menit))]: PKI, sertifikat digital, PGP, SSL/TLS, trust model, dan diskusi studi kasus. Media: PPT, papan tulis, LMS. Metode: Case Method & Small Group Discussion.	5. PKI dan Protokol Keamanan: - Infrastruktur Kunci Publik - Sertifikat digital - PGP - SSL/TLS	SDG 4, SDG 9, SDG 16	**CM: 15%**
11-12	Sub-CPMK 6: Mampu menganalisis penerapan kriptografi pada e-commerce, keuangan, dan layanan digital serta mengevaluasi ancaman, asumsi keamanan, dan pilihan mekanisme kriptografi melalui studi kasus (C4-C5).	1. Ketepatan merumuskan aset, ancaman, dan tujuan keamanan. 2. Ketepatan memilih mekanisme kriptografi sesuai kebutuhan. 3. Kualitas argumentasi, dokumentasi, dan verifikasi analisis kasus.	Kriteria: Rubrik Penilaian CM/PBL Bentuk: PBL - Milestone 1 (proposal, threat model, dan rancangan solusi konseptual).	BM [(2 x (2 x 60 menit))]: kajian referensi dan perumusan proyek. PT [(2 x (2 x 60 menit))]: PBL Milestone 1 - memilih kasus e-commerce/keuangan/layanan digital, merumuskan aset-ancaman, tujuan keamanan, dan rancangan mekanisme kriptografi. AI boleh digunakan untuk brainstorming ancaman atau pemeriksaan kelengkapan; data sensitif dan kunci rahasia tidak boleh dimasukkan ke sistem AI publik. Moda: LMS USU.	TM Teori [(2 x (2 x 50 menit))]: aplikasi kriptografi, threat modeling, pemilihan mekanisme, konsultasi, dan umpan balik proposal. Media: PPT, papan tulis, LMS. Metode: Project Based Learning.	6. Aplikasi Kriptografi: - E-commerce - Keuangan dan transaksi digital - Threat model - Pemilihan mekanisme kriptografi	SDG 4, SDG 9, SDG 16	**PBL: 10%**
13-14	Sub-CPMK 7: Mampu mengevaluasi perkembangan kriptografi modern dan kuantum serta merancang solusi konseptual keamanan data dalam proyek kelompok secara ilmiah dan bertanggung jawab (C4-C6).	1. Ketepatan menjelaskan tantangan komputasi kuantum terhadap kriptografi klasik. 2. Ketepatan mengevaluasi kebutuhan adaptasi/migrasi mekanisme kriptografi. 3. Kualitas integrasi konsep, evaluasi risiko, dan argumentasi pada proyek.	Kriteria: Rubrik Penilaian CM/PBL Bentuk: PBL - Milestone 2 (analisis lengkap, validasi argumentasi, dan laporan sementara).	BM [(2 x (2 x 60 menit))]: kajian perkembangan modern dan pengembangan proyek. PT [(2 x (2 x 60 menit))]: PBL Milestone 2 - melengkapi analisis solusi, membandingkan alternatif, menilai risiko, menyusun rencana adaptasi, dan merevisi berdasarkan umpan balik. Penggunaan AI harus disertai catatan prompt penting, koreksi, dan cara verifikasi. Moda: LMS USU.	TM Teori [(2 x (2 x 50 menit))]: kriptografi kuantum, masa depan kriptografi, sintesis materi, klinik proyek, dan peer review. Media: PPT, papan tulis, LMS. Metode: Project Based Learning.	7. Kriptografi Modern dan Masa Depan: - Kriptografi kuantum - Tantangan bagi algoritma klasik - Arah perkembangan dan kesiapan migrasi - Integrasi konsep dalam proyek	SDG 4, SDG 9, SDG 16	**PBL: 10%**

Minggu ke-	Kemampuan Akhir yang Diharapkan (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa [Estimasi Waktu]		Bahan Kajian (Materi Pembelajaran)	SDGS	Bobot Penilaian (%)
		Indikator	Kriteria dan Bentuk	Asinkronus	Sinkrons			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	8	(9)
15	Sub-CPMK 7: Mampu mendokumentasikan, mempresentasikan, dan mempertanggungjawabkan rancangan solusi kriptografi secara ilmiah, kolaboratif, dan transparan (C5-C6).	1. Kejelasan masalah, tujuan keamanan, dan rancangan solusi. 2. Kualitas analisis ancaman, argumentasi, dan evaluasi keterbatasan. 3. Kemampuan menjawab pertanyaan dan menjelaskan kontribusi anggota. 4. Transparansi dan keamanan penggunaan AI.	Kriteria: Rubrik Penilaian CM/PBL Bentuk: PBL - Finalisasi dan presentasi proyek.	BM [(1 x (2 x 60 menit))]: finalisasi laporan dan slide. PT [(1 x (2 x 60 menit))]: menyusun paket akhir proyek: laporan, diagram/rancangan, analisis ancaman, evaluasi alternatif, referensi, serta deklarasi penggunaan AI bila ada. Moda: LMS USU.	TM Teori [(1 x (2 x 50 menit))]: presentasi, tanya jawab, refleksi, dan sintesis Pengantar Kriptografi. Media: PPT, LMS. Metode: Project Based Learning & Presentation.	Evaluasi Solusi Kriptografi: - Analisis ancaman dan kebutuhan keamanan - Evaluasi mekanisme kriptografi - Dokumentasi hasil analisis	SDG 4, SDG 9, SDG 16	**PBL: 5%**
16	**UJIAN AKHIR SEMESTER (UAS)**							**20%**

Catatan sesuai dengan SN Dikti Permendikbud No 3/2020:

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-CP 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. Teknik 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.

RENCANA ASESMEN

Bentuk Evaluasi	Sub-CPMK	Instrumen Penilaian [Frekuensi]	Tagihan (bukti)	Bobot Penilaian (%)

		Formatif	Sumatif		
Tugas Individu	Sub-CPMK 1, 3	Umpan balik [2 kali]	Rubrik Tugas [2 kali]	Lembar analisis/perhitungan, argumentasi, referensi, dan catatan AI bila digunakan	10%
Kuis/Post-test	Sub-CPMK 2	Umpan balik [1 kali]	Rubrik Quiz [1 kali]	Jawaban kuis di LMS/lembar jawaban	5%
Case Method (CM)	Sub-CPMK 4-5	Umpan balik dan diskusi kasus [2 kali]	Rubrik CM/PBL [2 kasus]	Analisis kasus, diagram/alur, laporan, dan presentasi	25%
Project Based Learning (PBL)	Sub-CPMK 6-7	Umpan balik berkala [3 milestone]	Rubrik CM/PBL [1 proyek]	Proposal, threat model, rancangan solusi, laporan, slide, dan deklarasi AI	25%
Ujian Tengah Semester	Sub-CPMK 1-4	Umpan balik [1 kali]	Rubrik Ujian Esai [1 kali]	Lembar jawaban/berkas	15%
Ujian Akhir Semester	Sub-CPMK 5-7	Umpan balik [1 kali]	Rubrik Ujian Esai [1 kali]	Lembar jawaban/berkas	20%
Total					**100%**

Penjelasan:

1. Tugas 10% - Dua tugas individu masing-masing 5% untuk menilai ketepatan konsep, analisis algoritma/mekanisme, argumentasi, verifikasi, dan kemampuan menjelaskan solusi keamanan.
2. Kuis 5% - Satu kuis untuk mengukur penguasaan konsep dan analisis kriptografi kunci simetris. AI tidak digunakan pada kuis kecuali dosen menetapkan lain.
3. Case Method (CM) 25% - Dua studi kasus terstruktur (10% dan 15%) yang menilai kemampuan merumuskan kebutuhan keamanan, memilih mekanisme kriptografi, menganalisis ancaman dan asumsi, mengevaluasi alternatif, serta memberikan rekomendasi yang dapat dipertanggungjawabkan.
4. Project Based Learning (PBL) 25% - Satu proyek kelompok bertahap (milestone 10% + 10% + finalisasi/presentasi 5%) yang menilai threat model, desain solusi konseptual, analisis keamanan, validasi argumentasi, dokumentasi, kolaborasi, serta komunikasi ilmiah.
5. UTS 15% - Ujian mencakup Sub-CPMK 1-4. Penggunaan AI tidak diperkenankan kecuali dosen secara eksplisit menetapkan ujian terbuka berbantuan alat.
6. UAS 20% - Ujian mencakup Sub-CPMK 5-7. Penggunaan AI tidak diperkenankan kecuali dosen secara eksplisit menetapkan ujian terbuka berbantuan alat. Pada Tugas, CM, dan PBL, penggunaan AI harus transparan, aman, dan seluruh keluaran wajib diverifikasi.

RUBRIK PENILAIAN

Rubrik Penilaian Quiz (Post-test)

Nilai per butir soal	Kriteria
4 (>81)	Jawaban tepat dan lengkap; konsep kriptografi, tujuan keamanan, algoritma/mekanisme yang dipilih, langkah analisis, dan interpretasi benar serta konsisten.
3 (71-80)	Konsep dan langkah utama benar; terdapat sedikit kekeliruan pada detail algoritma, terminologi, asumsi keamanan, atau interpretasi.
2 (60-70)	Sebagian langkah benar, tetapi terdapat beberapa kesalahan konsep atau analisis yang memengaruhi kualitas jawaban.
1 (<60)	Konsep atau mekanisme utama kurang tepat; penyelesaian tidak selesai atau tidak menunjukkan pemahaman kriptografi yang memadai.

Skor kuis = jumlah nilai per butir soal / banyak soal (skor maksimal = 100)

Rubrik Penilaian Case Method (CM) dan Project Based Learning (PBL)

KATEGORI	4 Sangat Baik	3 Baik	2 Cukup	1 Kurang	Nilai
	> 81	71 -80	60 – 70	< 60	
Perumusan Masalah, Aset, dan Tujuan Keamanan	Masalah, aset, aktor, ancaman, asumsi, dan tujuan keamanan dirumuskan sangat jelas serta relevan dengan konteks kasus/proyek.	Perumusan masalah dan tujuan keamanan jelas dengan kekurangan kecil pada aset, ancaman, atau asumsi.	Masalah cukup teridentifikasi tetapi aset, ancaman, asumsi, atau tujuan keamanan belum lengkap.	Masalah dan tujuan keamanan tidak jelas atau tidak sesuai dengan konteks.	

Ketepatan Pemilihan Mekanisme Kriptografi	Mekanisme dipilih sangat tepat, disertai argumentasi teori, tujuan keamanan, syarat penggunaan, alternatif pembanding, dan keterbatasan yang kuat.	Mekanisme tepat dan argumentasi memadai; pembandingan alternatif masih terbatas.	Mekanisme cukup sesuai tetapi alasan pemilihan lemah atau mengabaikan beberapa syarat penting.	Mekanisme tidak sesuai atau dipilih tanpa argumentasi yang dapat dipertanggungjawabkan.	
Ketepatan Analisis dan Verifikasi	Alur algoritma/protokol dianalisis benar; asumsi diperiksa; konsistensi hasil diverifikasi melalui konsep, perhitungan, contoh uji, atau pembanding yang relevan.	Analisis benar dan verifikasi memadai dengan kekurangan kecil pada dokumentasi atau pengujian.	Analisis hanya sebagian benar atau verifikasi terbatas sehingga keandalan hasil belum kuat.	Analisis tidak sesuai dan hasil/argumentasi tidak diverifikasi.	
Analisis Keamanan dan Interpretasi Risiko	Kerahasiaan, integritas, autentikasi, non-repudiasi, ancaman, serangan, batas mekanisme, dan risiko residual dianalisis secara kritis serta kontekstual.	Analisis keamanan dan interpretasi risiko baik dengan beberapa detail yang belum mendalam.	Analisis keamanan hanya sebagian dan interpretasi masih deskriptif.	Tidak ada analisis keamanan yang memadai atau kesimpulan bertentangan dengan asumsi/fakta kasus.	
Kolaborasi, Dokumentasi, dan Komunikasi	Kontribusi anggota jelas, dokumentasi lengkap dan dapat ditelusuri, presentasi sistematis, serta kelompok mampu menjawab pertanyaan dengan argumentasi kuat.	Kolaborasi dan komunikasi baik; dokumentasi cukup lengkap dengan kekurangan kecil.	Pembagian kerja atau dokumentasi kurang jelas; presentasi/argumentasi masih terbatas.	Kolaborasi lemah, dokumentasi tidak memadai, atau kelompok tidak mampu mempertanggungjawabkan hasil.	
AI Generatif, Etika, dan Keamanan Informasi	AI digunakan proporsional sebagai alat bantu; prompt penting, koreksi, dan peran AI dinyatakan transparan; seluruh keluaran diverifikasi; tidak ada data sensitif/kunci rahasia yang dibagikan; mahasiswa mampu menjelaskan hasil tanpa bergantung pada AI.	Penggunaan AI sesuai dan dinyatakan; sebagian besar keluaran diverifikasi dan aspek keamanan informasi diperhatikan.	Penggunaan AI cukup dominan, dokumentasi kurang lengkap, verifikasi hanya sebagian, atau pertimbangan keamanan informasi belum memadai.	Keluaran AI diterima tanpa verifikasi, penggunaan AI disembunyikan, AI menggantikan penalaran utama, atau data sensitif/kunci rahasia digunakan secara tidak semestinya.	

Catatan: Penggunaan AI generatif tidak menggantikan penalaran, analisis keamanan, verifikasi, atau tanggung jawab akademik mahasiswa. Mahasiswa wajib dapat menjelaskan dan mempertanggungjawabkan seluruh hasil yang diserahkan serta tidak memasukkan data sensitif, kunci rahasia, atau informasi rahasia ke layanan AI publik.

Rubrik Penilaian Ujian Esai

Kategori	Sangat Baik > 81	Baik 71 -80	Cukup 60 – 70	Kurang < 60	Nilai
Pemahaman terhadap Pertanyaan	Memahami pertanyaan dengan tepat sekali	Memahami pertanyaan	Tidak memahami pertanyaan secara penuh dan tepat	Tidak memahami pertanyaan	
Isi	Jawaban menunjukkan pemahaman mendalam terhadap teori kriptografi; pemilihan algoritma/mekanisme, alur analisis, asumsi keamanan, dan interpretasi terintegrasi dengan tepat.	Jawaban menunjukkan pemahaman yang baik; konsep dan mekanisme utama tepat dengan sedikit kekurangan pada analisis keamanan atau interpretasi.	Jawaban menunjukkan pemahaman sebagian; terdapat kesalahan konsep/analisis dan argumentasi keamanan belum memadai.	Jawaban menunjukkan ketidakpahaman terhadap konsep/mekanisme yang ditanyakan sehingga penyelesaian tidak dapat dipertanggungjawabkan.	
Kejelasan Tulisan	Semua gagasan tulisan disampaikan dengan baik dan jelas.	Sebagian besar gagasan tulisan disampaikan dengan baik dan jelas.	Sebagian gagasan tulisan disampaikan dengan baik dan jelas.	Gagasan tulisan tidak disampaikan dengan baik dan jelas.	
Kejelasan Bahasa	Menggunakan Bahasa asing /Indonesia dengan baik dan benar sedikit kesalahan tatabahasa dan pilihan kata yang tidak mengganggu pemahaman	Menggunakan Bahasa asing /Indonesia dengan baik dan benar dengan sedikit kesalahan tatabahasa dan pilihan kata yang mengganggu pemahaman.	Menggunakan Bahasa asing /Indonesia dengan cukup baik dan benar dengan beberapa kesalahan tatabahasa dan pilihan kata	Tidak menggunakan Bahasa asing/Indonesia dengan baik dan benar karena tulisan memuat banyak kesalahan tatabahasa dan pilihan kata	

INTEGRASI SDGs DALAM MATA KULIAH

SDGs	Relevansi dengan Mata Kuliah
SDG 4 (Pendidikan Berkualitas)	Mata kuliah mengembangkan kemampuan berpikir kritis, analitis, problem solving, literasi keamanan digital, komunikasi ilmiah, kolaborasi, dan pembelajaran sepanjang hayat, termasuk literasi AI yang bertanggung jawab.
SDG 9 (Industri, Inovasi, dan Infrastruktur)	Kriptografi merupakan fondasi infrastruktur digital yang aman untuk layanan daring, e-commerce, keuangan, komunikasi, dan inovasi teknologi yang membutuhkan perlindungan data serta kepercayaan digital.
SDG 16 (Perdamaian, Keadilan, dan Kelembagaan yang Tangguh)	Pembelajaran menekankan integritas, autentikasi, perlindungan informasi, keterlacakan keputusan, etika keamanan siber, integritas akademik, transparansi penggunaan AI, serta tanggung jawab dalam pengelolaan data dan kunci.

Rubrik Penilaian Tugas

Deskripsi	Sangat Baik > 81	Baik 71 -80	Cukup 60 – 70	Kurang < 60	Nilai
	4	3	2	1	
Ketepatan konsep, analisis, dan hasil	Konsep dan mekanisme kriptografi sangat tepat; alur analisis/perhitungan valid; asumsi keamanan diperiksa; kesimpulan akurat dan dapat dipertanggungjawabkan.	Konsep dan analisis tepat; terdapat sedikit kekurangan pada detail perhitungan, asumsi, atau interpretasi.	Konsep cukup sesuai, tetapi beberapa kesalahan memengaruhi hasil atau interpretasi.	Konsep/mekanisme tidak sesuai, hasil tidak dapat dipertanggungjawabkan, atau penyelesaian tidak selesai.	
Dokumentasi, argumentasi, dan verifikasi	Argumentasi sistematis, sumber/rujukan dan langkah kerja terdokumentasi, serta hasil diverifikasi dengan konsep, perhitungan, atau pembanding yang relevan.	Dokumentasi dan verifikasi memadai dengan sedikit kekurangan.	Dokumentasi atau verifikasi hanya sebagian sehingga alasan/kesimpulan belum cukup kuat.	Dokumentasi dan verifikasi tidak memadai; kesimpulan tidak memiliki dasar yang jelas.	
Ketepatan waktu, kepatuhan instruksi, dan transparansi AI	Tugas tepat waktu; seluruh instruksi dipenuhi; penggunaan AI (jika ada) dinyatakan, dibatasi sesuai tugas, tidak melibatkan data sensitif/kunci rahasia, dan seluruh saran AI diverifikasi secara mandiri.	Tugas tepat waktu dan sebagian besar instruksi dipenuhi; penggunaan AI dinyatakan dengan dokumentasi dan verifikasi yang cukup.	Tugas terlambat maksimal satu hari atau beberapa instruksi belum dipenuhi; dokumentasi/verifikasi penggunaan AI kurang lengkap.	Tugas terlambat lebih dari satu hari/tidak memenuhi instruksi utama atau penggunaan AI tidak transparan/tidak sesuai ketentuan.	

Catatan:

1. **CPL-PRODI** adalah kemampuan yang dimiliki oleh setiap lulusan PRODI yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan keterampilan 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.
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-CP 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.
5. **Indikator penilaian** adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
6. **Kriteria Penilaian** adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan.
7. **Teknik 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.