RENCANA PEMBELAJARAN SEMESTER (RPS)

UNIVERSITAS DIPONEGORO

SPMI-UNDIP	RPS	S1.SK-FT-UNDIP	063

Revisi ke		1
Tanggal		5 Juli 2022
Dikaji Ulang Oleh		Ketua Program Studi Teknik Komputer
Dikendalikan Oleh		GPM Teknik Komputer
Disetujui Oleh		Dekan Fakultas Teknik

<table>
<tr><td colspan="2">UNIVERSITAS DIPONEGORO</td><td>SPMI-UNDIP/RPS/S1.SK-FT-UNDIP/063</td><td rowspan="2">Disetujui Oleh

Dekan Fak. Teknik</td></tr>
<tr><td>Revisi ke

1</td><td>Tanggal

5
Juli 2022</td><td>Rencana Pembelajaran Semester</td></tr>
</table>

	UNIVERSITAS DIPONEGORO **FAKULTAS TEKNIK** **DEPARTEMEN TEKNIK KOMPUTER** **PROGRAM SARJANA**	**SPMI-UNDIP/RPS/S1.SK-FT-UNDIP/063**

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	RUMPUN MK	BOBOT		SEMESTER	TANGGAL PENYUSUNAN
Kriptografi	PTSK6709	Umum	**T=3**	**P=0**	**7**	**5 Juli 2022**

OTORISASI/PENGESAHAN	DOSEN PENGEMBANG RPS	Koordinator RMK	KaPRODI

CAPAIAN PEMBELAJARAN	CPL yang dibebankan pada MK	
	CPL 2	Memiliki kompetensi keilmuan dan keahlian di bidang teknik komputer dan bidang terkait lainnya yang menunjang profesionalitas kerja, baik secara individu maupun tim, serta kemampuan beradaptasi dan pengembangan diri di lingkungan kerja.
	CPL 3	Memiliki pemahaman keilmuan dan penguasaan keterampilan di bidang teknik komputer, meliputi sistem tertanam dan robotika, jaringan dan keamanan komputer, rekayasa perangkat lunak, multimedia, game, dan kecerdasan buatan yang ditopang oleh profesionalitas, pengetahuan sains dasar dan rekayasa yang kuat.
	CPL 5	Mampu menganalisis permasalahan yang dihadapi secara kritis serta mampu merancang solusi dengan menerapkan metode dan alat yang tepat untuk menghasilkan solusi sistem yang andal berdasarkan eksperimen baku dengan memperhatikan aspek kebutuhan teknis, ekonomis, sosial, hukum, dan kelestarian lingkungan.
	CPL 6	Mampu menyampaikan ide dan gagasannya dengan baik dalam menghadirkan solusi dari suatu permasalahan berdasarkan pemahaman pengetahuan dan penguasaan keahlian yang kuat.
	CPL 7	Mampu menyajikan dan memaparkan hasil pengembangan solusi produk dan sistem dalam naskah akademik, tulisan non-akademik, dan/atau di forum ilmiah dengan baik, efektif, dan runtut sesuai dengan kaidah yang berlaku.
	CPL 8	Mampu menunjukkan kepeloporan dan kepemimpinan dalam tim, menerapkan manajemen proyek dan praktek bisnis dengan strategi komunikasi yang efektif, kerjasama multidisiplin ilmu, dan bertanggung secara profesional dan etika.
	CPMK (Capaian Pembelajaran Mata Kuliah)	

	CPMK 2-1	Mampu untuk belajar secara mandiri untuk mengembangkan kemampuan baik di bidang teknik komputer atau di bidang terkait lainnya
	CPMK 2-2	Mampu mengidentifikasikan konsep teoritis di bidang teknik komputer untuk berbagai permasalahan komputasi, jaringan komputer, dan perangkat keras
	CPMK 3-4	Mampu menerapkan aspek-aspek keamanan untuk komputer server dan jaringan komputer dengan berdasarkan best practice yang ada
	CPMK 5-1	Mampu untuk menggunakan tahapan-tahapan penelitian untuk menawarkan solusi pada suatu domain permasalahan, terutama di bidang teknik computer
	CPMK 5-2	Mampu menerapkan prinsip-prinsip legalitas, etika, sosial, dan kelestarian lingkungan dalam merancang suatu solusi, terutama di bidang teknik computer
	CPMK 6-1	Mampu mengkomunikasikan ide dan gagasan dengan memperhatikan aspek komunikasi yang baik
	CPMK 6-2	Mampu menggunakan berbagai perangkat lunak yang ada untuk membantu mempresentasikan ide dan gagasan
	CPMK 7-1	Mampu mengkomunikasikan ide dan gagasan secara tertulis dengan memperhatikan kaedah-kaedah penulisan ilmiah
	CPMK 7-2	Mampu untuk memaparkan secara detail solusi atau produk yang dibuat
	CPMK 8-1	Mampu untuk bekerja dalam kelompok dengan menerapkan prinsip 'ing ngarsa sung tuladha', 'ing madya mangun karsa', 'tut wuri handayani'
	CPMK 8-2	Mampu menerapkan praktik manajemen proyek untuk pengembangan produk atau solusi dengan baik
	CPMK 8-3	Mampu untuk membangun komunikasi dengan berbagai stakeholder untuk pengembangan produk
Deskripsi Singkat	Mata kuliah ini membahas tentang arti kriptografi dan tujuan dari kriptografi; kriptografi kunci publik dan kriptografi kunci rahasia; algoritma-algoritma kriptografi klasik; Block Cipher; fast exponentiation; RSA; Rabin-Williams Cryptosystem; El Gamal Encryption; Data Encryption Standard (DES); Advanced Encryption Standard (AES); Hash function dan MD5; Kriptografi dan e-commerce; dan Steganografi	
Bahan Kajian Materi Pembelajaran	1. Pendahuluan tentang kriptografi, kriptografi kunci rahasia dan kunci public 2. Algoritma Kriptografi Klasik 1 (Caesar Cipher, Vigenere Cipher, Matrix Encryption, dan Vernam Cipher) 3. Algoritma Kriptografi Klasik 2 (Sandi Affine, Sandi Hill, Sandi One-Time Pad, Sandi Rotor) 4. Block Cipher (ECB, CBC, CFB, OFB, dan Feistel Cipher) 5. Enkripsi RSA (Rivest-Shamir-Adleman), pembangkitan kunci, dan dekripsinya 6. Enkripsi El-Gamal dan Rabin-Williams Cryptosystem 7. Data Encryption Standard (DES) 8. Advanced Encryption Standard (AES) 9. Steganografi: Sejarah dan Teknik-tekniknya 10. Kriptografi dan Fungsi Hash Satu Arah (One-way Hash) 11. Algoritma Message Digest-5 (MD5) 12. Kriptografi dan E-Commerce 1 (Kontrak Digital, tanda tangan digital, dan Blind Signature) 13. Kriptografi dan E-Commerce 2 (Sertifikat Digital dan Pembayaran Menggunakan Kartu Kredit) 14. Keamanan Data dan Komputer; Kapita Selekta Kriptografi	

Pustaka		**1. Menezes, A.J., P.C. van Oorschot, and S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, 1996. 2. Pfleeger, C.P., Security in Computing, 2nd ed., Prentice-Hall International, Inc., New Jersey, 1997 3. Schneider, B. Applied Cryptography, John Wiley & Sons, New York, 1994. 4. Tanenbaum, A.S., Jaringan Komputer (Edisi Indonesia Dari Computer Network) Edisi III, Prenhallindo, Jakarta, 1997 5. Sentot Kromodimoeljo, Teori dan Aplikasi Kriptografi, SPK IT Consulting, 2009**				
Pengampu		**Team Pengajar Kriptografi**				
Prasyarat		**-**				
Media Pembelajaran		**Papan Tulis, LCD Projector, Laptop, dan Power Point**				
Mg ke-	**Sub-CPMK (sebagai kemampuan akhir yang diharapkan)**	**Penilaian**	**Bentuk pembelajaran; Metode Pembelajaran; Penugasan; [Estimasi Waktu]**		**Materi Pembelajaran**	**Bobot (%)**
		Indikator, Kriteria, dan Bentuk	**Tatap Muka/Luring**	**Daring**		
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**
1	Mahasiswa dapat menjelaskan definisi tentang kriptografi, enkripsi, dekripsi, kriptografi kunci publik dan kriptografi kunci rahasia paling sedikit 80% tepat.	• Dapat menjelaskan definisi kriptografi • Dapat menyebutkan dan mengartikan istilah-istilah dalam kriptografi: plainteks, cipherteks, enkripsi, dan dekripsi • Dapat menjelaskan konsep kunci dalam kriptografi, baik kunci publik maupun kunci rahasia	• Ceramah • Diskusi 3x50		Kontrak Perkuliahan; Pendahuluan tentang Kriptografi; Kriptografi Kunci Rahasia dan Kunci Publik	
2	Mahasiswa dapat mengerjakan soal-soal algoritma kriptografi klasik: *Caesar cipher*, *playfair, matrix encrypt-ion*, *vigenere cipher,* dan	• Dapat mengerjakan soal-soal tentang algoritma kriptografi klasik: Caesar cipher; Playfair; Matrix Encryption, Vigenere Cipher, dam Vernam Cipher	• Ceramah • Diskusi • Latihan soal 3x50		Algoritma Kriptografi Klasik 1 (Caesar Cipher, Vigenere Cipher, Matrix Encryption, dan Vernam Cipher)	

	vernam cipher					
3	Mahasiswa dapat mengerjakan soal-soal algoritma kriptografi klasik: Sandi *Affine*, Sandi Hill, Sandi *One-Time Pad*, dan Sandi Rotor	• Dapat mengerjakan soal-soal tentang algoritma klasik: Sandi Affine, Sandi Hill, Sandi One-Time Pad, dan Sandi Rotor.	• Ceramah • Latihan soal • Diskusi 3x50		Algoritma Kriptografi Klasik 2 (Sandi Affine, Sandi Hill, Sandi One-Time Pad, Sandi Rotor)	
4	Mahasiswa dapat menjelaskan dan mengerjakan soal-soal tentang *Block Cipher*: ECB, CBC, CFB, OFB, dan *Feistel Cipher* paling sedikit 80% tepat.	• Dapat menjelaskan perbedaan antara block cipher dan stream cipher • Dapat mengerjakan enkripsi dari algoritma-algoritma Block Cipher: *Block Cipher*: Electronic Codebook (ECB);Cipher Block Chaining (CBC); Cipher Feedback Mode (CFB); Output Feedback (OFB)dan Feistel Cipher	• Ceramah • Diskusi • Latihan soal • Simulasi 3x50		Block Cipher (ECB, CBC, CFB, OFB, dan Feistel Cipher)	
5	Mahasiswa dapat menjelaskan dan mengerjakan soal-soal tentang *Fast Exponentiation* dan algoritma RSA paling sedikit 80% tepat.	• Dapat menyelesaikan persoalan-persoalan berkaitan dengan *fast exponentiation* • Dapat mengerjakan soal-soal yang berkaitan dengan Algoritma RSA: Konversi plainteks menjadi angka; Pembangkitan kunci dengan RSA; Enkripsi dengan RSA, dan Dekripsi dengan RSA	• Ceramah • Simulasi • Diskusi • Latihan soal 3x50		Enkripsi RSA (Rivest-Shamir-Adleman), pembangkitan kunci, dan dekripsinya	

6	Mahasiswa dapat mengerjakan soal-soal yang berhubungan dengan algoritma El-Gamal Encryption dan Rabin Williams Cryptosystem paling sedikit 80% tepat.	• Dapat menyelesaikan soal-soal yang berkaitan dengan algoritma El Gamal Encryption, dari aspek pembangkitan kunci, enkripsi, dan dekripsi. • Dapat menyelesaikan soal-soal yang berkaitan dengan algoritma Rabin-Williams Cryptosystem dari aspek: pembangkitan kunci, replika bit, konversi biner ke desimal dan sebaliknya; enkripsi; dan dekripsi.	• Simulasi • Diskusi • Ceramah 3x50		Enkripsi El-Gamal dan Rabin-Williams Cryptosystem	
7	Mahasiswa dapat menjelaskan konsep tentang algoritma Data Encryption Standard (DES) paling sedikit 80% tepat.	• Dapat menyelesaikan soal-soal yang berkaitan dengan algoritma DES • Dapat memahami dan mengerjakan soal berkaitan dengan permutasi, ekspansi, dan substitusi pada DES • Dapat menjelaskan mengenai aspek keamanan pada DES	• Simulasi • Diskusi • Ceramah 3x50		Data Encryption Standard (DES)	
8	**UTS**					
9	Mahasiswa dapat menjelaskan konsep dan mengerjakan soal-soal tentang algoritma Advanced Encryption Standard (AES-Rijndael) paling sedikit 80% tepat	• Dapat menyelesaikan soal-soal yang berkaitan dengan algoritma AES-Rijndael • Dapat memahami dan mengerjakan soal berkaitan dengan pembangkitan kunci, ShiftRows, dam MixColumns pada AES • Dapat menjelaskan mengenai aspek keamanan pada AES.	• Simulasi • Diskusi • Ceramah 3x50		Advanced Encryption Standard (AES)	

10	Mahasiswa dapat menjelaskan dan mengerjakan soal-soal tentang Steganografi paling sedikit 80% tepat.	• Dapat memahami hubungan antara digital watermark dan steganografi • Dapat menjelaskan Aplikasi steganografi dalam keamanan data digital • Dapat memahami konsep dan fungsi, serta dapat mengerjakan soal-soal yang berkaitan penyembunyian data pada steganografi dan teknik pengungkapan datanya.	Contextual instruction 3x50		Steganografi: Sejarah dan Teknik-tekniknya	
11	Mahasiswa dapat menjelaskan konsep dan mengerjakan soal-soal tentang Fungsi Hash satu arah paling sedikit 80% tepat.	• Dapat memahami mengenai Fungsi Hash satu arah • Memahami arti dan Tujuan Fungsi Hash • Dapat menjelaskan aspek keamanan Fungsi Hash	• Simulasi • Diskusi • Ceramah • Cooperative Learning 3x50		Kriptografi dan Fungsi Hash Satu Arah (One-way Hash)	
12	Mahasiswa dapat menjelaskan konsep dan mengerjakan soal-soal tentang Message Digest 5 (MD5) paling sedikit 80% tepat.	• Dapat memahami mengenai Fungsi Message Digest 5 (MD5) • Memahami arti dan Tujuan MD5 • Dapat menjelaskan aspek keamanan MD5 • Dapat mengerjakan soal-soal yang berkaitan dengan Enkripsi dengan Algoritma MD5	• Simulasi • Diskusi • Ceramah • Cooperative Learning 3x50		Algoritma Message Digest-5 (MD5)	
13	Mahasiswa dapat menjelaskan dan mengerjakan soal-soal tentang aplikasi kriptografi dalam e-Commerce paling sedikit 80% tepat.	• Dapat memahami hubungan antara Kripto-grafi dan *e-Commerce* • Dapat menjelaskan Aplikasi kriptografi dalam *e-commerce* • Dapat memahami konsep dan fungsi, serta dapat mengerjakan soal-soal yang berkaitan dengan Tanda tangan digital, tanda tangan buta, Kontrak Digital, Sertifikat Digital, *dan* Protokol SET untuk transaksi dengan kartu kredit	Contextual Instruction 3x50		Kriptografi dan E-Commerce 1 (Kontrak Digital, tanda tangan digital, dan Blind Signature)	

14	Mahasiswa dapat menjelaskan dan mengerjakan soal-soal tentang aplikasi kriptografi dalam e-Commerce paling sedikit 80% tepat.	• Dapat memahami hubungan antara Kripto-grafi dan *e-Commerce* • Dapat menjelaskan Aplikasi kriptografi dalam *e-commerce* Dapat memahami konsep dan fungsi, serta dapat mengerjakan soal-soal yang berkaitan dengan Tanda tangan digital, tanda tangan buta, Kontrak Digital, Sertifikat Digital, *dan* Protokol SET untuk transaksi dengan kartu kredit	Contextual Instruction 3x50		Kriptografi dan E-Commerce 2 (Sertifikat Digital dan Pembayaran Menggunakan Kartu Kredit)	
15	Mahasiswa dapat menjelaskan dan mengerjakan soal-soal tentang Keamanan Data Digital paling sedikit 80% tepat.	• Dapat memahami dan menganalisis aspek-aspek Keamanan Data Digital • Dapat menjelaskan topik-topik terkini dalam keamanan data digital • Memahami garis-garis besar Kapita Selekta Kriptografi • Dapat menganalisis masa depan keamanan data digital dan kriptografi	Problem based learning. 3x50		Keamanan Data dan Komputer; Kapita Selekta Kriptografi	
16	**UAS**					