	UNIVERSITAS SAM RATULANGI **FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM** **PROGRAM STUDI SISTEM INFORMASI**			
RENCANA PEMBELAJARAN SEMESTER (RPS)				
Nama Mata Kuliah	Kode Mata Kuliah	Bobot (sks)	Semester	Tanggal Penyusunan
ANALISIS KEAMANAN INFORMASI DAN KRIPTOGRAFI	**SIS 3472**	2(2-0)	VI	
Otorisasi	Nama Koordinator Pengembang RPS	Koordinator Bidang Keahlian (Jika Ada)		Korprodi
	Winsy Weku			Altien J.Rindengan

Capaian Pembelajaran (CP)	**CPL-PRODI (Capaian Pembelajaran Lulusan Program Studi) Yang DibebankanPada Mata Kuliah**	
	S8	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri;
	S12	Menginternalisasi prinsip-prinsip belajar sepanjang hayat, literasi data, literasi teknologi, literasi manusia, dan mampu memahami tanda-tanda revolusi industri 4.0
	KU1	Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahliannya;
	KU9	Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin kesahihan dan mencegah plagiasi.
	KU10	Mampu melakukan analisis & desain dengan menggunakan kaidah rekayasa software dan hardware serta algoritma dengan cara menggunakan tools dan dapat menunjukkan hasil dan kondisi yang maksimal untuk aplikasi bisnis.
	KU11	Memiliki kemampuan untuk menjadi tenaga professional untuk pengolahan basis data, rekayasa perangkat lunak, jaringan komputer, komputer grafis, dan aplikasi multimedia serta memiliki kemampuan menulis laporan penelitian dengan baik serta mengelola proyek Sistem Informasi, mempresentasikan karya tersebut.
	KK1	Mampu menerapkan matematika dasar, prinsip algoritma, dan teori komputasi dalam pemodelan dan desain sistem berbasis komputer untuk memecahkan masalah nyata dibidang informasi.
	PP1	Menguasai konsep teoritis bidang pengetahuan Sistem Informasi secara umum dan konsep teoritis bagian khusus dalam bidang pengetahuan tersebut secara mendalam, serta mampu memformulasikan penyelesaian masalah prosedural.
	PP3	Mempunyai pengetahuan dalam penyusunan algoritma pemrograman yang efektif dan efisien serta dapat merancang, membangun dan mengelola aplikasi sistem informasi secara tepat dan akurat untuk pendukung pengambilan keputusan.
	CPMK (Capaian Pembelajaran Mata Kuliah)	
		Memahami secara pengertian keamanan, pengertian sistem dan pengertian keamanan sistem, evaluasi keamanan sistem, mengamankan sistem informasi, keamanan email, keamanan web, eksploitasi keamanan sistem, cyber law, keamanan sistem wireless, manajemen keamanan informasi serta metode hacking dan security. Merancang sistem dengan metode keamanan yang telah diajarkan

		Mengenal beberapa jenis algoritma kriptografi klasik dan modern Membuat beberapa jenis algoritma kriptografi sederhana terkait permasalahan sehari-hari
	1.	1. Pengenalan Keamanan Informasi 2. Masalah dalam Keamanan Informasi 3. Tujuan Keamanan Informasi 4. Manajemen Risiko
	2.	Dasar Dasar Keamanan Sistem: Steganografi, Kriptografi, Enkripsi, Kunci Private, kunci public, kombinasi kunci private dan public
	3.	Evaluasi Keamanan Sistem Informasi: Sumber lubang keamanan, Penguji keamanan sistem, Probing services, Penggunaan program penyerang, penggunaan program pemantau jaringan.
	4.	Mengamankan Sistem: Mengatur akses, menutup service yang tidak digunakan,memasang proteksi (Firewall), Pemantau adanya serangan, audit, backup rutin.
	5.	Keamanan Web: 1. Keamanan Server WWW 2. Keamanan Client WWW
	6.	Eksplotasi Keamanan: 1. Technical Vulnerabilities SQL Injection, XSS, Path Traversal, Command Injection, dan lain-lain. 2. Logical Vulnerabilities Value modification, privilege escalation, user impersonation, false account creation, dan lain-lain.
	7.	Keamanan email: Format email, penyadapan, pemalsuan, penyusupan virus, mailbomb, mail relaying.
	8.	Cyber Law Kompetisi Hacking: Capture The Flag
	9.	Manajemen Keamanan Informasi : ISO 27001 dan ISO 27002
	10	Kriptografi dan aplikasinya di kehidupan sehari-hari
	11	Beberapa jenis algoritma kriptografi klasik
	12	Cipher yang tak dapat dipecahkan
	13	Steganografi dan watermarking
	14	Beberapa jenis algoritma kriptografi modern: RSA dan Knapsack
Deskripsi Singkat Mata Kuliah	Materi kuliah mencakup pengertian keamanan, pengertian sistem dan pengertian keamanan sistem, evaluasi keamanan sistem, mengamankan sistem informasi, keamanan email, keamanan web, eksploitasi keamanan sistem, cyber law, keamanan sistem wireless, manajemen keamanan informasi serta metode hacking dan security.	

	Kemudian diberikan materi tentang kriptografi dan serangan terhadap kriptografi, beberapa jenis algoritma kriptografi klasik, cipher yang tidak dapat dipecahkan, steganografi dan watermarking, algoritma kriptografi modern, algoritma simetri, Data Encryption Standard, Advanced Encryption Standard, sistem kriptografi kunci-publik, algoritma RSA dan Knapsack	
Bahan Kajian/Materi Pembelajaran	1.	Dasar-dasar Keamanan Sistem
	2.	Evaluasi Keamanan Sistem Informasi
	3.	Mengamankan Sistem
	4.	Keamanan Web
	5.	Eksploitasi Keamanan
	6.	Keamanan email
	7.	Cyber Law
	8.	Manajemen Keamanan Informasi
	9.	Kriptografi dan aplikasinya di kehidupan sehari-hari
	10.	Beberapa jenis algoritma kriptografi klasik
	11.	Cipher yang tak dapat dipecahkan
	12.	Steganografi dan watermarking
	13.	Beberapa jenis algoritma kriptografi modern: RSA dan Knapsack
	14.	Kriptografi dan aplikasinya di kehidupan sehari-hari
	15.	Beberapa jenis algoritma kriptografi klasik
	16.	Cipher yang tak dapat dipecahkan
Daftar Referensi	Utama	
	1.	Digdo, Girindro Pringgo. 2012. Analisis Serangan dan Keamanan pada Aplikasi Web. Jakarta: Elex Media Komputindo.
	2.	Grossman, Jeremiah; Robert Hansen; Petko D.Petkov; Anton Rager; Seth Fogie. 2007. XSS Attacks: Cross Site Scripting Exploits and Defense. Burlington: Syngress Publishing, Inc.
	3.	Munir, R., *Kriptografi*, Penerbit Informatika, 2006.
	4.	Stinson, R., *Cryptography, Theory and Practice*, 3rd ed, Chapman and Hall, London
	5.	Rahardjo, Budi. 1999. Keamanan Sistem Informasi Berbasis Web. Bandung: PT Insan Infonesia
	6.	Clarke, Justin. 2009.SQL Injection Attacks and Defense . Burlington: Syngress Publishing, Inc.
	Pendukung	
	1.	
	2.	
Nama Dosen Pengampu	Winsy Weku	
Mata KuliahPrasyarat (jikaada)	Kalkulus Struktur Aljabar Matematika Diskrit	

Matriks Pembelajaran :

Minggu	Kemampuan akhir yang diharapkan (sub CPMK)	Bahan Kajian/Materi Pembelajaran	Bentuk & Metode Pembelajaran	Estimasi Waktu (Menit)	Tugas Mahasiswa	Penilaian		Bobot Nilai (%)
						Kriteria & Bentuk	Indikator	
1	• Memahami keamanan informasi dan masalahnya • Memahami dasar-dasar keamanan sistem	1. Pengenalan Keamanan Informasi 2. Masalah dalam Keamanan Informasi 3. Tujuan Keamanan Informasi 4. Manajemen Risiko Dasar Dasar Keamanan Sistem: Steganografi, Kriptografi, Enkripsi, Kunci Private, kunci public, kombinasi kunci private dan public	Bentuk : kuliah Metode: Diskusi	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: mendengarkan penjelasan dosen tentang kontrak perkuliahaan Pascakelas: Menyusun ringkasan dan mengunggah pada modul e-learning	Memahami Kesepakatan Dosen dengan Mahasiswa	- Keaktifan dalam diskusi kelompok - Kualitas ringkasan hasil kajian perorangan	
2	• Mengevaluasi keamanan sistem informasi	Evaluasi Keamanan Sistem Informasi: Sumber lubang keamanan, Penguji keamanan sistem, Probing services, Penggunaan program penyerang, penggunaan program pemantau jaringan. Mengamankan Sistem: Mengatur	Bentuk : kuliah Metode: Diskusi	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mendiskusikan permasalahan yang sudah disusun dosen dalam kelompok kecil Diskusi kelas Pascakelas: Menyusun ringkasan dan mengunggah pada modul e-learning	- Hasil ringkasan diskusi	- Keaktifan dalam diskusi kelompok - Kualitas ringkasan hasil kajian perorangan	5

		akses, menutup service yang tidak digunakan,memasang proteksi (Firewall), Pemantau adanya serangan, audit, backup rutin.						
3	• Memahami keamanan web	Keamanan Web: 1. Keamanan Server WWW 2. Keamanan Client WWW	Bentuk : kuliah Metode : Diskusi	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas:Mendiskusikan dan menyimpulkan masalah/tugas yang diberikan dosen secara kelompok Pascakelas: Menyusun ringkasan dan mengunggah pada modul e-learning	- Hasil tugas kelompok	- Keaktifan dalam diskusi kelompok - Hasil tugas kelompok	5
4	• Memahami eksploitas keamanan	Eksplotasi Keamanan: 1. Technical Vulnerabilities SQL Injection, XSS, Path Traversal, Command Injection, dan lain-lain. 2. Logical Vulnerabilities Value modification, privilege escalation, user impersonation, false account creation, dan lain-lain.	Bentuk : kuliah Metode : Diskusi	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: mendiskusikan permasalahan yang sudah disusun dosen dalam kelompok kecil Diskusi kelas Pascakelas:Menyusun ringkasan dan mengunggah pada modul e-learning	- Hasil tes formatif	- Keaktifan dalam diskusi kelompok - Hasil tes formatif perorangan	5
5	• Memahami keamanan email	Keamanan email: Format email, penyadapan, pemalsuan, penyusupan virus,	Bentuk : kuliah Metode : Diskusi	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: mendiskusikan permasalahan yang sudah disusun dosen dalam kelompok kecil	- Hasil tes formatif	- Keaktifan dalam diskusi kelompok - Hasil tes formatif perorangan	5

		mailbomb, mail relaying.			Pascakelas: Menyusun ringkasan dan mengunggah pada modul e-learning			
6	• Memahami cyber law dan kompetisi hacking	Cyber Law Kompetisi Hacking: Capture The Flag	Bentuk : kuliah Metode : Diskusi	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mengerjakan proyek yg dirancang secara sistematis Pascakelas: Membuat proyek dan mengunggah pada modul e-learning	- Hasil laporan proyek	- Kualitas hasil laporan proyek	5
7	• Memahami manajemen keamanan informasi	Manajemen Keamanan Informasi : ISO 27001 dan ISO 27002	Bentuk : kuliah Metode : Diskusi dan Project Based Learning	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mendiskusikan permasalahan yang sudah disusun dosen dalam kelompok kecil Pascakelas: Menyusun ringkasan dan mengunggah pada modul e-learning	- Hasil tes formatif	- Keaktifan dalam diskusi kelompok - Hasil tes formatif perorangan	5
8	• Kemampuan memahami beberapa terminology dalam kriptografi: sender, receiver, plaintext, ciphertext, cryptogram, enkripsi, dekripsi, kunci • Kemampuan mengetahui sejarah dan aplikasi kriptografi serta kegunaan kriptografi dalam kehidupan sehari-hari	• Beberapa terminology: sender, receiver, plaintext, ciphertext, cryptogram, enkripsi, dekripsi, kunci • Sejarah dan aplikasi kriptografi, kegunaan kriptografi • Kriptografi dalam kehidupan sehari-hari • Beberapa jenis serangan terhadap	Bentuk : kuliah Metode : Diskusi dan Project Based Learning	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mengerjakan proyek yg dirancang secara sistematis Pascakelas: Menyusun ringkasan dan mengunggah pada modul e-learning	- Hasil laporan proyek	- Kualitas hasil laporan proyek	10

	• Kemampuan memahami jenis-jenis serangan terhadap kriptografi, metode penyadapan • Kemampuan memahami kompleksitas serangan serta pentingnya keamanan algoritma kriptografi	kriptografi: exhaustive attack dan analytical attack • Metode penyadapan, kompleksitas serangan • Keamanan algoritma kriptografi						
9	• Kemampuan memahami dan menggunakan konsep Bblangan bulat, pembagi bersama terbesar, algoritma Euclid, prima relative serta kekongruenan • Kemampuan memahami Chinese Remainder Problem • Kemampuan mengaitkan Modulo aritmetika dengan kriptografi • Kemampuan memahami Teorema Fundamental Aritmetika dan Teorema Fermat • Kemampuan mengenal dan membedakan	• Bilangan bulat, pembagi bersama terbesar, algoritma Euclid, prima relative, kekongruenan • Chinese Remainder Problem • Modulo aritmetika dan kriptografi • Teorema Fundamental Aritmetika dan Teorema Fermat • Beberapa jenis algoritma kriptografi klasik: cipher substitusi, cipher transposisi • Menerka plainteks dari cipherteks	Bentuk : kuliah Metode : Diskusi dan Project Based Learning	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mengerjakan proyek yg dirancang secara sistematis Pascakelas: membuat proyek dan mengunggah pada modul e-learning	- Hasil laporan proyek	- Kualitas hasil laporan proyek	10

	beberapa jenis algoritma kriptografi klasik: cipher substitusi, cipher transposisi • Kemampuan menerka plainteks dari cipherteks							
10	• Kemampuan memahami bahwa terdapat cipher yang tak dapat dipecahkan dan mengetahui cara pembuatan cipher tersebut • Kemampuan mengenal salah satu cipher yang tak dapat dipecahkan: One-time Pad dan mengetahui kelemahannya • Kemampuan memahami steganografi dan sejarahnya, kriterianya, teknik penyembunyian data, ukuran data yang disembunyikan, teknik ekstraksi data	• Cipher yang tak dapat dipecahkan • One-time Pad dan kelemahannya • • Steganografi dan sejarahnya, kriterianya, teknik penyembunyian data, ukuran data yang disembunyikan, teknik ekstraksi data	Bentuk : kuliah Metode : Diskusi dan Project Based Learning	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mengerjakan proyek yg dirancang secara sistematis Pascakelas: membuat proyek dan mengunggah pada modul e-learning	- Hasil laporan proyek	- Kualitas hasil laporan proyek	10
11	• Kemampuan memahami watermarking dan	• Watermarking dan sejarahnya, beberapa jenis watermarking,	Bentuk : kuliah	TM:2x50 PT:2x60	Prakelas: mempelajari modul dalam e-learning	- Hasil laporan proyek	- Kualitas hasil laporan proyek	10

	sejarahnya, beberapa jenis watermarking, penyisipan watermarking, verifikasi watermarking • Kemampuan membedakan steganografi dengan watermarking • Kemampuan membuat steganografi atau watermarking sederhana • Kemampuan mengenal algoritma kriptografi modern: memahami cipher aliran dan beberapa serangan terhadap cipher aliran • Kemampuan memahami cipher blok, dan teknik kriptografi klasik yang digunakan dalam cipher blok • Kemampuan memahami dan menggunakan prinsip penyandian Shannon	penyisipan watermarking, verifikasi watermarking • Beda steganografi dengan watermarking • Algoritma kriptografi modern: tipe dan mode algoritma simetri: cipher aliran dan beberapa serangan terhadap cipher aliran • Cipher blok, dan teknik kriptografi klasik yang digunakan dalam cipher blok • Prinsip penyandian Shannon • Mode operasi cipher blok	Metode : Diskusi dan Project Based Learning	BM:2x60	Kelas: Mahasiswa mengerjakan proyek yg dirancang secara sistematis Pascakelas: membuat proyek dan mengunggah pada modul e-learning			

	• Kemampuan memahami mode operasi cipher blok							
12	• Kemampuan mengenal konsep Data Encryption Standard, skema global dan keamanannya • Kemampuan memahami konsep permutasi, pembangkitan kunci internal • Kemampuan melakukan enchipering, permutasi terakhir dan dekripsi • Kemampuan memahami Advanced Encryption Standard • Kemampuan memahami Algoritma Rijndael • Kemampuan menentukan panjang kunci dan ukuran blok Rijndael	• Data Encryption Standard, skema global dan keamanannya • Permutasi, pembangkitan kunci internal • Enchipering, permutasi terakhir dan dekripsi • Advanced Encryption Standard • Panjang kunci dan ukuran blok Rijndael, Algoritma Rijndael	Bentuk : kuliah Metode : Diskusi dan Project Based Learning	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mengerjakan proyek yg dirancang secara sistematis Pascakelas: membuat proyek dan mengunggah pada modul e-learning	- Hasil laporan proyek	- Kualitas hasil laporan proyek	10
13	• Kemampuan mengenal sistem kriptografi kunci-publik	• Sistem kriptografi kunci-publik • Kriptografi simetri dan kriptografi asimetri	Bentuk : kuliah Metode : Diskusi dan Project Based Learning	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mengerjakan proyek yg dirancang secara sistematis	- Hasil laporan proyek	- Kualitas hasil laporan proyek	10

	• Kemampuan membedakan kriptografi simetri dan kriptografi asimetri • Kemampuan mengenal algoritma RSA, property dan perumusan algoritma RSA, • Kemampuan membuat algoritma membangkitkan pasangan kunci dan algoritma enkripsi/dekripsi • Kemampuan mengetahui keamanan algoritma RSA	• Aplikasi kriptografi kunci-publik • Algoritma RSA, property dan perumusan algoritma RSA, • Algoritma membangkitkan pasangan kunci • Algoritma enkripsi/dekripsi • Keamanan RSA			Pascakelas: membuat proyek dan mengunggah pada modul e-learning			
14	• Kemampuan mengenal algoritma ElGamal, property dan perumusan algoritma ElGamal, • Kemampuan membuat algoritma membangkitkan pasangan kunci, dan algoritma enkripsi/dekripsi • Kemampuan mengetahui keamanan Algoritma ElGamal	• Algoritma ElGamal, property dan perumusan algoritma ElGamal, • Algoritma membangkitkan pasangan kunci • Algoritma enkripsi/dekripsi • Keamanan Algoritma ElGamal • Algoritma Knapsack • Superincreasing Knapsack	Bentuk : kuliah Metode : Diskusi dan Project Based Learning	TM:2x50 PT:2x60 BM:2x60	Prakelas: mempelajari modul dalam e-learning Kelas: Mahasiswa mengerjakan proyek yg dirancang secara sistematis Pascakelas: membuat proyek dan mengunggah pada modul e-learning	- Hasil laporan proyek	- Kualitas hasil laporan proyek	10

	• Kemampuan memahami algoritma Knapsack dan mengenal superincreasing Knapsack • Kemampuan membuat algoritma Knapsack Kunci-publik sederhana	• Algoritma Knapsack Kunci-publik • Implementasi Knapsack						