



STMIK HANDAYANI MAKASSAR
FAKULTAS KOMPUTER
JURUSAN/PROGRAM STUDI SISTEM KOMPUTER

RENCANA PEMBELAJARAN SEMESTER (RPS)

NAMA MATA KULIAH	KODE MK	Rumpun MK	BOBOT (sks)	SEMESTER	Tgl Penyusunan
Pengamanan Sistem Komputer	KB033636	Matakuliah Wajib	3	3	
OTORISASI	Nama Koordinator Pengembang RPS		Koordinator RMK	Ka PRODI	
Mata Kuliah : Keamanan Komputer	Semester: 4		SKS: 3		
Mata Kuliah Pra Syarat					
Program Studi : Sistem Komputer	Dosen Pengembang RPS : Matalangi, S.Kom., M.Kom				
Capaian Pembelajaran Lulusan (CPL)	<ol style="list-style-type: none">1. Memiliki integritas dan komitmen yang tinggi terhadap kecendikiaan dan profesi (CP-U3)2. Mampu menerapkan konsep-konsep yang berkaitan dengan arsitektur dan organisasi komputer (CP-KKD)3. Merancang sistem jaringan komputer serta pengolahan secara kontinu (CP-KKC1)				
Capaian Pembelajaran Mata Kuliah (CPMK)	<ol style="list-style-type: none">1. Mahasiswa memiliki pengetahuan dan pemahaman tentang arti penting keamanan komputer dan jaringan dalam menjaga aset informasi (CP-KKC2)2. Mahasiswa memahami tentang prinsip dasar dan cara kerja suatu sistem yang aman pada komputer dan jaringan (CP-KKC2)3. Mahasiswa memahami tentang cryptographi dan cryptosystem yang merupakan salah satu teknik dalam keamanan komputer dan jaringan (CP-KKC2)4. Mahasiswa mengerti dan dapat menerapkan beberapa teknik Cryptography dasar dalam program aplikasi (CP-KKB3)5. Mahasiswa dapat mengidentifikasi program berbahaya dan dapat melakukan penanganan dalam menghadapi gangguan (CP-KKB3)6. Memahami beberapa aspek di luar sistem yang dapat menyebabkan gangguan keamanan (CP-KKC2)7. Mahasiswa memahami dasar keamanan pada sistemjaringan dan dapat mengidentifikasi gangguan (CP-KKC2)8. Mahasiswa memahami cara kerja dan dapat memiliki pengetahuan sistem operasi yang baik dari segi keamanan (CP-KKC2)9. Mahasiswa dapat mengevaluasi, mendefinisikan penyebab dan menangan masalah keamanan komputer dan jaringan (CP-KKC2)				

		<p>10. Mahasiswa memahami cara mengamankan dan melakukan pemulihan data (CP-KKC2)</p> <p>11. Mahasiswa mengerti tentang kode etik profesi TI dan dapat menerapkan dalam profesinya penggiat TI (CP-KKA3)</p> <p>12. Mahasiswa paham mengenai perundang-undang TI dan menjaga untuk tidak melanggarnya (CP-KKA3)</p>
Deskripsi Mata Kuliah		Mengenai permasalahan-permasalahan yang menyangkut keamanan suatu sistem komputer dan cara-cara mengatasinya
Materi Pembelajaran		<ol style="list-style-type: none"> 1. Pendahuluan keamanan komputer dan kejahatan komputer 2. Prinsip dasar keamanan komputer 3. Cryptosystem dan Cryptography 4. Teknik Cryptography 5. Devil program 6. Keamanan komputer secara fisik 7. Keamanan jaringan 8. Keamanan sistem informasi 9. Evaluasi keamanan sistem informasi 10. Keamanan database dan teknik pemulihan data 11. Kode etik profesi TI 12. Perspektif Cyber Law dan UU ITE
Daftar Pustaka	Utama:	Cryptography and Network Security Principles and Practice, William Stallings, Pearson Education
	Tambahan:	Diktat dan Handout Keamanan Komputer. Tim Dosen STMIK Handayani Makassar

Minggu ke	Kemampuan yang diharapkan (Sub CP-MK)	Bahan Kajian/ Materi Pembelajaran	Metode Pembelajaran	Waktu	Pengalaman Belajar Mahasiswa	Indikator, Kriteria, dan Bentuk Penilaian	Bobot/Nilai
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	<ul style="list-style-type: none"> Mahasiswa memiliki pengetahuan dan pemahaman tentang arti penting keamanan komputer dalam menjaga aset informasi 	Pendahuluan keamanan dan kejahatan komputer <ul style="list-style-type: none"> Faktor kebutuhan keamanan komputer Penyebab meningkat kejahatan komputer Klasifikasi keamanan dan karakteristik penyusup Fase seorang hacker Aspek keamanan komputer 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi membahas mengenai kasus umum yang pernah dihadapi 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah Keamanan komputer Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> Kuis 	5%
2	<ul style="list-style-type: none"> Mahasiswa memahami tentang prinsip dasar dan cara kerja suatu sistem yang aman pada komputer dan jaringan 	Prinsip dasar keamanan dan kejahatan komputer <ul style="list-style-type: none"> Security Model Attact Kasus keamanan komputer Cara Hacker bekerja Prinsip dasar perancangan sistem yang aman Lapisan keamanan 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi dan berdiskusi mengenai suatu kasus dan pemecahan masalah 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah prinsip dasar keamanan komputer Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> Kuis 	5%
3	<ul style="list-style-type: none"> Mahasiswa memahami tentang cryptographi dan cryptosystem yang 	Cryptosystem dan Cryptography <ul style="list-style-type: none"> Jenis-jenis 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 	<ul style="list-style-type: none"> Berinteraksi dan berdiskusi mengenai suatu kasus dan 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah 	5%

Minggu ke	Kemampuan yang diharapkan (Sub CP-MK)	Bahan Kajian/ Materi Pembelajaran	Metode Pembelajaran	Waktu	Pengalaman Belajar Mahasiswa	Indikator, Kriteria, dan Bentuk Penilaian	Bobot/Nilai
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	merupakan salah satu teknik dalam keamanan komputer	cryptosystem <ul style="list-style-type: none"> Fungsi Protokol Cryptosystem Jenis penyerangan protokol dan jalur komunikasi Pengenalan dasar cryptography 		120 menit <ul style="list-style-type: none"> BM; 2x60 = 120 menit 	pemecahan masalah	Cryptography Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> Kuis 	
4-6	<ul style="list-style-type: none"> Mahasiswa mengerti dan dapat menerapkan beberapa teknik cryptography dasar dalam program aplikasi 	Teknik Cryptography metode klasik <ul style="list-style-type: none"> Teknik mono/poly Alphabet Block, karakter, zigzag Kode vigenere Teknik transposisi One time pad 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi dan diskusi Memberi pelatihan contoh dan kasus 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menerapkan metode cryptography Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> Latihan soal dan kasus 	20%
7	<ul style="list-style-type: none"> Mahasiswa dapat mengidentifikasi program berbahaya dan dapat melakukan penanganan dalam menghadapi gangguan 	Devil Program <ul style="list-style-type: none"> Keamanan devil program Tipe-tipe program jahat Siklus hidup virus Klasifikasi tipe virus Generasi perkembangan antivirus 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi dan diskusi 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah Devil program Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> kuis 	10%
8	UJIAN TENGAH SEMESTER						
9	<ul style="list-style-type: none"> Mahasiswa memahami beberapa aspek diluar sistem 	Keamanan jaringan <ul style="list-style-type: none"> Jaringan lokal Jaringan internet 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 	<ul style="list-style-type: none"> Berinteraksi dan diskusi 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah 	5%

Minggu ke	Kemampuan yang diharapkan (Sub CP-MK)	Bahan Kajian/ Materi Pembelajaran	Metode Pembelajaran	Waktu	Pengalaman Belajar Mahasiswa	Indikator, Kriteria, dan Bentuk Penilaian	Bobot/Nilai
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	yang dapat menyebabkan gangguan	email		120 menit • BM; 2x60 = 120 menit		keamanan fisik Kriteria: • Ketepatan dan penguasaan masalah Bentuk Penilaian: • Kuis	
10	<ul style="list-style-type: none"> Mahasiswa memahami dasar keamanan pada sistem jaringan dan dapat mengidentifikasi gangguan 	Keamanan jaringan <ul style="list-style-type: none"> Jaringan lokal Jaringan internet email 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi dan diskusi 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah keamanan jaringan Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> Kuis 	10%
11	<ul style="list-style-type: none"> Mahasiswa memahami cara kerja dan dapat memiliki pengetahuan sistem operasi yang baik dari segi keamanan 	Keamanan sistem operasi <ul style="list-style-type: none"> access control Security Architecture dan model Prinsip dan tingkat jaminan keamanan System architecture security Keamanan sistem operasi linux dan winNt 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi dan diskusi Melakukan simulasi 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah Sistem operasi dan keamanannya Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> Kuis dan pemberian tugas 	20%
12	<ul style="list-style-type: none"> Mahasiswa dapat mengevaluasi, mendefinisikan penyebab dan 	Evaluasi keamanan sistem informasi <ul style="list-style-type: none"> Penyebab masalah keamanan 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi dan diskusi 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah keamanan database 	5%

Minggu ke	Kemampuan yang diharapkan (Sub CP-MK)	Bahan Kajian/ Materi Pembelajaran	Metode Pembelajaran	Waktu	Pengalaman Belajar Mahasiswa	Indikator, Kriteria, dan Bentuk Penilaian	Bobot/Nilai
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	menangani masalah keamanan komputer dan jaringan	<ul style="list-style-type: none"> • Sumber lubang keamanan • Probing service dan OS fingerprinting • Penggunaan program penyerang • Penggunaan sistem pemantau jaringan 		<ul style="list-style-type: none"> • BM; 2x60 = 120 menit 		<p>Kriteria:</p> <ul style="list-style-type: none"> • Ketepatan dan penguasaan masalah <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> • Kuis 	
13	<ul style="list-style-type: none"> • Mahasiswa memahami cara mengamankan dan melakukan pemulihan data 	<p>Keamanan database dan teknik pemulihan data</p> <ul style="list-style-type: none"> • keamanan database keamanan data dan teknik pemulihan data 	<ul style="list-style-type: none"> • Problem based learning 	<ul style="list-style-type: none"> • TM; 2x50 = 100 menit • BT; 2x60 = 120 menit • BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> • Berinteraksi dan diskusi 	<p>Indikator:</p> <ul style="list-style-type: none"> • Kemampuan dalam menjelaskan masalah keamanan database <p>Kriteria:</p> <ul style="list-style-type: none"> • Ketepatan dan penguasaan masalah <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> • Kuis 	5%
14	<ul style="list-style-type: none"> • Mahasiswa mengerti tentang kode etik profesi IT dan dapat menerapkan dalam profesinya sebagai penggiat IT 	<p>Kode Etik profesi IT</p> <ul style="list-style-type: none"> • Etika keamanan komputer • Isu dalam etika komputer • Pelanggaran kode etik profesi IT • Peran perkembangan ilmu pengetahuan dan teknologi • Contoh kasus dalam etika komputer dan 	<ul style="list-style-type: none"> • Problem based learning 	<ul style="list-style-type: none"> • TM; 2x50 = 100 menit • BT; 2x60 = 120 menit • BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> • Berinteraksi dan diskusi 	<p>Indikator:</p> <ul style="list-style-type: none"> • Kemampuan dalam menjelaskan masalah kode Etik <p>Kriteria:</p> <ul style="list-style-type: none"> • Ketepatan dan penguasaan masalah <p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> • Kuis 	5%

Minggu ke	Kemampuan yang diharapkan (Sub CP-MK)	Bahan Kajian/ Materi Pembelajaran	Metode Pembelajaran	Waktu	Pengalaman Belajar Mahasiswa	Indikator, Kriteria, dan Bentuk Penilaian	Bobot/Nilai
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
		teknologi					
15	<ul style="list-style-type: none"> Mahasiswa paham mengenai perundang-undang IT dan menjaga untuk tidak melanggarnya 	Perspektif cyber law dan UU ITE <ul style="list-style-type: none"> Perundangan dan pemanfaatan teknologi informasi Implementasi hukum ITE indonesia Isi UU ITE dan manfaatnya Masalah dan tantangan penerapan UU ITE indonesia 	<ul style="list-style-type: none"> Problem based learning 	<ul style="list-style-type: none"> TM; 2x50 = 100 menit BT; 2x60 = 120 menit BM; 2x60 = 120 menit 	<ul style="list-style-type: none"> Berinteraksi dan diskusi 	Indikator: <ul style="list-style-type: none"> Kemampuan dalam menjelaskan masalah UU ITE Kriteria: <ul style="list-style-type: none"> Ketepatan dan penguasaan masalah Bentuk Penilaian: <ul style="list-style-type: none"> Kuis 	5%
16	UJIAN AKHIR SEMESTER						