



UNIVERSITAS HASANUDDIN

FAKULTAS TEKNIK

PROGRAM STUDI TEKNIK INFORMATIKA – S1

RENCANA PEMBELAJARAN SEMESTER

Mata Kuliah (MK)	KODE	Rumpun MK	Bobot (sks)	SEMESTER	Tgl Penyusunan
Keamanan Digital	23D12121303	Teknik Informatika	3	4	

OTORITAS

Dosen Pengembang RPS

Koordinator MK

Ketua Prodi

Dr. Eng. Ady Wahyudi Paundu, ST., MT.

Dr. Eng. Ady Wahyudi Paundu, ST., MT.

Prof. Dr. Ir. Indrabayu, S.T., M.T., M.Bus.Sys., IPM., ASEAN.Eng.

Capaian Pembelajaran Mata Kuliah

CPL-PRODI yang dibebankan pada MK

- CPL-1:** Memiliki dasar pengetahuan Teknik Informatika yang meliputi teori dan konsep dasar dari Ilmu Komputer, Matematika dan Statistika, Algoritma dan Pemrograman, Rekayasa Perangkat Lunak, Manajemen Informasi dan Ketahanan Digital, serta pengetahuan tingkat lanjut pada bidang-bidang khusus Teknik Informatika, seperti Kecerdasan Buatan, Data Science, Jaringan Komputer, Komputasi Awan dan Internet of Things. (IK 1.1)
- CPL-3:** Mampu menganalisis permasalahan komputasi yang kompleks, melibatkan banyak komponen dan tingkat risiko, dengan menerapkan prinsip komputasi, komunikasi, dan desain, serta mengintegrasikan pengetahuan dari bidang ilmu lain yang relevan untuk mengidentifikasi solusi yang tepat. (IK 3.1, 3.2)
- CPL-8:** Mampu mengikuti dinamika perkembangan Teknologi Informasi serta menghormati keberagaman perspektif, budaya, ide, dan karya orisinal dalam praktik komputasi. (8.1)

CPL ⇒ Capaian Pembelajaran Mata Kuliah (CPMK)

Setelah menyelesaikan mata kuliah ini, diharapkan:

- CPL-1:** **CPMK-1.1** : Setelah mengikuti Mata Kuliah Keamanan Digital selama 1 (satu) semester, mahasiswa mampu menunjukkan kemampuan untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital serta mampu mendesiminasi pengetahuan dasar-dasar prinsip keamanan digital keluar kelas Mata Kuliah untuk memberikan dampak kepada masyarakat.
- CPL-3:** **CPMK-3.1** : Setelah mengikuti Mata Kuliah Keamanan Digital selama 1 (satu) semester, mahasiswa mampu menunjukkan kemampuan melakukan analisis serta melakukan prosedur logis dan sistematis untuk mengidentifikasi, mencari solusi, serta menyelesaikan suatu masalah terseleksi dalam topik keamanan digital.
- CPL-8:** **CPMK-8.1** : Setelah mengikuti Mata Kuliah Keamanan Digital selama 1 (satu) semester, mahasiswa mampu menunjukkan kemampuan mengenali perkembangan terbaru dari kemajuan teknologi keamanan digital serta menunjukkan sikap apresiasi terhadap karya orisinal dalam bidang keamanan digital.

CPMK ⇒ Sub-CPMK

- CPMK-1.1** **SUB-CPMK-1.1.1:** Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (IK 1.1)
- SUB-CPMK-1.1.2:** Mahasiswa mampu mendesiminasi pengetahuan dasar-dasar prinsip keamanan digital ke masyarakat (IK 1.1)
- CPMK-3.1** **SUB-CPMK-3.1.1:** Mahasiswa mampu menganalisis suatu masalah terseleksi dalam topik keamanan digital untuk mendapatkan solusi. (IK 3.1)
- SUB-CPMK-3.1.2:** Mahasiswa mampu mendemonstrasikan kemampuan melakukan prosedur logis dan sistematis untuk menyelesaikan suatu masalah terseleksi dalam topik keamanan digital. (IK 3.2)
- CPMK-8.1** **SUB-CPMK-8.1.1:** Mahasiswa mampu melaporkan isu terbaru dalam topik keamanan digital, baik dalam bentuk perkembangan terbaru dari kemajuan teknologi keamanan digital maupun berbagai ancaman keamanan yang terbaru. (IK.8.1)
- SUB-CPMK-8.1.2:** Mahasiswa mampu menunjukkan sikap apresiasi terhadap karya orisinal dalam bidang keamanan digital. (IK 8.1)

Korelasi antara CPL/CPMK terhadap Sub-CPMK

CPL yang
dibebankan
pada MK

CPMK	SUB CPMK	Bentuk Asesmen*		Bobot	Nilai	Skor Mahasiswa
		Formative	Sumative			
			Tugas	Hasil Project		
CPL-1	CPMK-1.1	SUB-CPMK-1.1.1	15	0	15	
CPL-1	CPMK-1.1	SUB-CPMK-1.1.2	20	10	30	
CPL-3	CPMK-3.1	SUB-CPMK-3.1.1	0	20	20	
CPL-3	CPMK-3.1	SUB-CPMK-3.1.2	0	20	20	
CPL-8	CPMK 8.1	SUB-CPMK-8.1.1	10	0	10	
CPL-8	CPMK-8.1	SUB-CPMK-8.1.2	5	0	5	

		50	50	100
Deskripsi Matakuliah	Mata kuliah Keamanan Internet merupakan mata kuliah wajib 3 SKS yang diberikan pada semester IV. Aspek keamanan digital merupakan sebuah bahan kajian yang sangat luas karena berhubungan dengan seluruh aspek teknologi informasi (IT), sehingga mata kuliah ini diarahkan pada pengenalan dasar secara meluas berbagai aspek keamanan digital. Pengenalan mendalam terhadap topik-topik khusus keamanan digital diberikan pada mata kuliah pilihan di semester-semester selanjutnya, seperti M.K. Forensik Digital dan M.K. Kriptografi. Penanggungjawab mata kuliah adalah Laboratorium Ubicon (Ubiquitous Computing & Networks). Metode pembelajaran bauran berbasis teori dan praktek. Pelaksanaan mata kuliah di Ruang Kelas dan Laboratorium Komputer Laboratorium Ubicon Departemen Teknik Informatika Fakultas Teknik Unhas di Gowa. Luaran dari Mata Kuliah ini adalah portofolio kemampuan mahasiswa, baik dalam bentuk sertifikat industri, video presentasi, code repository, serta kegiatan yang berdampak langsung pada masyarakat.			
	Materi Pembelajaran/Pokok Bahasan	<ul style="list-style-type: none"> - Keamanan digital dalam perspektif pengguna awam - Fungsi-fungsi dalam keamanan digital - Prinsip dasar desain keamanan digital - Otentikasi sistem digital - Otorisasi sumberdaya digital - Metode kriptografi dan kriptanalisis - Mekanisme keamanan aplikasi dan data - Mekanisme keamanan sistem operasi - Mekanisme keamanan jaringan komputer dan infrastruktur komputasi - Mekanisme deteksi intrusi - Mekanisme forensik digital - Konsep Resiliensi - Keamanan rekayasa sosial - Regulasi dan etika keamanan komputer - Isu privasi - Manajemen operasi keamanan digital - Pengorganisasian operasi keamanan digital pada skala organisasi, regional dan internasional - Pemanfaatan alat bantu perangkat lunak dalam operasi keamanan digital - Sertifikasi dalam profesi keamanan digital - Side Channel Attack - Isu keamanan digital terbaru 		
Referensi	Referensi Utama			
[1] William Stallings and Lawrie Brown, 2019, Computer Security: Principles and Practice, 4th ed, Pearson Education Inc. ISBN 978-9-35-343886-9				
Tim Pengajaran	Referensi Tambahan			
	Internet			
Mata Kuliah Syarat	<ul style="list-style-type: none"> - Dr. Eng. Ady Wahyudi Paundu, ST., MT., - Muhammad Aryandi, S.T., M.Kom. - Sistem Digital - Algoritma dan Struktur Data - Arsitektur dan Organisasi Komputer 			

Pertemuan Ke-	Sub CPMK (Kemampuan akhir tiap tahapan belajar)	Penilaian (Assesment)		Bentuk dan Metode Pembelajaran [estimasi waktu] (Learning Method)		Materi Pembelajaran (Content)	Bobot Penilaian (%)
		Indikator (Indicator)	Teknik & Kriteria (Techniques & Criteria)	Luring (Offline System)	Daring (Online System)		
1	2	3	4	5	6	7	8
1	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Formative: Tidak ada Sumative: - mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital.	Kriteria Formative: Kriteria Sumative: Tugas (5) dinilai dengan rubrik 23D121 Teknik Penilaian: Tes	Kuliah: Self-Directed Learning, Metode lainnya 3*50		Keamanan Digital 101 - Ruang lingkup topik keamanan digital (KD) - CIA - Arti penting KD - Situasi terkini seputar topik KD - KD dalam sudut pandang pengguna awam Penjelasan RPS Penjelasan Tugas-Tugas Penjelasan Aturan Perkuliahan	5
2	Mahasiswa mampu mendesiminasi pengetahuan dasar-dasar prinsip keamanan digital ke masyarakat. (SUB-CPMK 1.1.2)	Formative: Tidak ada Sumative: - mendesiminasi pengetahuan dasar-dasar prinsip keamanan digital ke masyarakat.	Kriteria Formative: Kriteria Sumative: Tugas (20) dinilai dengan rubrik 23D121 Teknik Penilaian: Laporan (Tertulis dan Video)	Kuliah: Presentasi 3*50		Fungsi dan Desain - Fungsi-fungsi utama dalam sistem KD - Prinsip dasar desain sistem KD Diskusi Security Awareness Campaign Project	20
3	Mahasiswa mampu mendemonstrasikan	Formative:	Kriteria Formative:	Kuliah:		Otentikasi - Otorisasi - Akunting - Macam-macam metode otentikasi	0

	kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Tidak ada Sumative: Tidak ada	Kriteria Sumative: Teknik Penilaian:	Self-Directed Learning, Metode lainnya 3*50	<ul style="list-style-type: none"> - Tantangan keamanan metode otentikasi - Macam-macam metode otorisasi - Tantangan keamanan metode otorisasi - Use-case framework: Federated Authentication 	
4	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	Kriptografi <ul style="list-style-type: none"> - Taksonomi kriptologi - Kriptografi simetris vs asimetris - Kriptografi berbasis block vs stream - Arti penting prinsip Kerckhoff - Dasar Aritmetika Modular - Pengenalan kriptanalisis dan implementasinya pada kriptografi tradisional Monitoring dan Deteksi 	0
5	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	IDS <ul style="list-style-type: none"> - Pendekatan analisis (signature, heuristic, anomaly-based) - IDS Tools/Frameworks (honeypots, snorts, ...) - IPS 	0
6	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Formative: Tidak ada	Kriteria Formative: Kriteria Sumative:	Kuliah: Self-Directed Learning, Metode	Konsep Resiliensi <ul style="list-style-type: none"> - Backup - Redundansi - Incident Response - Business Continuity Plan 	0

	permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Sumative: Tidak ada		lainnya 3*50	- Testing and Metrics	
7	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Tugas (5) Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	Forensik Digital - Definisi dan tujuan forensik digital - Pengenalan dasar fase- fase operasi forensik - Pengenalan kebutuhan standar operasi - Pengenalan beberapa kategori forensik digital (host, os, network, multimedia, mobile)	5
8	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	Keamanan Aplikasi dan Data - Beberapa bentuk serangan umum pada aplikasi komputer/web/basisdata - prinsip dasar pencegahannya - Pengenalan tool untuk mempelajari bentuk serangan aplikasi web	0
9	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Tugas (5) Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	Keamanan Sistem Operasi - Beberapa bentuk serangan umum pada sistem operasi - prinsip dasar pencegahannya (hardening) - Perawatan keamanan pada OS - Keamanan pada sistem virtual	5

10	keamanan digital. (SUB-CPMK 1.1.1)					
	Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	Keamanan Infrastruktur Komputasi dan Jaringan Komputer - review sistem jaringan komputer, teknik enkapsulasi dan data pada header - konsep-konsep umum pengamanan jarkom - Protokol komunikasi untuk keamanan jarkom (IPSec, SSL, HTTPS, dll) - Beberapa bentuk serangan umum pada jarkom dan pencegahannya	0
11	Mahasiswa mampu melaporkan isu terbaru dalam topik keamanan digital, baik dalam bentuk perkembangan terbaru dari kemajuan teknologi keamanan digital maupun berbagai ancaman keamanan yang terbaru. (SUB-CPMK 8.1.1)	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Tugas (10) Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	Social Engineering - Pengenalan Social Engineering - Pengenalan berbagai bentuk SocEng - Beberapa saran pencegahan Aspek Etika dan Privasi - Beberapa tipe kejahatan komputer - Konsep Intellectual Property - Konsep privasi - Isu-isu etika Riset Social Engineering	10
12	Mahasiswa mampu menunjukkan sikap apresiasi terhadap karya orisinal dalam bidang keamanan digital (SUB-CPMK 8.1.2)	Formative: Tidak ada Sumative: Tidak ada	Kriteria Formative: Kriteria Sumative: Tugas (5) Teknik Penilaian:	Kuliah: Self-Directed Learning, Metode lainnya 3*50	Aspek Aturan dan Manajemen - Pengenalan konsep manajemen dan kebijakan sistem KD - Arti penting manajemen resiko (dalam konteks KD) - Contoh prosedur operasional sistem KD - keamanan fisik dalam sistem KD Governance - Sistem Governance	5

					<ul style="list-style-type: none"> - Standards 	
					Alat Bantu (Tools)	
					<ul style="list-style-type: none"> - Pengenalan konsep sistem Security Information and Event Management (SIEM) - Pengenalan sistem bantu keamanan digital yang umum digunakan, baik yang Open Source maupun yang proprietary 	
13	<p>Mahasiswa mampu mendemonstrasikan kemampuan melakukan analisis dan memberikan solusi terhadap suatu permasalahan terseleksi dalam fungsi keamanan digital untuk mendapatkan pengakuan kompetensi dari pihak industri bidang keamanan digital. (SUB-CPMK 1.1.1)</p>	<p>Formative:</p> <p>Tidak ada</p> <p>Sumative:</p> <p>Tidak ada</p>	<p>Kuliah:</p> <p>Self-Directed Learning, Metode lainnya</p> <p>3*50</p>		Side Channel Attack	0
14	<p>Mahasiswa mampu menganalisis suatu masalah terseleksi dalam topik keamanan digital untuk mendapatkan solusi. (SUB-CPMK 3.1.1)</p>	<p>Formative:</p> <p>Tidak ada</p> <p>Sumative:</p> <p>- mendesain sebuah Intrusion Detection System sederhana</p>	<p>Kriteria Formative:</p> <p>Kriteria Sumative:</p> <p>Presentasi (20) dinilai dengan rubrik 23D121</p> <p>Teknik Penilaian:</p> <p>Presentasi</p>	<p>Kuliah:</p> <p>Presentasi</p> <p>2*3*50</p>	Presentasi Project IDS	20
15	<p>Mahasiswa mampu mendemonstrasikan kemampuan melakukan prosedur logis dan sistematis untuk menyelesaikan suatu</p>	<p>Formative:</p> <p>Tidak ada</p>	<p>Kriteria Formative:</p> <p>Kriteria Sumative:</p> <p>Presentasi (20) dinilai</p>	<p>Kuliah:</p> <p>Presentasi</p> <p>2*3*50</p>	Presentasi Isu Terbaru Keamanan Digital (termasuk topik-topik riset Keamanan Digital)	20

16	masalah terseleksi dalam topik keamanan digital.	Sumative:	dengan rubrik 23D121			
	(SUB-CPMK 3.1.2)	- mempresentasikan isu keamanan digital terbaru	Teknik Penilaian:	Presentasi		
	Mahasiswa mampu mendesiminasi pengetahuan dasar-dasar prinsip keamanan digital ke masyarakat	Formative:	Kriteria Formative:	Kuliah:	Presentasi laporan tugas cybersecurity awareness program	10
	(SUB-CPMK 1.1.2)	Tidak ada	Kriteria Sumative:	Presentasi		
		Sumative:	Presentasi (10) dinilai dengan rubrik 23D121	2*3*50		
	-mempresentasikan laporan cybersecurity awareness program	Teknik Penilaian:	Presentasi			