Mata Kuliah (MK)	Nama MK	: Keamanan Informasi dan Kriptografi
	Kode MK	: EE185536
	Kredit	: 2 sks
	Semester	: (MK Pilihan)

Deskripsi Mata Kuliah

Dengan semakin pesatnya perkembangan jaringan komunikasi dan internet dan semakin luasnya penggunaan perangkat serta data yang terhubung ke jaringan, tantangan terhadap keamanan informasi dan jaringan semakin penting. Pada mata kuliah ini mahasiswa akan mempelajari permasalahan keamanan dan teknik untuk mengatasinya dari dua aspek, yaitu aspek teori informasi dan aspek komputasi atau kriptografi. Secara khusus akan dasar teori informasi, kapasitas keamanan, keamanan efektif, pengkodean yang aman, pembangkitan kunci rahasia, teori bilangan dan finite field teknik-teknik kriptografi, baik simetrik dan asimetrik, serta algoritma-algoritma untuk melindungi integritas data.

CPL Prodi yang Dibebankan

PENGETAHUAN

(P01) Menguasai konsep dan prinsip keilmuan secara komprehensif, dan untuk mengembangkan prosedur dan strategi yang diperlukan untuk analisis dan perancangan sistem terkait bidang keahlian Teknik Sistem Tenaga, Teknik Sistem Pengaturan, Telekomunikasi Multimedia, Teknik Elektronika, Jaringan Cerdas Multimedia, atau Telematika sebagai bekal untuk pendidikan lanjut atau karir profesional.

KETERAMPILAN KHUSUS

(KK01) Mampu memformulasikan permasalahan rekayasa dengan ide-ide baru untuk pengembangan teknologi dalam bidang keahlian Teknik Sistem Tenaga, Teknik Sistem Pengaturan, Telekomunikasi Multimedia, Teknik Elektronika, Jaringan Cerdas Multimedia, atau Telematika.

KETERAMPILAN UMUM

(KU11) mampu mengimplementasikan teknologi informasi dan komunikasi dalam konteks pelaksanaan pekerjaannya.

SIKAP

(S09) Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri.

Capaian Pembelajaran Mata Kuliah

PENGETAHUAN

Menguasai tantangan dan konsep keamanan pada sistem komunikasi dan jaringan untuk distribusi data dari aspek teori informasi dan aspek komputasi, serta teknik-teknik berbasis kriptografi untuk mengatasi permasalahan keamanan dan melindungi integritas data.

KETERAMPILAN KHUSUS

Mampu menjelaskan prinsip dari keamanan lapisan fisik dan mengimplementasika pembangkitan kunci rahasia dan menjelaskan teknik-teknik kriptografi simetrik dan asimetrik serta penerapannya untuk mengatasi permasalahan keamanan pada sistem komunikasi dan jaringan.

KETERAMPILAN UMUM

Mampu menggunakan perangkat lunak dan tool untuk mengimplementasikan teknik-teknik kriptografi dan simulasi sistem keamanan di jaringan, misal Matlab dan ns-3.

SIKAP

Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri.

Topik/Pokok Bahasan

1. Pengantar tentang konsep keamanan pada sistem komunikasi dan jaringan
2. Dasar teori informasi dan keamanan lapisan fisik
3. Kapasitas keamanan
4. Pembangkitan kunci rahasia
5. Dasar-dasar teori bilangan
6. Block Cipher dan Data Encryption Standard (DES)
7. Dasar-dasar finite field
8. Advanced Enryption Standard (AES)
9. Kriptografi kunci publik dan RSA
10. Keamanan jaringan nirkabel

Pustaka

[1] William Stallings, “Cryptography and Network Security: Principles and Practice,” 7th ed., Pearson, 2017.

[2] Jonathan Katz & Yehuda Lindell, “Introduction to Modern Cryptography,” 2nd ed., CRC Press, 2015.

[3] Rafael F. Schaefer, Holger Boche, Ashish Khisti, & H. Vincent Poor, “Information Theoretic Security and Privacy of Information Systems,” Cambridge University Press, 2017.

Prasyarat

--

Rencana Pembelajaran Semester
Prodi Magister Departemen Teknik Elektro
Fakultas Teknologi Elektro
INSTITUT TEKNOLOGI SEPULUH NOPEMBER

1	**Kode & Nama**	:	EE185536 Keamanan Informasi dan Kriptografi
2	**Kredit**	:	2 sks
3	**Semester**	:	
4	**Dosen**	:	Wirawan
5	**Deskripsi Mata Kuliah**	:	Dengan semakin pesatnya perkembangan jaringan komunikasi dan internet dan semakin luasnya penggunaan perangkat serta data yang terhubung ke jaringan, tantangan terhadap keamanan informasi dan jaringan semakin penting. Pada mata kuliah ini mahasiswa akan mempelajari permasalahan keamanan dan teknik untuk mengatasinya dari dua aspek, yaitu aspek teori informasi dan aspek komputasi atau kriptografi. Secara khusus akan dasar teori informasi, kapasitas keamanan, keamanan efektif, pengkodean yang aman, pembangkitan kunci rahasia, teori bilangan dan finite field teknik-teknik kriptografi, baik simetrik dan asimetrik, serta algoritma-algoritma untuk melindungi integritas data.
6	**CPL Prodi yang Dibebankan**	:	PENGETAHUAN (P01) Menguasai konsep dan prinsip keilmuan secara komprehensif, dan untuk mengembangkan prosedur dan strategi yang diperlukan untuk analisis dan perancangan sistem terkait bidang keahlian Teknik Sistem Tenaga, Teknik Sistem Pengaturan, Telekomunikasi Multimedia, Teknik Elektronika, Jaringan Cerdas Multimedia, atau Telematika sebagai bekal untuk pendidikan lanjut atau karir profesional. KETERAMPILAN KHUSUS (KK01) Mampu memformulasikan permasalahan rekayasa dengan ide-ide baru untuk pengembangan teknologi dalam bidang keahlian Teknik Sistem Tenaga, Teknik Sistem Pengaturan, Telekomunikasi Multimedia, Teknik Elektronika, Jaringan Cerdas Multimedia, atau Telematika. KETERAMPILAN UMUM (KU11) mampu mengimplementasikan teknologi informasi dan komunikasi dalam konteks pelaksanaan pekerjaannya. SIKAP (S09) Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri.

7	**Capaian Pembelajaran Mata Kuliah**	:	PENGETAHUAN Menguasai tantangan dan konsep keamanan pada sistem komunikasi dan jaringan untuk distribusi data dari aspek teori informasi dan aspek komputasi, serta teknik-teknik berbasis kriptografi untuk mengatasi permasalahan keamanan dan melindungi integritas data. KETERAMPILAN KHUSUS Mampu menjelaskan prinsip dari keamanan lapisan fisik dan mengimplementasika pembangkitan kunci rahasia dan menjelaskan teknik-teknik kriptografi simetrik dan asimetrik serta penerapannya untuk mengatasi permasalahan keamanan pada sistem komunikasi dan jaringan. KETERAMPILAN UMUM Mampu menggunakan perangkat lunak dan tool untuk mengimplementasikan teknik-teknik kriptografi dan simulasi sistem keamanan di jaringan, misal Matlab dan ns-3. SIKAP Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri.
8	**Tahapan Capaian Pembelajaran**	:	PENGETAHUAN 1. Menguasai permasalahan dan konsep keamanan pada sistem komunikasi dan jaringan 2. Menguasai prinsip keamanan lapis fisik dari aspek teori informasi 3. Menguasai konsep kapasitas keamanan 4. Menguasai konsep dan implementasi pembangkitan kunci secara rahasia 5. Menguasai dasar-dasar teori bilangan 6. Menguasai prinsip penghitungan block cipher dan DES 7. Menguasai dasar-dasar finite field 8. Menguasai struktur dan penghitungan AES 9. Menguasai prinsip kriptografi asimetrik dengan kunci publik 10. Menguasai permasalahan keamanan pada jaringan nirkabel dan teknik-teknik untuk mengatasi KETERAMPILAN 1. Mampu menjelaskan permasalahan dan konsep keamanan pada sistem komunikasi dan jaringan 2. Mampu menjelaskan prinsip keamanan lapis fisik dari aspek teori informasi 3. Mampu menjelaskan konsep kapasitas keamanan 4. Mampu menjelaskan konsep dan mengimplementasikan pembangkitan kunci secara rahasia 5. Mampu menghitung algoritma pembagian bilangan bulat, menjelaskan aritmatika modular dan algoritma Euclidean

			6. Mampu menjelaskan prinsip blok cipher dan DES, serta menghitung enkripsi terkait 7. Mampu menjelaskan group, ring dan field serta mampu melakukan penghitungan pada GF(p) 8. Mampu menjelaskan prinsip dan struktur AES serta menghitung enkripsi terkait 9. Mampu menjelaskan konsep dan prinsip kriptografi asimetrik dengan kunci publik 10. Mampu menjelaskan permasalahan keamanan pada jaringan nirkabel dan teknik-teknik untuk mengatasi
9	**Topik/Pokok Bahasan**	:	1. Pengantar tentang konsep keamanan pada sistem komunikasi dan jaringan 2. Dasar teori informasi dan keamanan lapisan fisik 3. Kapasitas keamanan 4. Pembangkitan kunci rahasia 5. Dasar-dasar teori bilangan 6. Block Cipher dan Data Encryption Standard (DES) 7. Dasar-dasar finite field 8. Advanced Enryption Standard (AES) 9. Kriptografi kunci publik dan RSA 10. Keamanan jaringan nirkabel
10	**Pustaka**	:	[1] William Stallings, "*Cryptography and Network Security: Principles and Practice*," 7th ed., Pearson, 2017. [2] Jonathan Katz & Yehuda Lindell, "*Introduction to Modern Cryptography*," 2nd ed., CRC Press, 2015. [3] Rafael F. Schaefer, Holger Boche, Ashish Khisti, & H. Vincent Poor, "*Information Theoretic Security and Privacy of Information Systems*," Cambridge University Press, 2017.
11	**Prasyarat**	:	

No	Capaian Pembelajaran Pokok Bahasan	Materi Pembelajaran	Metode Pembelajaran (Estimasi Waktu)	Asesmen		
				Indikator Capaian Pembelajaran	Pengalaman Belajar*	Bobot (%)
1	Pengantar keamanan pada sistem komunikasi dan jaringan	Permasalahan keamanan pada sistem komunikasi dan jaringan Contoh-contoh kejadian serangan dan teknik-teknik yang dikembangkan	Belajar mandiri (1x3x60 menit) Pembelajaran dalam kelas. (1x3x50 menit) Belajar terstruktur (1x3x60 menit)	Mampu menjelaskan permasalahan keamanan pada sistem komunikasi, pertukaran data dan jaringan Mampu menjelaskan contoh aplikasi penerapan keamanan dan teknik terkait		
2	Teori informasi dan keamanan lapisan fisik	Dasar teori informasi Informasi bersama Komunikasi yang aman pada kanal berderau Keamanan lapisan fisik	Belajar mandiri (2x3x60 menit) Pembelajaran dalam kelas. (2x3x50 menit) Belajar terstruktur (2x3x60 menit)	Mampu menjelaskan aspek teori informasi dari sistem komunikasi yang aman Mampu menjelaskan konsep dan prinsip keamanan lapisan fisik	Tugas 1 Penyelesaian soal	**15%**
3	Kapasitas keamanan	Sistem cipher Shannon Keamanan sempurna, lemah dan kuat Kanal wiretap Wyner Kanal broadcast dengan pesan rahasia	Belajar mandiri (2x3x60 menit) Pembelajaran dalam kelas. (2x3x50 menit) Belajar terstruktur (2x3x60 menit)	Mampu menjelaskan konsep sistem cipher Shannon Mampu menjelaskan konsep keamanan dengan kriteria sempurna, lemah dan kuat Mampu menjelaskan konsep kanal wiretap Wyner	Tugas 2 Penyelesaian soal	**10%**

4	Pembangkitan kunci rahasia	Pembangkitan kunci rahasia Model hirarkis Model seluler	Belajar mandiri (1x3x60 menit) Pembelajaran dalam kelas. (1x3x50 menit) Belajar terstruktur (1x3x60 menit)	Mampu menjelaskan prinsip kerja dan mengimplementasikan pembangkitan kunci rahasia Mampu menjelaskan prinsip pembangkitan dengan model hirarkis dan seluler	Tugas 3 Penyelesaian soal	**15%**
5	Dasar-dasar teori bilangan	Divisibilitas dan algoritma pembagian Algoritma Euclidean Bilangan prima Pengujian primalitas Logaritma diskrit	Belajar mandiri (1x3x60 menit) Pembelajaran dalam kelas. (1x3x50 menit) Belajar terstruktur (1x3x60 menit)	Mampu menghitung algoritma pembagian Mampu menghitung algoritma Euclidean Mampu menghitung logaritma diskrit	Tugas 4 Penyelesaian soal	**10%**
6	Block Cipher dan Data Encryption Standard (DES)	Struktur block cipher dasar Data Encryption Standard dan kekuatannya Prinsip desain block cipher	Belajar mandiri (2x3x60 menit) Pembelajaran dalam kelas. (2x3x50 menit) Belajar terstruktur (2x3x60 menit)	Mampu menjelaskan prinsip dan struktur block cipher Mampu menjelaskan prinsip DES dan menhitung enkripsi DES	Tugas 5 Penyelesaian soal	**10%**
7	Dasar-dasar finite field	Group Ring Field	Belajar mandiri (1x3x60 menit)	Mampu menjelaskan struktur group, ring dan field Mampu menyusun finite field GF(p) dan menghitung operasi pada GF(p)	Tugas 6 Penyelesaian soal	10%

		Finite field dalam bentuk GF(p) Aritmatika polinomial	Pembelajaran dalam kelas. (1x3x50 menit) Belajar terstruktur (1x3x60 menit)	Mampu menghitung aritmatika polinomial		
8	Advanced Enryption Standard (AES)	Struktur AES Fungsi transformasi AES Contoh AES dan implementasinya	Belajar mandiri (2x3x60 menit) Pembelajaran dalam kelas. (2x3x50 menit) Belajar terstruktur (2x3x60 menit)	Mampu menjelaskan prinsip dan struktur AES Mampu menghitung fungsi transformasi pada AES Mampu menjelaskan contoh AES dan implementasinya	Tugas 7 Penyelesaian soal	10%
9	Kriptografi kunci publik dan RSA	Prinsip kriptografi kunci publik Analisa kripto untuk kunci publik Algoritma RSA	Belajar mandiri (1x3x60 menit) Pembelajaran dalam kelas. (1x3x50 menit) Belajar terstruktur (1x3x60 menit)	Mampu menjelaskan prinsip kriptografi kunci publik Mampu menjelaskan prinsip analisa kripto pada kunci publik Mampu menghitung enkripsi dengan algoritma RSA	Tugas 8 Penyelesaian soal	10%
10	Keamanan jaringan nirkabel	Keamanan pada sistem komunikasi dan jaringan nirkabel Perangkat mobile IEEE 802.11i WLAN security	Belajar mandiri (1x3x60 menit) Pembelajaran dalam kelas. (1x3x50 menit) Belajar terstruktur	Mampu menjelaskan tantangan komunikasi dan jaringan nirkabel Mampu menjelaskan permasalahan keamanan pada perangkat mobile Mampu menjelaskan protokol IEEE 802.11i	Tugas 9 Penyelesaian soal	10%

			(1x3x60 menit)			

*) Presentasi, tugas, quiz, praktikum lab