RENCANA PEMBELAJARAN SEMESTER
PROGRAM STUDI TEKNIK INFORMATIKA DAN KOMPUTER
PROGRAM PASCASARJANA S2 TERAPAN

Kode	VI200015	Mata Kuliah	Network Security
Bobot SKS	2	Semester	2, 3, atau 4
Kelompok MK	MK Pilihan (Elective Lecture)	Jam/minggu	2
Tim Pengampu MK	Amang Sudarsono		NoId: RF-DTEL-PSTE-4.05.Rev.01[031]

Capaian Pembelajaran	Mahasiswa mampu membangun pengetahuan dan keahlian dalam keamanan jaringan. Setelah mengikuti kuliah ini, mahasiswa mampu: 1. Secara detil mengerti dasar, prinsip dan praktis tentang sistem kriptografi 2. Mengerti secara global isu-isu dasar yang berhubungan dengan keamanan jaringan 3. Mengerti secara praktis dan analisis tentang pentingnya keamanan jaringan dan aplikasi-aplikasinya seperti Kerberos, X.509 certificate, PGP email security dan settingnya 4. Menganalisis dan mengimplementasikan secara aktual beberapa komponen dasar dari sistem kriptografi 5. Menjelaskan konsep yang berhubungan dengan applied cryptography, termasuk plaintext, ciphertext, symmetric cryptography, asymmetric cryptography, digital signature dan digital certificate. 6. Menjelaskan tentang teori dibalik keamanan jaringan seperti berbagai macam algoritma-algoritma kriptografi 7. Menjelaskan dan analisis tentang kerapuhan/ancaman pada jaringan pada umumnya, mekanisme pertahanan melawan serangan-serangan tersebut, dan mekanisme proteksi kriptografi 8. Mengidentifikasi persyaratan dan mekanisme identification and authentication system 9. Mengidentifikasi kemungkinan serangan untuk masing-masing mekanisme dan solusi untuk memproteksi ancaman tersebut 10. Menjelaskan persyaratan dari keamanan jaringan secara nyata dan isu-isu yang berhubungan dengan keamanan dalam web services 11. Menjelaskan persyaratan dari sistem keamanan non-realtime seperti email security dan cara untuk mendukung privacy, authentication, message integrity, non-repudiation, proof of submission, proof of delivery, message flow confidentiality, dan anonymity
Pokok Bahasan	Mata kuliah ini dirancang untuk membangun kemampuan dasar yang dibutuhkan dalam analisa keamanan terhadap ancaman dan serangan baik internal maupun eksternal dalam jaringan dan membangun policy yang akan digunakan untuk memproteksi aset data dari suatu institusi. Mata kuliah ini akan mengenalkan mahasiswa dalam tantangan-tantangan dan kerapuhan-kerapuhan pada keamanan suatu sistem jaringan komputer. Topik-topik meliputi pembelajaran secara detil dan komprehensif dari keamanan jaringan seperti: 1. dasar keamanan jaringan, 2. kriptografi, baik kriptografi simetris maupun asimetris beserta matematika yang mendasarinya, 3. digital signature dan digital certificate. 4. security di layer network, transport dan aplikasi. 5. disain dan analisis security yang meliputi confidentiality, data integrity, authenicity, non-repudiation, dan anonimity.
Referensi	1. Network Security Essentials Applications and Standards 5th edition William Stallings Prentice Hall 2014 2. William Stallings, Cryptography and Network Security: Principles and Practice, 6/e, Prentice Hall, 2014, 731 pp., ISBN-13: 978-0-13-335469-0

	3. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition. Bruce Schneier. ISBN: 978-0-471-11709-4. 784 pages. November 1995 4. Wireless and Mobile Networks Security Hardcover – October 12, 2009, by Hakima Chaouchi, Maryline Laurent-Maknavicius
MK Prasyarat	1. Advanced Mathematics, Algorithm & Programming 2. Network Management and Security
Media Pembelajaran	Software: Hardware: PC/Laptop, LCD Projector, Papan Tulis
Asesmen (%)	UTS (30 %), UAS (40 %), Tugas (20 %), Sikap (10 %)

Mgg Ke-	Sub Capaian Pembelajaran MK (Kemampuan Akhir Yang Direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk Pembelajaran	Waktu Belajar (menit)	Kriteria Asesmen (Indikator)	Bentuk Asesmen	Bobot
(1)	1) Mahasiswa mampu memahami konsep dasar dari keamanan jaringan dan fungsi penggunaan keamanan pada jaringan komputer 2) Mahasiswa mampu mengidentifikasi dan memahami aplikasi-aplikasi yang menggunakan keamanan jaringan pada era sebelumnya, era modern dan yang akan datang 3) Mahasiswa memahami jenis-jenis serangan dan cara penanggulangannya	○ Pengantar Keamanan Jaringan ○ Struktur dan syarat dasar keamanan: confidentiality, integrity, availability dan jenis serangannya serta security policies, security mechanisms & assurance	Kuliah Pengantar & Brainstorming, Diskusi	TM: 100 menit Tgs: 100 menit BM: 120 menit	○ Mengidentifikasi fungsi penggunaan keamanan jaringan ○ Mengidentifikasi syarat dasar keamanan, jenis serangan dan penanggulangannya	Tugas, penyelesaian soal/studi kasus di kelas	5%
(2,3,4)	1) Menjelaskan dasar kriptografi yang terdiri atas *symmetric cryptography* dan *asymmetric cyptography* 2) Menjelaskan dan analisa tentang symmetric cryptography : Fiestel Cipher, Data Encryption Standard (DES) dan Advanced Encryption Standard (AES) beserta mode operasinya 3) Menjelaskan tentang kerahasiaan data, pembangkitan bilangan acak RND & PRN, *stream cipher* dan *block cipher*	○ Kriptografi simetris: Data Encryption Standard (DES), Advanced Encryption Standard (AES), mode operasi: ECB, CBC, CFB, OFB dan CTR ○ Pengantar kriptografi asimetris ○ RND dan PRN, *Stream Cipher* dan *Cipher Block*	Kuliah, Brainstorming, Diskusi	TM: 300 menit Tgs: 300 menit BM: 360 menit	○ Mengidentifikasi dan memahami kriptografi simetris dan asimetris, serta mode operasinya ○ Mengidentifikasi dan memahami, serta mendisain kriptografi asimetris ○ Mengidentifikasi dan memahami RND, PRN, *stream cipher* dan *cipher block*	Tugas, penyelesaian soal/studi kasus di kelas	15%
(5,6,7)	1) Menjelaskan tentang metode fungsi hash dan *message digest* atau fungsi satu arah 2) Menjelaskan dan analisa tentang mekanisme kerja, algoritma pada *public key cryptography* dan aplikasinya 3) Menjelaskan dan analisa tentang mekanisme kerja, algoritma pada *public key cryptography* variant dari RSA, algoritma alternatif dari RSA dan aplikasinya	○ Strong dan weak collision resistance, Birthday paradox ○ Metode MD5, SHA-1, SHA-256 dan contoh-contoh aplikasinya ○ Dasar matematika: Euclidean algorithm, Euler Theorem, Fermat Theorem, Totent Functions, Multiplicative dan additive inverse	Kuliah, Brainstorming, Diskusi, maju di depan kelas	TM: 300 menit Tgs: 300 menit BM: 360 menit	○ Mengerti, mengidentifikasi dan menyelesaikan metode fungsi hash dan *message digest* atau fungsi satu arah: MD5, SHA-1, SHA-256 ○ Mengerti, mengidentifikasi dan menyelesaikan serta mendisain dan analisis algoritma *public key cryptography*: RSA, Elgamal, dan ECC.	Tugas, penyelesaian soal/studi kasus di kelas	20%

		○ RSA algorithm beserta public dan private keys beserta contoh-contoh aplikasinya dan cara perhitungannya ○ Elgamal algorithm ○ Dasar matematika dan metode Elliptic curve cryptography (ECC) beserta contoh-contoh aplikasinya dan cara perhitungannya					
(8, 10, 11)	1) Menjelaskan tentang proses dan mekanisme pembangkitan key, pembuatan signature, dan verifikasinya 2) Menjelaskan tentang proses autentikasi 3) Menjelaskan dan analisa tentang trusted intermediate, sertifikasi dan distribusi key dan contoh aplikasi penggunaan trusted 3rd party Kerberos	○ Digital signature dan digital certificate: DSA, Elgamal, ECDSA, X.509 certificate ○ Algoritma autentikasi: Diffie-Helman, per-session keys, key distribution centers dan certificate authorities ○ *Public key infrastructure* (PKI), certification authorities dan key distribution center (KDC), Kerberos system	Kuliah, Brainstorming, Diskusi	TM: 300 menit Tgs: 300 menit BM: 360 menit	○ Mengerti, mengidentifikasi, dan menyelesaikan serta analisis algoritma digital signature dan digital certificate: DSA, Elgamal, ECDSA dan X.509 ○ Mengerti, mengidentifikasi, dan menyelesaikan serta analisis algoritma autentikasi: DH dan session key ○ Mengerti, mengidentifikasi dan menyelesaikan serta analisis algoritma PKI, KDC dan Kerberos system	Tugas, penyelesaian soal/studi kasus di kelas	20%
(9)	**Ujian Tengah Semester (UTS)**						
(12)	Menjelaskan dan analisa tentang teknik-teknik keamanan untuk komunikasi secara riil pada layer network	○ Keamanan pada sistem komunikasi (Real-time communication security) pada layer network ○ Metode IPSec: AH dan ESP ○ Metode IPSec: IKE ○ Aplikasi VPN	Kuliah, Brainstorming, Diskusi	TM: 100 menit Tgs: 100 menit BM: 120 menit	○ Mengerti dan mengidentifikasi serta analisis real-time communication security pada layer network ○ Mengerti dan mengidentifikasi serta analisis metode IPSec: AH, ESP dan IKE serte aplikasi VPN	Tugas, penyelesaian soal/studi kasus di kelas	5%
(13)	Menjelaskan dan analisa tentang teknik-teknik keamanan untuk komunikasi secara riil pada layer transport	○ Keamanan pada sistem komunikasi (Real-time communication security) pada layer transport ○ Metode SSL/TLS ○ Metode HTTPS, FTPS dan secure remote protocol: SSH	Kuliah, Brainstorming, Diskusi	TM: 100 menit Tgs: 100 menit BM: 120 menit	○ Mengerti dan mengidentifikasi serta analisis real-time communication security pada layer transport ○ Mengerti dan mengidentifikasi serta analisis metode SSL/TLS, HTTPS, FTPS, dan SSH	Tugas, penyelesaian soal/studi kasus di kelas	5%
(14, 15)	1) Menjelaskan dan analisa tentang keamanan pada jaringan wireless dan selular. Konsentrasi pada	○ Kemanan pada wireless dan mobile networks:	Kuliah, Brainstorming,	TM: 200 menit Tgs: 200 menit	○ Mengerti dan mengidentifikasi serta analisis keamanan pada	Penilaian tugas, penyelesaian	15%

	keamanan pada jaringan wireless 2) Menjelaskan dan analisa tentang keamanan pada jaringan wireless dan selular. Konsentrasi pada keamanan pada jaringan selular	pada jaringan WiFi, IEEE802.11i, IEEE802.1x, IEEE802.11x dan Radius ○ Keamanan pada wireless dan mobile networks: pada jaringan selular dan Internet Multimedia Subsystem (IMS)	Diskusi	BM: 240 menit	jaringan wireless dan mobile. ○ Mengerti dan mengidentifikasi serta analisis keamanan pada jaringan selular: GSM, GPRS, UMTS, WiMax dan IMS	soal/studi kasus di kelas	
(16)	Menjelaskan dan analisa tentang proses dan mekanisme keamanan pada layer aplikasi. Konsentrasi pada electronic mail security	○ Distribution list ○ Establishing key ○ Metode Pretty Good Privacy (PGP) ○ MIME dan S/MIME ○ Email treats	Kuliah, Brainstorming, Diskusi	TM: 100 menit Tgs: 100 menit BM: 120 menit	○ Mengerti dan mengidentifikasi serta analisis proses dan mekanisme keamanan pada layer aplikasi untuk security pada electronic mail	Tugas, penyelesaian soal/studi kasus di kelas	10%
(17)	Menjelaskan dan analisa tentang proses dan mekanisme dari firewall dan web security disertai dengan contoh-contoh aplikasinya	Firewall dan intrusion detection system (IDS)	Kuliah, Brainstorming, Diskusi	TM: 100 menit Tgs: 100 menit BM: 120 menit	○ Mengerti dan mengidentifikasi serta analisis packet filter, encrypted tunnel, cookies, IDS dan password management	Tugas, penyelesaian soal/studi kasus di kelas Tugas akhir semester	5%
(18)	**Ujian Akhir Semester (UAS)**						

Keterangan:
TM : Tatap Muka
Tgs : Tugas
BM : Belajar Mandiri