ITTelkom Surabaya *Solution for The Nation*	**INSTITUT TEKNOLOGI TELKOM SURABAYA** **FAKULTAS TEKNIK ELEKTRO** **PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI**	**Kode Dokumen**

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)		SEMESTER	Tgl Penyusunan
Keamanan Jaringan	TEA40E3	Sistem Jaringan Transmisi Telekomunikasi (SJT)	T=3	P=0	8	27 Maret 2018

OTORISASI	Pengembang RPS	Koordinator RMK	Ketua PRODI
	Nilla Rachmaningrum., S.T., M.T	Nilla Rachmaningrum., S.T., M.T	Hamzah. U. Mustakim S.T., M.T

Capaian Pembelajaran (CP)

CPL-PRODI

- Mempunyai kemampuan untuk menggunakan pengetahuan dasar matematika, sains, dan rekayasa
- Mempunyai kemampuan merancang dan melaksanakan eksperimen, termasuk menganalisis dan menginterpretasikan data secara ilmiah menggunakan metoda ilmiah
- Mempunyai kemampuan merancang suatu sistem, komponen, atau proses untuk memenuhi kebutuhan yang diharapkan dalam batasan-batasan realistis termasuk pengiriman konten broadband melalui metoda rekayasa dibidang telekomunikasi
- Mempunyai keterampilan dalam mengoperasikan perangkat keras, menggunakan aplikasi perangkat lunak dan kemampuan pemrogramannya berkaitan dengan teknologi informasi dan telekomunikasi

CPMK

- Mahasiswa mampu memahami dasar-dasar kriptografi (simetris dan asimetris); menjelaskan bagaimana kriptografi kunci publik dapat digunakan untuk memastikan identitas pengirim pesan terenkripsi
- Mahasiswa mmapu Jelaskan risiko keamanan mengenai integritas data dan sistem ketersediaan di lapisan fisik dan datalink, menjelaskan perbedaan yang signifikan antara keamanan untuk data melalui jaringan publik dan lalu lintas dienkripsi melalui LAN nirkabel
- Mahasiswa mampu membangun model Internet Security dari aliran paket dan titik segmen pandang (jaringan dan transport layer)
- Mahasiswa mampu menjelaskan berbagai cara di mana informasi dapat diproses dalam lapisan aplikasi, mengetahui implikasi keamanan

	• Mahasiswa secara mandiri mampu menganalisis dan memahami bagaimana Jaringan Keamanan Devices (Firewall, IDS / IPS, NAT, Proxy.) Bekerja. Temukan dan mengidentifikasi kelainan dalam jaringan yang disebabkan oleh cacing, virus, Bots dan Jaringan terkait memperlakukan keamanan
Diskripsi Singkat MK	Memberikan pengetahuan mengenai aplikasi praktis keamanan jaringan telekomunikasi secara umum yang dapat dipelajari melalui konsep dasar dan teori kriptografi (simetrik dan asimetrik), contoh standar industri, analisis algoritma pertukaran kunci, pemodelan otentikasi, fungsi one-way dan hash, konsep dan sistem serangan tiap lapisan protokol, sistem pertahanan untuk tujuan keamanan jaringan.
Bahan Kajian / Materi Pembelajaran	1. Kriptografi simetris dan asimetris 2. Caesar dan Vigenere Cryptography 3. Kriptografi DES dan 3DES 4. Algoritma RSA dan serangan man in the middle 5. Mekanisme penggunaan fungsi satu arah untuk hash function.
Pustaka	**Utama :** 1. C. Kaufman, R. Perlman, & M. Speciner, Network Security (Private Communication in a Public World), 2nd ed., Prentice Hall, 2002 2. R. Anderson, Security Engineering (A Guide to Building Dependable Distributed Systems), 2nd ed., John Wiley & Sons, 2008 3. W. Stallings, Cryptography and Network Security, 6th ed., Prentice Hall, 2013 4. Katz, J., Lindell, Y., Introduction to Modern Cryptography, Chapman & Hall, 2008 5. A.J. Menezes, P.C. van Oorschot, & S.A. Vanstone, Handbook of Applied Cryptography, 5th ed., CRC Press, 2001 6. S. Fergueson, Practical Cryptography, John Wiley & Sons, 2003. **Pendukung :** 1. S. Fergueson, Practical Cryptography, John Wiley & Sons, 2003.
Dosen Pengampu	1. Nilla Rachmaningrum., S.T., M.T 2. Hamzah. U. Mustakim S.T., M.T
Matakuliah syarat	Jaringan Komunikasi dan Data

Mg Ke-	Sub-CPMK (Kemampuan akhir tiap tahapan belajar)	Indikator Penilaian	Kriteria & Bentuk Penilaian	Bentuk, Metode Pembelajaran, dan Penugasan Mahasiswa [Media & Sumber belajar] [Estimasi Waktu]	Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1,2,3,4	menjelaskan bagaimana	• mahasiswa	Quiz (Tertulis)	• Tatap Muka	1. Sejarah dan tujuan	30%

	kriptografi kunci publik dapat digunakan untuk memastikan identitas pengirim pesan terenkripsi	dapat menjelaskan dan mengaplikasikan metode enkripsi • Menjelaskan dan mengaplikasikan metode dekripsi • Menyebutkan dan menjelaskan macam-macam attack • Menjelaskan Algoritma Caesar dan Vigenere Cryptography • Menjelaskan Algoritma DES dan 3DES • mahasiswa dapat menjelaskan tentang kriptografi asimetri dan dalam kondisi apa		• Penugasan terstruktur (Latihan soal) [TM: 3x(3x50')]	kriptografi, Permasalahan keamanan dari dahulu sampai sekarang 2. Kebutuhan akan confidentiality,integrity, authority, dan non-repudiasi 3. Aplikasi kriptografi untuk menjawab permasalahan tersebut dengan teknik simetrik, asimetrik, dan hashing (termasuk protokolnya) 4. Terminologi Kripto: Pesan, Cipher, Kunci, Enkripsi dan Dekripsi, serta attack yang mungkin 5. Caesar Cipher, cara kerja enkripsi dan dekripsi, kekurangan 6. Vigenere Cipher, cara kerja, enkripsi dan dekripsi, kekurangan 7. Dua fokus algoritma enkripsi : diffusion and confussion 8. Data Encryption Standard (DES) 9. Mode kerja DES: ECB, CBC 10. Skema Kerja Kriptografi Asimetrik 11. Dasar Matematik 12. RSA 13. Penerapan untuk message confidentiality, authority dan non-repudiasi	

		teknik ini diperlukan • Menjelaskan dasar matematik asymetric cryptography • Mahasiswa dapat memberi contoh cara perhitungan RSA • mahasiswa dalam diskusi dapat ditanya dengan soal-soal singkat sambil diskusi di kelas • Menjelaskan Algoritma RSA dan serangan man in the middle • Menjelaskan macam-macam algoritma pertukaran kunci (beserta			14. Serangan yang mungkin pada kripto asimetrik 15. Challenge and Response 16. Diffie Hellman 17. El Gamal 18. Penerapan untuk authentikasi user 19. Serangan yang mungkin pada pertukaran kunci 20. Prinsip kerja one-way function beserta contoh-contohnya 21. Algoritma hash-function yang ada dan penerapannya 22. Attack pada hash-function: birthday attack	

		penerapannya) dan dapat membedakannya				
5,6,7	Memahami metoda keamanan lapis fisik Memahami jenis serangan pada lapis fisik Mengetahui dan memahami perkembangan network security WEP, WPA dan WPA2	• Mahasiswammapu Jelaskan risiko keamanan mengenai integritas data dan sistem ketersediaan di lapisan fisik dan datalink, menjelaskan perbedaan yang signifikan antara keamanan untuk data melalui jaringan publik dan lalu lintas dienkripsi melalui LAN nirkabel	Quiz (Tertulis)	• Tatap Muka • Penugasan terstruktur (Latihan soal) [TM: 3x(3x50')]	1. RF fingerprinting 2. Denial of service 3. Kriptografi pada Wireless LAN: standard: WEP 4. WPA dan WPA2	**20%**
8	**Evaluasi Tengah Semester / Ujian Tengah Semester**					
9,10	Mengetahui dan	• Mahasiswa	Quiz (Tertulis)	• Tatap Muka	1. IP smurfing 2. Address spoofing	**15%**

	memahami metoda keamanan lapis jaringan Memahami aplikasi dan serangan lain seperti HTTPS, SYN flooding, dll. Mengetahui dan memahami metoda keamanan lapis transpormengukur performansinya	mampu membangun model Internet Security dari aliran paket dan titik segmen pandang (jaringan dan transport layer)		• Penugasan terstruktur (tugas) [TM: 3x(3x50')]	attacks 3. Routing security 4. Protocol design 5. Kriptografi pada jaringan komputer : Protokol SSL, sertifikasi server dan HTTPS 6. SYN flooding, RIP attacks, sequence number prediction 7. Protokol SSL, TLS 8. IPSec key management 9. Access control	
11,12	Mengetahui dan memahami metoda keamanan dan jenis serangan pada lapis sesi Mengetahui dan memahami metoda keamanan dan jenis serangan pada lapis aplikasi	• Mahasiswa mampu menjelaskan berbagai cara di mana informasi dapat diproses dalam lapisan aplikasi, mengetahui implikasi keamanan	Quiz (Tertulis)	• Tatap Muka • Penugasan terstruktur (tugas dan resume) [TM: 3x(3x50')]	1. RPC worms 2. Portmapper exploits 3. SIP and VoIP 4. Sendmail, FTP, NFS bugs, chosen-protocol and version-rollback attacks 5. Phishing attacks, usability 6. Sertifikasi server dan HTTPS	**15%**
13,14, 15	Mengetahui dan memahami metoda peningkatan keamanan sistem secara keseluruhan	• Mahasiswa mampu secara mandiri mampu menganalisis dan memahami bagaimana	Presentasi	• Tatap Muka • Penugasan terstruktur (tugas dan resume) [TM: 3x(3x50')]	1. Kriptografi pada GSM: Algoritma A3, A5, dan A8. 2. Firewall 3. Intrusion detection system 4. Password manager	**20%**

		Jaringan Keamanan Devices (Firewall, IDS / IPS, NAT, Proxy.) Bekerja. • Mahasiswa mampu mengidentifikasi kelainan dalam jaringan yang disebabkan oleh cacing, virus, Bots dan Jaringan terkait memperlakukan keamanan.			5. Network scanning 6. Privacy	
16	**Evaluasi Akhir Semester / Ujian Tengah Semester**					

Catatan :

1. Capaian Pembelajaran Lulusan PRODI (CPL-PRODI) adalah kemampuan yang dimiliki oleh setiap lulusan PRODI yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. CPL yang dibebankan pada mata kuliah adalah beberapa capaian pembelajaran lulusan program studi (CPL-PRODI) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampulan umum, ketrampilan khusus dan pengetahuan.
3. CP Mata kuliah (CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. Sub-CP Mata kuliah (Sub-CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.

5. Kreteria Penilaian adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
6. Indikator penilaian kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.

Catatan tambahan:
(1). Bobot SKS (P = Praktek; T= Teori).
(2). TM: Tatap Muka; BT: Beban Tugas; BM: Belajar Mandiri.
(3). 1 sks = (50’ TM + 50’ PT + 60’ BM)/Minggu
(4). Simbol-simbol elemen KKNI pada CPL-Prodi: S = Sikap; KU = Ketrampilan Umum; KK = Ketrampilan Khusus; P = Pengetahuan

Disusun oleh:	**Disahkan oleh:**
Dosen Pengampu **Nilla Rachmaningrum, S.T., M.T** **NIP 17780080**	**KaProdi Teknik Telekomunikasi** **Hamzah U Mustakim,S.T., M.T.** **NIP. 19900004**