MK : Keamanan Jaringan
KODE : TT G4L3
Program : S1 TT
SKS : 3
Semester : 6 (MK Wajib)

Minggu	Materi		Bentuk Pembelajaran	Course Learning Outcome
	Topik	Sub Topik		
1	Pendahuluan	1. Aturan perkulihan 2. Aturan penilaian: Quis, Ujian, Tugas dll 3. Silabus, referensi, kontrak belajar (target kehadiran minimal), sasaran pengajaran	Ceramah dan diskusi	CLO 1: Understand cryptography foundations (symmetric and asymmetric) as well as key exchange algorithms; explain how public key cryptography can be used to ensure the identity of the sender of an encrypted message.
	Pengantar Kriptografi	4. Sejarah dan tujuan kriptografi 5. Permasalahan keamanan dari dahulu sampai sekarang 6. Kebutuhan akan *confidentiality* , *integrity* ,*authority* , dan non-repudiasi 7. Aplikasi kriptografi untuk menjawab permasalahan tersebut dengan teknik simetrik, asimetrik, dan *hashing* (termasuk protokolnya)	Ceramah dan diskusi Ceramah dan diskusi Ceramah dan diskusi Ceramah dan diskusi atau tugas	
2	Kriptografi Simetrik	8. Terminologi Kripto: Pesan, Cipher, Kunci, Enkripsi dan Dekripsi, serta *attack* yang mungkin 9. Caesar Cipher, cara kerja enkripsi dan dekripsi, kekurangan 10. Vigenere Cipher, cara kerja, enkripsi dan dekripsi, kekurangan	Ceramah dan diskusi Ceramah, Tugas, Diskusi	
	Contoh standard industri algoritma Simetrik	11. Dua fokus algoritma enkripsi : *diffusion and confussion* 12. Data Encryption Standard (DES) 13. Mode kerja DES: ECB, CBC	Ceramah dan diskusi	
3	Kriptografi Asimetrik	14. Skema Kerja Kriptografi Asimetrik 15. Dasar Matematik 16. RSA 17. Penerapan untuk message *confidentiality, authority* dan non-repudiasi 18. Serangan yang mungkin pada kripto asimetrik	Ceramah, diskusi, Tugas	
4	Algoritma Pertukaran Kunci	19. Challenge and Response 20. Diffie Hellman 21. El Gamal 22. Penerapan untuk authentikasi user 23. Serangan yang mungkin pada pertukaran kunci	Ceramah dan diskusi Ceramah, Tugas, Diskusi	
		24. Prinsip kerja one-way function beserta contoh-contohnya		

	One-way and *Hash Function*	25. Algoritma hash-function yang ada dan penerapannya	Ceramah dan diskusi	
		26. Attack pada hash-function: birthday attack		
5	Keamanan dan Serangan Lapis Fisik	27. RF fingerprinting	Diskusi	CLO 2: Describe security risks concerning data integrity and systems availability in physical and datalink layer, explain the significant differences between security for data over a public network and encrypted traffic over a wireless LAN
		28. Denial of service	Ceramah, diskusi dan ilustrasi	
6	Keamanan dan Serangan Lapis Datalink	29. Kriptografi pada Wireless LAN: standard: WEP	Ceramah, diskusi dan ilustrasi	
		30. WPA dan WPA2		
7	Serangan Lapis Jaringan	31. IP smurfing	Ceramah, diskusi, Tugas kecil	CLO 3: Building an Internet Security models from the packet flow and segment point of view (network and transport layer)
		32. Address spoofing attacks		
	Keamanan Lapis Jaringan	33. Routing security		
		34. Protocol design		
8	Serangan Lapis Transport	35. Kriptografi pada jaringan komputer : Protokol SSL, sertifikasi server dan HTTPS		
		36. SYN flooding, RIP attacks, sequence number prediction	Ceramah dan diskusi	
9	Keamanan Lapis Transpor	37. Protokol SSL, TLS		
		38. IPSec key management		
		39. Access control		
10	Keamanan dan Serangan Lapis Sesi	40. RPC worms	Ceramah dan diskusi	CLO 4: Explain the diverse ways in which information can be processed in the application layer, know the security implications
		41. Portmapper exploits		
		42. SIP and VoIP		
11	Serangan Lapis Aplikasi	43. Sendmail, FTP, NFS bugs, chosen-protocol and version-rollback attacks	Ceramah dan diskusi	
		44. Phishing attacks, usability		
	Keamanan Lapis Aplikasi	45. Sertifikasi server dan HTTPS		
12	Sistem Pertahanan	46. Kriptografi pada GSM: Algoritma A3, A5, dan A8.	Simulasi dan diskusi	CLO 5: Independently analyze and understand how Network Security Devices (Firewalls, IDS/IPS, NAT, Proxies.) works. Discover and identify abnormalities within the network caused by worms, viruses, Bots and Network related security treats.
		47. Firewall		
		48. Intrusion detection system		
		49. Password manager		
		50. Network scanning		
		51. Privacy		
13	Presentasi Tugas Besar		Presentasi	
14		52. Presentasi Akhir Tugas Besar		