

**RENCANA PEMBELAJARAN SEMESTER (RPS)**

**(KEMAMAN JARINGAN MULTIMEDIA)**

**(Dr. Teuku Yuliar Arif, ST., M.Kom)**

**(Dr. Khairul Munadi, M.Eng)**



**PROGRAM STUDI TEKNIK ELEKTRO  
FAKULTAS TEKNIK  
UNIVERSITAS SYIAH KUALA  
(2018)**

## RENCANA PEMBELAJARAN SEMESTER (RPS)

Mata Kuliah : Keamana Jaringan Multimedia  
Program Studi : Teknik Elektro

Semester : 6  
Dosen :

Kode : TEL530 SKS : (3-0)  
1) Dr. Teuku Yuliar Arif, ST., M.Kom,  
2) Dr. Khairul Munadi, M.Eng

### Capaian Pembelajaran Program Studi (CP-PRODI) :

- E. mampu menggunakan metode dan instrumen-instrumen keteknikan secara benar sesuai petunjuk standar, dan memperbaharui keterampilan penggunaan instrumen tersebut secara berkelanjutan.

### Capaian Pembelajaran Mata Kuliah (CP-MK) :

- 1 Mampu memahami konsep keamanan jaringan dan jenis serangan keamanan jaringan multimedia.
- 2 Mampu memahami algoritma kriptografi block cipher simetris seperti DES dan AES serta block cipher asimetris seperti AES.
- 3 Mampu memahami algoritma kriptografi stream cipher seperti RC4.
- 4 Mampu memahami sistem keamanan web, email, wireless, IP security dan firewall.

### Kriteria Penilaian:

Nomor	Nilai Angka	Nilai Huruf
1	$\geq 87$	A
2	78 - <87	AB
3	69 - <78	B
4	60 - <69	BC
5	51 - <60	C
6	41 - <51	D
7	<41	E

### Item Penilaian :

Item	%
Absensi	5%
Tugas	20%
Kuis	10%
UTS	30%
UAS	35%
<b>Total</b>	<b>100%</b>

**JADWAL, URAIAN MATERI DAN KEGIATAN PERKULIAHAN**

<b>Minggu Ke-</b>	<b>Kemampuan Akhir Yang Diharapkan</b>	<b>Bahan Kajian (Materi Pelajaran)</b>	<b>Strategi Pembelajaran/Metode Pembelajaran</b>	<b>Waktu Belajar (menit)</b>	<b>Pengalaman Belajar Mahasiswa</b>	<b>Kriteria Penilaian (Indikator)</b>	<b>Bobot Nilai (%)</b>
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1.	Mengetahui ruang lingkup perkuliahan Keamanan Jaringan Multimedia, dan memahami konsep keamanan jaringan.	Kontrak Kuliah, cakupan materi dan pengantar keamanan jaringan.	Metode: ceramah, tanya jawab, dan demonstrasi (memberikan contoh)	510			
2.	Mampu memahami tipe-tipe serangan keamanan jaringan dan algortima enkripsi klasik.	Tipe-tipe serangan keamanan jaringan dan algortima enkripsi klasik.	Metode: ceramah, demonstrasi, tanya jawab, memberikan latihan.	510			
3.	Mampu memahami boks permutasi, subsitusi, XOR, shift sirkular dan swap yang digunakan pada algoritma DES-Sederhana dan DES.	Algoritma kriptografi simetris DES-Sederhana dan DES.	Metode: ceramah, demonstrasi, tanya jawab.	510			10
4.	Mampu memahami kekuatan dan kelemahan DES, unit data AES, struktur enkripsi/dekripsi	Algoritma kriptografi simetris DES dan AES.	Metode: ceramah, demonstrasi, tanya jawab, memberikan latihan	510			

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	AES dan transformasi AES.						
5.	Mampu memahami dan dapat melakukan ekspansi kunci AES serta memahami penerapan algoritma DES dan AES.	Ekspansi kunci AES.	Metode: ceramah, demonstrasi, tanya jawab, memberikan tugas	510			10
6.	Mampu memahami mode operasi, bilangan acak, sistem sandi stream dan sandi RC4.	Mode operasi dan sistem sandi stream RC4.	Metode: ceramah, demonstrasi, tanya jawab.	510			
7.	Mampu memahami kriptografi kunci public, kriptografi RSA, algoritma pembangkit kunci RSA, algoritma enkripsi/dekripsi RSA, keamanan RSA dan RSA-CRT.	Algoritma kriptografi kunci public RSA.	Metode: ceramah, demonstrasi, tanya jawab.	510		Benar/Salah menjawab soal	
8.	Mampu mengaplikasikan materi pertemuan 1 s.d. 7 dalam	Ujian Tengah Semester (UTS)	Metode: ujian	510			30

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	menganalisis keamanan jaringan.						
9.	Mampu memahami fungsi hash dan keutuhan data, keamanan fungsi hash dan fungsi hash dengan iterasi.	Algoritma fungsi Hash.	Metode: ceramah, tanya jawab, dan demonstrasi (memberikan contoh)	510			
10.	Mampu memahami keamanan digital signature, skema-skema digital signature dan skema digital signature standar.	Algoritma digital signature.	Metode: ceramah, demonstrasi, tanya jawab, memberikan latihan.	510			
11.	Mampu memahami keamanan web, Secure Socket Layer (SSL), Transport Layer Security (TLS), HTTPS dan Secure Shell (SSH).	Sistem keamanan Web.	Metode: ceramah, demonstrasi, tanya jawab.	510			
12.	Mampu memahami keamanan WLAN IEEE, 802.11i, keamanan lapisan	Sistem keamanan nirkabel.	Metode: ceramah, demonstrasi, tanya jawab, memberikan latihan	510			10

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	transport wireless dan keamanan WAP.						
13.	Mampu memahami system keamanan email menggunakan Pretty Good Privacy (PGP), S/MIME dan DKIM.	Sistem keamanan email.	Metode: ceramah, demonstrasi, tanya jawab, memberikan tugas	510			
14.	Mampu memahami IP Security Policy, Encapsulating Security Payload dan Internet Key Exchange.	Sistem keamanan IP.	Metode: ceramah, demonstrasi, tanya jawab.	510		Benar/Salah menjawab soal	
15.	Mampu memahami ancaman keamanan jaringan dan system pencegahannya.	Malicious Software, Intruders dan Firewall.	Metode: ceramah, demonstrasi, tanya jawab.	510		Tugas kelompok	5
16	Mampu melakukan sintesis dari semua materi yang telah diajarkan dalam menganalisis keamanan jaringan.	Ujian Akhir Semester (UAS)		510		UAS (90 menit)	35

#### Sumber Belajar/ Referensi

- [1]. Network Security Essentials: Applications and Standards, 4th ed., by William Stallings, Pearson Education, Inc., 2011.
- [2]. Cryptography and Network Security: Principles and Practice, Fifth Edition, by William Stallings, Prentice-Hall, 2011.

**Mengetahui,**  
Ketua Program Studi,

Banda Aceh, September 2018  
Koordinator/ Penanggungjawab,

(Zulhelmi, S.T., M.Sc)  
NIP. 197907022003121001

(Dr. Teuku Yuliar Arif, ST., M.Kom)  
NIP. 197307031999031003