

# **RENCANA PEMBELAJARAN SEMESTER (RPS)**

**KEAMANAN INFORMASI  
CE 3226 (3 sks)**



**Pengampu Mata Kuliah  
Mohammad Hafiz Hersyah, MT**

**Program Studi Sistem Komputer  
Fakultas Teknologi Informasi  
Universitas Andalas  
Padang, Tahun 2019**

## A. LATAR BELAKANG

Ide dasar di dalam semua tipe komunikasi adalah tersedianya tiga bahan dasar yang fundamental untuk terciptanya komunikasi yang efektif. Pertama, adanya dua entitas yang disebut dengan *sender* dan *receiver*. Dua entitas ini harus mempunyai sesuatu yang dibagi. Kedua, harus adanya sebuah perantara yang dilalui oleh hal / item yang dipertukarkan. Bagian ini disebut media transmisi. Dan ketiga, harus adanya kesepakatan tentang aturan komunikasi dari protocol.

Keamanan informasi termasuk dalam salah satu mata kuliah wajib pada kurikulum 016. Keamanan Informasi menempati lini depan yang sangat essential dalam menunjang kompetensi akhir yang diharapkan dicapai oleh mahasiswa Sistem Komputer. Hal ini dibuktikan pada realisasi tugas akhir mahasiswa yang berbasis *Internet of Things* dimana prinsip keamanan informasi pada jaringan merupakan salah satu hal yang essential di dalam pembuatan rancangan bangun alat / *prototype*. Aspek keamanan pada teknik dan perancangan komputasi menjadi irisan yang sangat strategis dalam IPTEKS yang dikembangkan, karena bersifat dinamis.


Hubungan mata kuliah Keamanan Informasi dengan mata kuliah lain terutama mata kuliah jaringan computer dan system operasi jaringan akan membentuk sebuah gugus yang saling melengkapi atribut atribut penting mengenai sebuah komunikasi jaringan internet yang aman pada kondisi ideal.

Kontribusi kompetensi pada mata kuliah Keamanan Informasi ini terhadap kompetensi inti bersifat complementary / pelengkap yang penting terutama pada penyelesaian perancangan tugas akhir mahasiswa. Inovasi metode pembelajaran yang terus dilakukan sangat bervariasi. Mulai dari kegiatan simulasi sederhana sampai kepada pembuatan video edukatif tentang pentingnya aspek keamanan pada komunikasi jaringan internet yang dapat dilihat pada media internet dan repository on-line universitas andalas.

Inovasi yang telah dilakukan terkait mata kuliah keamanan informasi adalah salah satunya pembuatan video edukasi tutorial yang diunggah ke media web berskala internasional tentang pembelajaran, tips dan antisipasi terkait aspek aspek materi keamanan informasi.

**B. PERENCANAAN PEMBELAJARAN**

**a. DEKSRIpsi RPS MATA KULIAH KEAMANAN INFORMASI**

		<b>RENCANA PEMBELAJARAN SEMESTER (RPS)</b> <b>PROGRAM STUDI : SISTEM KOMPUTER</b> <b>FAKULTAS /PPs: TEKNOLOGI INFORMASI</b> <b>UNIVERSITAS ANDALAS</b>			
MATA KULIAH	KODE	Rumpun MK	BOBOT (sks)	SEMESTER	Tgl Penyusunan
Keamanan Informasi	CE3226	Matakuliah Wajib	3	6	01-01-2019
		Dosen Pengembang RPS	Koordinator Rumpun MK	Ka Program Studi	
		Mohammad Hafiz Hersyah, MT		Ratna Aisuwarya, M.Eng	
<b>Capaian Pembelajaran (CP)</b>  Catatan : S : Sikap P : Pengetahuan KU : Keterampilan Umum KK : Keterampilan Khusus	CP Program Studi				
	S	Menunjukkan sikap antisipasi, improvisasi dan kuratif terkait objek permasalahan yang dihadapi pada kehidupan sehari hari			
	P	Mampu memetakan permasalahan terkait Keamanan Informasi internet dan mengimplementasikan solusi yang relevan			
	KU1	Mampu menerapkan pemikiran logis, kritis, sistematis dan inovatif dalam konteks pengembangan atau implementasi Keamanan Informasi yang tetap memperhatikan aspek humanis dan kearifan lokal			
	KU2	Mampu mengimplementasikan standar Keamanan Informasi			
	KU3	Mampu mengkorelasikan aspek keamanan pada bidang perekayasaan komputer			
	KK1	Mampu mengimplementasikan aspek Keamanan Informasi sebagai bagian terintegrasi pada kompetensi embedded system perancangan bangun alat.			
	CP Mata Kuliah				
	1	Mahasiswa mampu menjelaskan sejarah dan konsep dasar perekayasaan Keamanan Informasi			
	2	Mahasiswa mampu merumuskan masalah dan mencari solusi terkait keamana jaringan			
3	Mahasiswa mampu menjelaskan berbagai metode umum pokok bahasan Keamanan Informasi				
4	Mahasiswa mampu mensimulasikan keterampilan terkait Keamanan Informasi dan mengkorelasikannya dengan aspek budaya dan kearifan lokal				
Deskripsi Singkat Mata Kuliah	Pada mata kuliah ini mahasiswa difasilitasi tentang konsep dan penerapan Keamanan Informasi di mulai dari sejarah pengaplikasian penyandian keamanan, sampai kepada pengayaan yang relevan pada penerapan aspek Keamanan Informasi seperti <i>wireless security, internet protocol security, intrusion detection system, adhoc networking</i>				

<b>Materi Pembelajaran/ Pokok Bahasan</b>	<ol style="list-style-type: none"> <li>1. Sejarah dan introduction Keamanan Informasi</li> <li>2. Keamanan Informasi : pasif dan aktif</li> <li>3. Perkenalan Kriptografi</li> <li>4. Symetric Encryption</li> <li>5. Asymmetric Encryption</li> <li>6. Steganalisis</li> <li>7. Watermarking</li> <li>8. Wriress security</li> <li>9. Web Security</li> <li>10. IP (Internet Protocol) Security</li> <li>11. Firewall</li> <li>12. Intrusion Detection System</li> <li>13. Adhoc Networking</li> <li>14. Mobile Adhoc Networking</li> </ol>	
<b>Pustaka</b>	<p><b>Utama :</b></p> <p>Cryptography and Network Security – William Stallings  A Guide to Computer Network Security – Joseph Migga Kizza  Introduction to Cryptography – Nigel Smart</p> <p><b>Pendukung :</b></p>	
<b>Media Pembelajaran</b>	<b>Perangkat lunak :</b> Wireshark Enigma Simulation	<b>Perangkat keras :</b> LCD & Projector
<b>Team Teaching</b>	1. Mohammad Hafiz Hersyah, MT	
<b>Assessment</b>	<p>Tugas Pribadi 1 = <b>5%</b>  Tugas Pribadi 2 = <b>5%</b>  Tugas Kelompok 1 = <b>10%</b>  Quiz 1 = <b>10%</b>  UTS = <b>20%</b></p> <hr/> <p>Tugas Pribadi 3 = <b>5%</b>  Tugas Pribadi 4 = <b>5%</b>  Tugas Kelompok 2 = <b>5%</b>  Quiz 2 = <b>10%</b>  UAS = <b>25%</b>  <b>TOTAL = 100%</b></p>	
<b>Matakuliah Syarat</b>	-	

**b. DESKRIPSI SINGKAT MATA KULIAH**

Berikut ini adalah penjelasan tabel tentang deskripsi mata kuliah yang dijelaskan pada tabel 1.

Tabel 1. Deskripsi Mata Kuliah

<b>Mg Ke-</b>	<b>Bahan Kajian (Materi Ajar)</b>	<b>Referensi</b>
1	Sejarah dan Intro Keamanan Informasi	Cryptography and Network Security – William Stallings
2	Keamanan Informasi : Serangan Aktif dan Pasif	
3	Perkenalan Kriptografi	
4	<i>Public Key Encryption / Symetric Encryption</i>	
5	<i>Asyemetric Encryption</i>	
6	Steganalisis : Informasi Tersembunyi	
7	Digital Watermarking	
8	<b>UJIAN TENGAH SEMESTER</b>	
9	<i>Message Authentcication Code</i>	A Guide to Computer Network Security – Joseph Migga Kizza
10	<i>Digital Signature</i>	
11	<i>Internet Protocol (IP) Security</i>	
12	<i>Firewall</i>	
13	<i>Intrusion Detection System</i>	
14	<i>Adhoc Networking</i>	
15	<i>Mobile Adhoc Networking</i>	
16	<b>UJIAN AKHIR SEMESTER</b>	

c. **TUJUAN PEMBELAJARAN**

Berikut adalah tujuan pembelajaran dari masing masing pertemuan mata kuliah di jelaskan pada tabel 2.

Tabel 2. Tujuan Pembelajaran Mata Kuliah Keamanan Informasi

Minggu Ke	Bahan Kajian	Learning Outcome
1	Sejarah dan Intro Keamanan Informasi	Mahasiswa mampu mengenali Konsep alir komunikasi pada infrastruktur jaringan dan protokol komunikasi
		Mahasiswa mampu menganalisa kelemahan yang dapat terjadi pada jaringan komputer
2	Keamanan Informasi : Serangan Aktif dan Pasif	Mahasiswa mampu memahami konsep tujuan kunci keamanan informasi
		Mahasiswa mampu membedakan jenis serangan aktif dan pasif pada jaringan internet.
3	Perkenalan Kriptografi	Mahasiswa mampu memahami fungsi dari kriptografi, kripanalisis dan Kriptologi
		Mahasiswa mampu mengklasifikasikan teknik penyandian substitusi, transposisi dan gabungan
		Mahasiswa mampu mengkonstruksi teknik penyandian sederhana
4.	<i>Public Key Encryption / Symetric Encryption</i>	Mahasiswa mampu memahami konsep <i>public key</i> pada teknik penyandian kriptografi
		Mahasiswa mampu membangun konsep <i>public key</i> berdasarkan teknik kriptografi dan kearifan local minangkabau
5.	<i>Asymmetric Encryption</i>	Mahasiswa mampu memahami konsep <i>private key</i> pada teknik penyandian kriptografi
		Mahasiswa mampu membangun aplikasi <i>private key</i> berdasarkan teknik kriptografi
6.	Steganalisis : Informasi Tersembunyi	Mahasiswa mampu menjelaskan keterkaitan antara : kapasitas, keamanan dan kehandalan pada konsep dasar penyembunyian informasi
		Mahasiswa dapat menggabungkan konsep penyandian dan penyembunyian informasi
7	Digital Watermarking	Mahasiswa mampu memahami cara menanamkan pola unik atau beberapa data ke dalam konten digital tanpa mengubah kualitas perseptual
		Mahasiswa mampu memahami proses kunci perlindungan kepemilikan data elektronik yang akan dipertukarkan lewat jaringan internet
8	<b>UJIAN TENGAH SEMESTER</b>	
9	<i>Message Authentication Code</i>	Mahasiswa mampu menspesifikasikan standarisasi pengaplikasian autentifikasi code pada pesan
		Mahasiswa mampu menjelaskan pemamfaatan penerapan message authentication code pada komunikasi harian

10	<i>Digital Signature</i>	Mahasiswa mampu memahami konsep dasar digital signature
		Mahasiswa mampu mengobservasi modul yang berkaitan dengan digital signature
11	<i>Internet Protocol Security</i>	Mahasiswa mampu memahami 3 fungsi dasar : <i>authentication, confidentiality dan key management</i>
		Mahasiswa dapat mengkorelasikan format enkripsi encapsulating security payload pada mode <i>tunneling dan transport</i>
		Mahasiswa dapat menerapkan mode standar keamanan protocol internet dan memberikan edukasi yang baik kepada masyarakat
12	<i>Firewall</i>	Mahasiswa mampu memahami konsep dasar <i>firewall</i>
		Mahasiswa mampu mendesign dan mengimplementasikan jenis <i>firewall</i>
		Mahasiswa mampu memahami tipe dan penempatan fisik / logic <i>firewall</i>
13	<i>Intrusion Detection System</i>	Mahasiswa mampu memahami konsep dasar <i>intrusion detection system, denial of services dan distributed denial of services</i>
		Mahasiswa mampu mengimplementasikan bentuk bentuk <i>intrusion detection system</i> yang efektif
14	<i>Adhoc Networking</i>	Mahasiswa mampu mengkorelasikan keterkaitan antara <i>wireless security dan adhoc networking</i>
		Mahasiswa mampu memahami bentuk bentuk pengaplikasian adhoc networking
15	<i>Mobile Adhoc Networking</i>	Mahasiswa mampu memahami konsep <i>routing protocol</i> dan jenis serangan pada <i>mobile adhoc</i>
		Mahasiswa mampu mengimplementasikan pengamanan <i>adhoc network routing protocol</i>

**d. METODE PELAKSANAAN PERKULIAHAN DAN ALOKASI WAKTU**

Mg Ke-	Kemampuan akhir yg diharapkan	Bahan Kajian (Materi Ajar)	Metode Pembelajaran dan Alokasi Waktu	Pengalaman Belajar Mahasiswa	Kreteria (Indikator) Penilaian	Bobot Penilan (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1	<ol style="list-style-type: none"> <li>Mahasiswa mampu mengenali Konsep alir komunikasi pada infrastruktur jaringan dan protokol komunikasi</li> <li>Mahasiswa mampu menganalisa kelemahan yang dapat terjadi pada jaringan komputer</li> </ol>	Sejarah Keamanan Informasi, dimulai dengan ditemukannya <i>turing machine</i> , <i>enigma machine</i>	<p>Kuliah dan diskusi, (TM; (2x50 Menit)</p> <p>Tugas 1; Mencari bahan referensi tentang sejarah Keamanan Informasi</p>	Mahasiswa mencari informasi dari berbagai sumber (terutama Internet) tentang konsep, sejarah Keamanan Informasi	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>Perluasan wawasan sejarah Keamanan Informasi</li> </ul> <p><b>Bentuk non-test;</b></p> <ul style="list-style-type: none"> <li>Tulisan bertemplate IEEE</li> </ul>	2,5
2	<ol style="list-style-type: none"> <li>Mahasiswa mampu memahami konsep tujuan kunci keamanan informasi</li> <li>Mahasiswa mampu membedakan jenis serangan aktif dan pasif pada jaringan internet.</li> </ol>	Konsep yang melatarbelakangi serangan pasif dan aktif pada sebuah jaringan internet	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>Perluasan wawasan tentang metode yang umum dipakai hacker</li> </ul> <p><b>Bentuk non-test;</b> Presentasi Tugas</p>	-
3	<ol style="list-style-type: none"> <li>Mahasiswa mampu memahami fungsi dari kriptografi, kripanalisis dan Kriptologi</li> <li>Mahasiwa mampu mengkasifikasikan teknik penyandian subsitusi, transposisi dan gabungan</li> <li>Mahasiswa mampu mengkonstruksi teknik penyandian sederhana</li> </ol>	Konsep dan implementasi dasar dari teknik yang terdapat pada kriptografi seperti perpaduan teknik substitusi, transposisi dan gabungan	<p>Kuliah dan diskusi, (TM; (2x50 Menit)</p> <p>Tugas 2; Mengkreasikan teknik penyandian self-customized</p>	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>Perluasan wawasan tentang konsep kriptografi</li> </ul> <p><b>Bentuk non-test;</b> -</p>	2,5




Mg Ke-	Kemampuan akhir yg diharapkan	Bahan Kajian (Materi Ajar)	Metode Pembelajaran dan Alokasi Waktu	Pengalaman Belajar Mahasiswa	Kreteria (Indikator) Penilaian	Bobot Penilan (%)
4	<ol style="list-style-type: none"> <li>Mahasiswa mampu memahami konsep <i>public key</i> pada teknik penyandian kriptografi</li> <li>Mahasiswa mampu membangun konsep <i>public key</i> berdasarkan teknik kriptografi dan kearifan local minangkabau</li> </ol>	Mempelajari tentang konsep dasar <i>public key management</i> pada penyandian dari client – host atau sebaliknya	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>Perluasan wawasan tentang konsep public key encryption</li> </ul> <p><b>Bentuk non-test;</b> -</p>	-
5	<ol style="list-style-type: none"> <li>Mahasiswa mampu memahami konsep <i>private key</i> pada teknik penyandian kriptografi</li> <li>Mahasiswa mampu membangun aplikasi <i>private key</i> berdasarkan teknik kriptografi</li> </ol>	Mempelajari tentang konsep dasar <i>private key management</i> pada penyandian dari client – host atau sebaliknya	<p>Kuliah dan diskusi, (TM; (2x50 Menit)</p> <p>Tugas Kelompok 1 : Mensimulasikan bentuk serangan dan penyandian pada Keamanan Informasi</p>	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>Perluasan wawasan tentang konsep private key encryption</li> </ul> <p><b>Bentuk non-test;</b> -</p>	10
6	<ol style="list-style-type: none"> <li>Mahasiswa mampu menjelaskan keterkaitan antara : kapasitas, keamanan dan kehandalan pada konsep dasar penyembunyian informasi</li> <li>Mahasiswa dapat menggabungkan konsep penyandian dan penyembunyian informasi</li> </ol>	Mempelajari tentang konsep <i>information hiding</i>	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>Perluasan wawasan tentang konsep steganalisis</li> </ul> <p><b>Bentuk non-test;</b> -</p>	-
7	<ol style="list-style-type: none"> <li>Mahasiswa mampu memahami cara menanamkan pola unik atau beberapa data ke dalam konten digital tanpa mengubah kualitas perseptual</li> <li>Mahasiswa mampu</li> </ol>	Mempelajari tentang penambahan konten informasi <i>intangible</i>	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>Perluasan wawasan tentang konsep watermarking</li> </ul> <p><b>Bentuk non-test;</b></p>	-

Mg Ke-	Kemampuan akhir yg diharapkan	Bahan Kajian (Materi Ajar)	Metode Pembelajaran dan Alokasi Waktu	Pengalaman Belajar Mahasiswa	Kreteria (Indikator) Penilaian	Bobot Penilan (%)
	memahami proses kunci perlindungan kepemilikan data elektronik yang akan dipertukarkan lewat jaringan internet				-	
<b>8</b>	<b>Ujian Tengah Semester</b>				<b>Bentuk Test</b> Ujian Tertulis (2 x 45 menit)	<b>25</b>
<b>9</b>	1. Mahasiswa mampu menspesifikasikan standarisasi pengaplikasian autentifikasi code pada pesan Mahasiswa mampu menjelaskan pemamfaatan WAP (Wireless Application Protocol) 2. Mahasiswa mampu menjelaskan pemamfaatan penerapan message authentication code pada komunikasi harian	Konsep tentang message authentication code	Kuliah dan diskusi, (TM; (2x50 Menit)  Tugas Pribadi 1 : Membuat resume tentang message authentication code pada pengiriman pesan elektronik	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<b>Indikator</b> <ul style="list-style-type: none"> <li>• Perluasan wawasan tentang message authentication code</li> <li>• Pemahaman konsep tentang OSI layer</li> </ul> <b>Bentuk non-test;</b> -	<b>2,5</b>
<b>10</b>	1. Mahasiswa mampu memahami konsep dasar digital signature. 2. Mahasiswa mampu mengobservasi modul yang berkaitan dengan digital signature	Mempelajari alur dan mekanisme keamanan pada digital signature	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<b>Indikator</b> <ul style="list-style-type: none"> <li>• Perluasan wawasan tentang konsep pembuatan dan perekayasaan digital signature</li> </ul> <b>Bentuk non-test;</b> Presentasi Tugas	-
<b>11</b>	1. Mahasiswa dapat mengkorelasikan format enkripsi encapsulating	Mempelajari tentang struktur fisik internet protocol security	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode	<b>Indikator</b> <ul style="list-style-type: none"> <li>• Perluasan wawasan tentang Internet</li> </ul>	<b>2,5</b>

Mg Ke-	Kemampuan akhir yg diharapkan	Bahan Kajian (Materi Ajar)	Metode Pembelajaran dan Alokasi Waktu	Pengalaman Belajar Mahasiswa	Kreteria (Indikator) Penilaian	Bobot Penilan (%)
	<p>security payload pada mode <i>tunneling</i> dan <i>transport</i>.</p> <p>2. Mahasiswa dapat menerapkan mode standar keamanan protocol internet dan memberikan edukasi yang baik kepada masyarakat</p>		Tugas 2 : Membuat resume korelasi antara Wireless dan Adhoc Network	Group	<p>Protocol Security</p> <p><b>Bentuk non-test;</b> -</p>	
12	<p>1. Mahasiswa mampu memahami konsep dasar <i>firewall</i></p> <p>2. Mahasiswa mampu mendesign dan mengimplementasikan jenis <i>firewall</i></p> <p>3. Mahasiswa mampu memahami tipe dan penempatan fisik / logic <i>firewall</i></p>	Membahas tentang konsep dan pengaplikasian firewall	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>• Perluasan wawasan tentang Firewall</li> </ul> <p><b>Bentuk non-test;</b> Presentasi Tugas</p>	-
13	<p>1. Mahasiswa mampu memahami konsep dasar <i>intrusion detection system</i>, <i>denial of services</i> dan <i>distributed denial of services</i></p> <p>2. Mahasiswa mampu mengimplementasikan bentuk bentuk <i>intrusion detection system</i> yang efektif</p>	Mempelajari perbedaan antara denial of services dan distributed denial of services	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>• Perluasan wawasan tentang Intrusion Detection System</li> <li>• Konsep topologi Jaringan</li> </ul> <p><b>Bentuk non-test;</b> Presentasi Tugas</p>	-
14	<p>1. Mahasiswa mampu mengkorelasikan keterkaitan antara <i>wireless security</i> dan <i>adhoc networking</i></p> <p>2. Mahasiswa mampu memahami bentuk bentuk</p>	Memperkaya wawasan tentang konsep transmisi / komunikasi data mobile	Kuliah dan diskusi, (TM; (2x50 Menit)	Pemamfaatan metode SCL (Student Learning Center) – Metode Group	<p><b>Indikator</b></p> <ul style="list-style-type: none"> <li>• Perluasan wawasan tentang perpaduan wireless security dan ad hoc networking</li> </ul>	-

Mg Ke-	Kemampuan akhir yg diharapkan	Bahan Kajian (Materi Ajar)	Metode Pembelajaran dan Alokasi Waktu	Pengalaman Belajar Mahasiswa	Kreteria (Indikator) Penilaian	Bobot Penilan (%)
	pengaplikasian adhoc networking				<b>Bentuk non-test;</b> -	
<b>15</b>	1. Mahasiswa mampu memahami konsep <i>routing protocol</i> dan jenis serangan pada <i>mobile adhoc</i> 2. Mahasiswa mampu mengimplementasikan pengamanan <i>adhoc network routing protocol</i>	Mempelajari salah satu bentuk ad hoc networking	Kuliah dan diskusi, (TM; (2x50 Menit)  Quiz	Pemamfaatan metode SCL (Student Learning Center) – Metode Group  Quiz	<b>Indikator</b> <ul style="list-style-type: none"> <li>• Perluasan wawasan tentang perpaduan wireless security dan ad hoc networking</li> </ul> <b>Bentuk test</b> Quiz tertulis 1 x 45 menit	<b>10</b>
<b>16</b>	<b>Ujian Akhir Semester</b>				<b>Bentuk test</b> Ujian Tertulis 2 x 45 Menit / Tugas Besar / Tugas Pengganti UAS	<b>30</b>

e. CONTOH RANCANGAN TUGAS MAHASISWA

		<b>PROGRAM STUDI : SISTEM KOMPUTER</b> <b>FAKULTAS /PPs: TEKNOLOGI INFORMASI</b> <b>UNIVERSITAS ANDALAS</b>			
<b>TUGAS MAHASISWA</b>					
<b>MATA KULIAH</b>	KEAMANAN INFORMASI				
<b>KODE</b>	CE 3226	<b>sks</b>	3	<b>SEMESTER</b>	6
<b>DOSEN PENGAMPU</b>	Mohammad Hafiz Hersyah, MT				
<b>BENTUK TUGAS</b>					
PAPER KREASI RANCANGAN TEKNIK PENYANDIAN BERTEMPLATE IEEE					
<b>JUDUL TUGAS</b>					
Tugas 1 : Membuat Kreasi Teknik Penyandian Self-Costumized					
<b>SUB CAPAIAN PEMBELAJARAN MATA KULIAH</b>					
Mahasiswa mampu mengkonstruksi teknik penyandian sederhana					
<b>DESKRIPSI TUGAS</b>					
Kreasikan bentuk teknik penyandian dengan memanfaatkan teknik substitusi, transposisi dan gabungan					
<b>METODE Pengerjaan Tugas</b>					
<ol style="list-style-type: none"> <li>1. Mencari dan menyadur minimal 3 publikasi ilmiah melalui akses EBSCO melalui laman web <a href="http://www.pustaka.unand.ac.id">www.pustaka.unand.ac.id</a></li> <li>2. Dikerjakan dalam 1 minggu</li> <li>3. Tipe tugas individu</li> </ol>					
<b>BENTUK DAN FORMAT LUARAN</b>					
<p><b>a. Obyek Garapan:</b> Penyusunan Paper Publikasi</p> <p><b>b. Bentuk Luaran:</b></p> <ol style="list-style-type: none"> <li>1. Paper bertemplate IEEE tentang Teknik Penyandian</li> <li>2. Slide presentasi</li> </ol>					
<b>INDIKATOR, KRETERIA DAN BOBOT PENILAIAN</b>					
<p><b>a. Ringkasan hasil kajian journal (bobot 30%)</b>            Ringkasan journal dengan sistematika dan format yang telah ditetapkan, kemutakhiran journal (5 tahun terakhir), kejelasan dan ketajaman meringkas, konsistensi dan kerapian dalam sajian tulisan.</p>					

**b. Paper Publikasi / Konten (30%)**

1. Ketepatan sistematika penyusunan proposal sesuai dengan standar panduan penulisan bertemplate IEEE
2. Ketepatan tata tulis proposal sesuai dengan ejaan bahasa Indonesia yang benar dan sesuai dengan standard IEEE dalam penyajian tabel, gambar, penulisan rujukan dan penisan sitasi;

**c. Penyusunan Slide Presentasi (bobot 20%)**

Jelas dan konsisten, Sederhana & inovative, menampilkan gambar & blok sistem, tulisan menggunakan font yang mudah dibaca, jika diperlukan didukung dengan gambar dan video clip yang relevant.

**d. Presentasi (bobot 20%)**

Bahasa komunikatif, penguasaan materi, penguasaan audiensi, pengendalian waktu (15 menit presentasi + 5 menit diskusi), kejelasan & ketajaman paparan, penguasaan media presentasi.

**JADWAL PELAKSANAAN**

Meringkas Journal	2 Oktober - 3 Oktober 2016
Menyusun paper	2 Oktober - 8 Oktober 2016
Presentasi proposal	9 Oktober 2016
Pengumuman hasil penilaian	9 Oktober 2016

**LAIN-LAIN**

Bobot penilaian tugas ini adalah 2,5% dari dari 100% penilaian mata kuliah