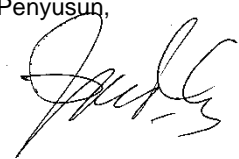

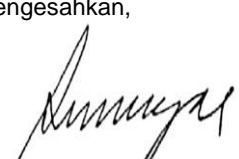


RENCANA PEMBELAJARAN SEMESTER (RPS) PROGRAM STUDI INFORMATIKA INF522

Issue/Revisi	: V1/R0	Tanggal	: 01 Agustus 2020
Mata Kuliah	: Kriptografi	Kode MK	: INF522
Rumpun MK	: MKPIL	Semester	: 6 (Enam)
Dosen Penyusun	: Prio Handoko, S.Kom., M.T.I.	Bobot (sks)	: 3
Penyusun,	Menyetujui,	Mengesahkan,	
 (Prio Handoko, S.Kom., M.T.I.)	 (Safitri Jaya, S.Kom., M.T.I.)	 (Ir. Resdiansyah, S.T., M.T., Ph.D)	

RENCANA PEMBELAJARAN SEMESTER	
Capaian Pembelajaran (CP)	CPL - PRODI
	S3 Berkontribusi dalam peningkatan mutu kehidupan bermasyarakat, berbangsa, bernegara, dan peradaban berdasarkan Pancasila;
	S9 Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri;
	KU1 Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahliannya;
	KU2 Mampu menunjukkan kinerja mandiri, bermutu, dan terukur;
	KS1 Mampu menggunakan ilmu pengetahuan dan teknologi dalam menyelesaikan masalah;
	KS9 Mampu menguasai algoritma dan kompleksitas dengan cara mempelajari konsep-konsep sentral dan kecakapan yang dibutuhkan untuk merancang, menerapkan, dan menganalisis algoritma yang digunakan untuk pemodelan dan desain sistem berbasis komputer;
	CP-MK
	II.A.1 Menguasai konsep-konsep matematika untuk memecahkan berbagai masalah yang berkaitan dengan logika
	II.A.2 Menguasai prinsip-prinsip pemodelan matematika, program linear serta metode numerik
III.A.1 Menguasai teori dan konsep yang mendasari ilmu komputer	
III.A.4 Menguasai bidang fokus pengetahuan ilmu komputer serta mampu beradaptasi dengan perkembangan ilmu pengetahuan dan teknologi	
VI.A.4 Merancang sistem keamanannya serta melakukan pengelolaan secara kontinu terhadap proteksi profil yang ada	
Deskripsi Singkat MK	Mata kuliah ini memberikan pemahaman mengenai konsep pengamanan informasi dan komunikasi menggunakan menggunakan beragam metode proteksi ke dalam bentuk kode. Pembahasan materi perkuliahan berkisar kepada pemahaman konsep kriptografi, perkembangan metode kriptografi, mulai dari metode konvensional hingga modern, ragam metode serta mekanisme enkripsi dan dekripsi informasi, jenis-jenis enkripsi.

RENCANA PEMBELAJARAN SEMESTER (RPS) PROGRAM STUDI INFORMATIKA INF522

RENCANA PEMBELAJARAN SEMESTER				
Materi Pembelajaran/Pokok Bahasan	<ol style="list-style-type: none"> 1. Kriptografi (Pendahuluan) 2. Kriptografi Konvensional 3. Serangan Kriptografi 4. Kriptografi Modern 5. Fungsi Hash dan Pembangkit Bilangan Acak 6. Steganografi dan Watermark 7. Kriptografi Visual 			
Pustaka	Utama			
	1. Rinaldi Munir. 2019. Kriptografi. Edisi Kedua. Informatika, Bandung			
	Pendukung			
	1. -			
Media Pembelajaran	Perangkat Lunak:			
	<table border="1"> <tr> <td>- Menggunakan aplikasi MS. PowerPoint untuk menjelaskan materi</td> <td>Perangkat Keras:</td> </tr> <tr> <td></td> <td>- LCD Projector</td> </tr> </table>	- Menggunakan aplikasi MS. PowerPoint untuk menjelaskan materi	Perangkat Keras:	
- Menggunakan aplikasi MS. PowerPoint untuk menjelaskan materi	Perangkat Keras:			
	- LCD Projector			
Team Teaching	-			
Mata Kuliah Prasyarat	-			
Indikator, Kriteria dan Bobot Penilaian	<ul style="list-style-type: none"> - Ujian Akhir Semester 25% - Ujian Tengah Semester 30% - Tugas 15% - Studi Kasus 30% 			

RENCANA PEMBELAJARAN SEMESTER (RPS) PROGRAM STUDI INFORMATIKA INF522

RENCANA PEMBELAJARAN SEMESTER						
Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1	1. Mahasiswa memahami konsep dasar kriptografi 2. Mahasiswa memahami komponen-komponen kriptografi 3. Mahasiswa memahami metode validasi keabsahan pesan yang dienkripsi	<ul style="list-style-type: none"> - Mampu menjelaskan definisi dan konsep kriptografi - Mampu menjelaskan dan menguraikan komponen-komponen kriptografi - Mampu menjelaskan metode 	Kriteria: Pemahaman dan Penguasaan Bentuk Penilaian: Tanya jawab	Kuliah dan Diskusi [TM: 1 x (3x50)] Kuliah Mandiri [KM: 1 x (3x60)] Terstruktur [TS: 1 x (3x60)]	- Kriptografi (Pendahuluan)	2
2, 3	1. Mahasiswa memahami klasifikasi kriptografi 2. Mahasiswa memahami beragam jenis kriptografi konvensional/klasik 3. Mahasiswa memahami prinsip kerja beberapa jenis kriptografi konvensional/klasik 4. Mahasiswa melakukan simulasi proses enkripsi dan dekripsi kriptografi konvensional	<ul style="list-style-type: none"> - Mampu menjelaskan 2 klasifikasi kriptografi - Mampu membedakan antara beragam jenis kriptografi konvensional /klasik - Mampu menjelaskan prinsip kerja beragam jenis kriptografi konvensional - Mampu melakukan simulasi enkripsi dan dekripsi beragam jenis kriptografi - Menyelesaikan kasus-kasus yang berkenaan dengan kriptografi konvensional 	Kriteria: Pemahaman dan Penguasaan Bentuk Penilaian: Tugas mandiri dan Tanya jawab	Kuliah dan Diskusi [TM: 2 x (3x50)] Kuliah Mandiri [KM: 2 x (3x60)] Terstruktur [TS: 2 x (3x60)]	- Kriptografi Konvensional	4

4	<ol style="list-style-type: none"> Mahasiswa memahami konsep serangan terhadap teknik kriptografi yang digunakan Mahasiswa memahami jenis-jenis serangan pada kriptografi Mahasiswa memahami teknik serangan pada kriptografi 	<ul style="list-style-type: none"> Mampu menjelaskan konsep serangan terhadap kriptografi Mampu membedakan antar tiap jenis serangan pada sebuah kriptografi Mampu menjelaskan dan memberikan contoh penggunaan teknik serangan pada kriptografi 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian: Tugas mandiri, tanya jawab, dan KUIZ</p>	<p>Kuliah dan Diskusi [TM: 1 x (3x50)]</p> <p>Kuliah Mandiri [KM: 1 x (3x60)]</p> <p>Terstruktur [TS: 1 x (3x60)]</p>	- Serangan Kriptografi	2
Tugas 1						4
5, 6	<ol style="list-style-type: none"> Mahasiswa memahami konsep kriptografi modern Mahasiswa memahami beragam tipe kriptografi modern serta penggunaannya Mahasiswa memahami beberapa akategori chiper sebagai hasil enkripsi sebuah pesan 	<ul style="list-style-type: none"> Mampu membedakan konsep antara kriptografi konvensional /klasik dan kriptografi modern Mampu menjelaskan dan memberikan contoh penggunaan beragam tipe kriptografi modern Mampu menunjukkan karakteristik chiper beragam tipe kriptografi modern 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian: Tugas mandiri, tanya jawab, dan KUIZ</p>	<p>Kuliah dan Diskusi [TM: 1 x (3x50)]</p> <p>Kuliah Mandiri [KM: 1 x (3x60)]</p> <p>Terstruktur [TS: 1 x (3x60)]</p>	- Kriptografi Modern	4
7	Studi Kasus 1					6
8	Evaluasi Tengah Semester : 25% Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya					
9, 10, 11	<ol style="list-style-type: none"> Mahasiswa memahami metode-metode pembangkit bilangan acak Mahasiswa memahami konsep hash dalam menyederhanakan ukuran enkripsi pesan Mahasiswa memahami proses penggunaan hash dalam melakukan enkripsi pesan 	<ul style="list-style-type: none"> Mampu menjelaskan metode-metode pembangkit bilangan acak Mampu membandingkan perbedaan dan kelebihan antara setiap metode pembangkit bilangan acak Mampu mengimplementasikan fungsi hash dalam melakukan 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian: Tanya jawab</p>	<p>Kuliah dan Diskusi [TM: 3 x (3x50)]</p> <p>Kuliah Mandiri [KM: 3 x (3x60)]</p> <p>Terstruktur [TS: 3 x (3x60)]</p>	- Fungsi Hash dan Pembangkit Bilangan Acak	6

	4. Mahasiswa memahami proses pembangkitan bilangan acak menggunakan metode pembangkit bilangan acak	<p>enkripsi pesan</p> <ul style="list-style-type: none"> - Mampu menyelesaikan kasus yang berhubungan dengan 2 metode pembangkit bilangan acak, Blum Blum Shub dan Algoritma RSA 				
Tugas 2						4
12, 13	<ol style="list-style-type: none"> 1. Mahasiswa memahami konsep Steganografi untuk menyembunyikan pesan dalam bentuk pesan lainnya 2. Mahasiswa memahami 2 properti utama dalam penggunaan teknik steganografi 3. Memahami sejarah perkembangan steganografi 4. Mahasiswa memahami konsep Watermark 5. Mahasiswa memahami proses pembuatan watermark sebagai pengamanan sebuah hasil ciptaan 	<ul style="list-style-type: none"> - Mampu menjelaskan konsep steganografi sebagai metode menyembunyikan pesan dalam bentuk pesan lainnya - Mampu menjelaskan properti terbentuknya steganografi - Menjelaskan perbedaan kelebihan dan kekurangan steganografi klasik dan modern - Mampu menjelaskan akan pentingnya penggunaan Watermarking pada hasil ciptaan - Mampu menjelaskan dan melakukan simulasi pembuatan watermarking 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian: Tugas mandiri dan tanya jawab</p>	<p>Kuliah dan Diskusi [TM: 2 x (3x50)]</p> <p>Kuliah Mandiri [KM: 2 x (3x60)]</p> <p>Terstruktur [TS: 2 x (3x60)]</p>	- Steganografi dan Watermark	4
14	<ol style="list-style-type: none"> 1. Mahasiswa memahami konsep mengenai kriptografi visual 2. Mahasiswa memahami hal yang mendasari kebutuhan akan penggunaan kriptografi visual 3. Mahasiswa memahami prosedur pembuatan sebuah 	<ul style="list-style-type: none"> - Mampu menjelaskan konsep dan memberikan contoh penggunaan kriptografi visual - Mampu menjelaskan munculnya kebutuhan akan kriptografi visual - Mampu melakukan 	<p>Kriteria: Ketepatan dan Penguasaan</p> <p>Bentuk Penilaian: Tugas mandiri dan tanya jawab</p>	<p>Kuliah dan Diskusi [TM: 1 x (3x50)]</p> <p>Kuliah Mandiri [KM: 1 x (3x60)]</p> <p>Terstruktur [TS: 1 x (3x60)]</p>	- Kriptografi Visual	2

	kriptografi visual	langkah-langkah pembuatan kriptografi visual yang disebut dengan Steganograph.				
	4. Mahasiswa memahami jenis pembagian citra dalam kriptografi visual					
15	Studi Kasus 2					6
16	Evaluasi Akhir Semester: 30% Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa					

RANCANGAN TUGAS MAHASISWA					
Mata Kuliah	Kriptografi				
Kode MK	INF522	sks:	3	Semester:	6
Dosen Pengampu	Prio Handoko, S.Kom, M.T.I				
BENTUK TUGAS					
1. Tugas mandiri 2. Tugas kelompok					
JUDUL TUGAS					
1. Kriptografi (Pendahuluan) 2. Kriptografi Konvensional 3. Serangan Kriptografi 4. Kriptografi Modern 5. Fungsi Hash dan Pembangkit Bilangan Acak 6. Steganografi dan Watermark 7. Kriptografi Visual					
SUB CAPAIAN PEMBELAJARAN MATA KULIAH					
1. Mahasiswa mampu menjelaskan konsep dasar kriptografi beserta komponen-komponen kriptografi 2. Mahasiswa mampu menjelaskan klasifikasi kriptografi 3. Mahasiswa mampu menjelaskan beragam jenis kriptografi konvensional/klasik berikut perbedaan prinsip kerja beberapa jenis kriptografi konvensional/klasik 4. Mahasiswa mampu melakukan simulasi proses enkripsi dan dekripsi kriptografi konvensional 5. Mahasiswa mampu menjelaskan serangan terhadap kriptografi berdasarkan jenis-jenis serangan 6. Mahasiswa mampu melakukan simulasi penggunaan beragam tipe kriptografi modern serta penggunaannya 7. Mahasiswa mampu menyelesaikan kasus-kasus yang berhubungan dengan pembangkitan bilangan acak menggunakan metode perancangan CSPRING Blum Blum Shub dan Algoritma RSA 8. Mahasiswa menjelaskan konsep steganografi untuk menyembunyikan pesan dalam bentuk pesan lainnya 9. Mahasiswa mampu melakukan simulasi menyembunyikan pesan dengan teknik steganografi 10. Mahasiswa mampu melakukan proses pembuatan watermark sebagai pengaman sebuah hasil ciptaan 11. Mahasiswa mampu menjelaskan konsep kriptografi visual dan menjalankan prosedur pembuatan sebuah kriptografi visual					
DESKRIPSI TUGAS					
1. Menyelesaikan tugas yang diberikan dan menuliskannya dalam <i>logbook</i> (buku catatan) yang akan dievaluasi dan dinilai setiap minggunya dan dikirimkan melalui laman Google Classroom .					
METODE Pengerjaan Tugas					

RENCANA PEMBELAJARAN SEMESTER (RPS) PROGRAM STUDI INFORMATIKA INF522

RANCANGAN TUGAS MAHASISWA	
1. Menyelesaikan kasus-kasus yang diberikan secara tertulis. 2. Kasus dikerjakan secara individu maupun kelompok dan dosen pengampu akan menunjuk secara acak mahasiswa dan memintanya untuk mengerjakan dalam selang waktu tertentu.	
BENTUK DAN FORMAT LUARAN	
1. Tugas tertulis dalam buku catatan	
INDIKATOR, KRITERIA DAN BOBOT PENILAIAN	
1. Tugas mandiri/kelompok (bobot 8%)	
JADWAL PELAKSANAAN	
Tugas 1 diberikan sebelum UTS, dengan jadwal pengumpulan pada minggu ke-4 (empat)	Tugas 2 diberikan sebelum UAS, dengan jadwal pengumpulan pada minggu ke-11 (sebelas)
LAIN-LAIN	
1. Tugas dikerjakan secara mandiri maupun kelompok.	
DAFTAR RUJUKAN	
1. Buku catatan 2. Materi kuliah yang dapat diunduh di laman OCW Universitas Pembangunan Jaya 3. Rinaldi Munir. 2019. Kriptografi. Edisi Kedua. Informatika, Bandung	