

SILABUS MATAKULIAH

Revisi : -
 Tanggal Berlaku : 12 Februari 2014

A. Identitas

- 1. Nama Matakuliah : A11. 54606/ Kriptografi
- 2. Program Studi : Teknik Informatika-S1
- 3. Fakultas : Ilmu Komputer
- 4. Bobot sks : 3 SKS
- 5. Elemen Kompetensi : MKK
- 6. Jenis Kompetensi : Sistem Komputer dan Komunikasi Data
- 7. Alokasi waktu total : 14 X 150 Menit

B. Unsur-unsur Silabus

Kompetensi Dasar	Indikator	Pokok Bahasan/Materi	Strategi Pembelajaran	Alokasi Waktu	Referensi	Evaluasi
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> • Memperoleh gambaran secara lengkap mengenai proses pembelajaran yang akan dilaksanakan selama satu semester. • Memahami dan menjelaskan peran kriptografi dalam pengamanan data 	<ol style="list-style-type: none"> 1. Cakupan materi dan pokok bahasan 2. Buku-buku yang digunakan 3. Memahami pentingnya kriptografi yang digunakan untuk menyelesaikan masalah keamanan komputer 	<ol style="list-style-type: none"> a. Menjelaskan Diskripsi matakuliah, Buku referensi yang digunakan, sistem penilaian serta kontrak perkuliahan dengan mahasiswa b. Paradigma Keamanan Komputer <ul style="list-style-type: none"> • Masalah, Ancaman dan Aspek Keamanan Komputer • Studi kasus permasalahan dalam pengiriman pesan elektronik 	<ol style="list-style-type: none"> 1. Menjelaskan ancaman kemananan data pada transaksi elektronik 2. Menjelaskan manfaat mempelajari mata kuliah kriptografi dalam kehidupan sehari-hari 	150 menit	1, 2, 3, 4	<ol style="list-style-type: none"> a. Melakukan tanya jawab pemahaman mahasiswa tentang kriptografi b. Memberi latihan di kelas. c. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.

Kompetensi Dasar	Indikator	Pokok Bahasan/Materi	Strategi Pembelajaran	Alokasi Waktu	Referensi	Evaluasi
		<ul style="list-style-type: none"> Konsep, peran dan pentingnya Kriptografi 				
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memperoleh gambaran secara lengkap mengenai sejarah dan terminologi kriptografi Memahami dan menjelaskan perbedaan kriptografi klasik dan modern 	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan terminologi yang digunakan dalam kriptografi Menganalisa perbedaan antara metode kriptografi klasik dan modern Menyelesaikan persoalan yang diberikan 	Sejarah dan Perkembangan Kriptografi <ol style="list-style-type: none"> Sejarah Kriptografi Terminologi dalam kriptografi Algoritma Kriptografi Kriptografi Klasik Kriptografi Modern 	<ol style="list-style-type: none"> Menjelaskan sejarah dan perkembangan kriptografi Menjelaskan beberapa contoh penerapan kriptografi yang sudah dilakukan sepanjang sejarah manusia Menjelaskan terminologi dalam kriptografi (plaintext, algoritma enkripsi, kunci dan ciphertext) Perbedaan kriptografi klasik dan modern 	150 menit	1, 2, 3, 4	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memahami dan menjelaskan teknik substitusi abjad Menganalisa dan menyelesaikan persoalan yang diberikan menggunakan teknik substitusi abjad secara tepat 	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan konsep substitusi abjad Mengklasifikasikan jenis-jenis teknik substitusi abjad 	Teknik Substitusi Abjad <ol style="list-style-type: none"> Teknik Caesar Cipher Cipher abjad-tunggal (monoalphabetic cipher) Cipher substitusi homofonik (Homophonic substitution cipher) Cipher abjad-majemuk (Polyalphabetic substitution cipher) Cipher substitusi poligram (Polygram substitution cipher) 	<ol style="list-style-type: none"> Menjelaskan konsep proses substitusi abjad Menjelaskan metode caesar cipher Menjelaskan konsep Cipher abjad tunggal Menjelaskan konsep Cipher substitusi homofonik Menjelaskan konsep Cipher abjad-majemuk Menjelaskan konsep Cipher substitusi poligram 	150 menit	1, 2, 3, 4	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.

Kompetensi Dasar	Indikator	Pokok Bahasan/Materi	Strategi Pembelajaran	Alokasi Waktu	Referensi	Evaluasi
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memahami dan menjelaskan langkah enkripsi playfair Menerapkan playfair kedalam program aplikasi 	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan dan memahami langkah-langkah playfair cipher Mengevaluasi metode playfair 	Teknik Playfair Cipher <ol style="list-style-type: none"> Sejarah dan konsep Playfair cipher Aturan untuk Plaintext Pembangkitan kunci pada playfair Algoritma enkripsi pada playfair 	<ol style="list-style-type: none"> Menjelaskan sejarah dan konsep playfair cipher Menjelaskan langkah-langkah enkripsi menggunakan playfair Memberi contoh enkripsi playfair 	150 menit	1, 3	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memahami dan menjelaskan konsep Vigenere dan Hill Menerapkan metode Vigenere dan Hill untuk menyelesaikan persoalan yang diberikan. 	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan dan memahami langkah-langkah Vigenere cipher Menjelaskan dan memahami langkah-langkah Hill cipher Menganalisa kelebihan dan kekurangan masing-masing metode enkripsi 	Vigenere dan Hill Cipher <ol style="list-style-type: none"> Sejarah dan konsep Vegenere Cipher Algortima vigenere Cipher Sejarah dan konsep Hill Cipher Algoritma Hill Cipher 	<ol style="list-style-type: none"> Menjelaskan sejarah konsep Vigenere cipher Menjelaskan langkah-langkah enkripsi Vigenere Menjelaskan sejarah konsep Hill cipher Menjelaskan langkah-langkah enkripsi Hill 	150 menit	1, 2, 3, 4	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memahami dan menjelaskan berbagai jenis teknik transposisi Menerapkan secara 	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan dan memahami langkah-langkah teknik transposisi Menganalisa perbedaan dari 	Teknik Transposisi/Permutasi <ol style="list-style-type: none"> Konsep Metode Transposisi Perbedaan dengan konsep Subtitusi Transposisi rail fence Transposisi Route 	<ol style="list-style-type: none"> Menjelaskan konsep teknik transposisi Menjelaskan teknik Transposisi rail fence Menjelaskan teknik Transposisi Route Menjelaskan teknik Transposisi Kolom 	150 menit	1, 2, 3, 4	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.

Kompetensi Dasar	Indikator	Pokok Bahasan/Materi	Strategi Pembelajaran	Alokasi Waktu	Referensi	Evaluasi
tepat metode transposisi untuk menyelesaikan studi kasus yang diberikan	masing-masing teknik transposisi	e. Transposisi Kolom f. Transposisi Ganda g. Transposisi Myszkowski	5. Menjelaskan teknik Transposisi Ganda 6. Menjelaskan teknik Transposisi Myszkowski			
Setelah mengikuti kuliah ini mahasiswa dapat memahami dan menjelaskan konsep algoritma sempurna	Mahasiswa mampu: 1. Menjelaskan dan memahami konsep algoritma sempurna 2. Mengetahui jenis-jenis algoritma super enkripsi, one time pad dan enigma motor machine	Super Enkripsi dan Algoritma Sempurna a. Konsep Algoritma yang sempurna b. Super Enkripsi c. One Time Pad d. Enigma Rotor Machine	1. Menjelaskan konsep algoritma sempurna 2. Menjelaskan teknik super enkripsi 3. Menjelaskan teknik One Time Pad 4. Menjelaskan Enigma Motor Machine	150 menit	2, 3	a. Melakukan tanya jawab pemahaman mahasiswa b. Memberi latihan di kelas. c. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.
Ujian Tengah Semester						
Setelah mengikuti kuliah ini mahasiswa dapat menganalisa kelebihan dan kekurangan stream cipher dibandingkan teknik sebelumnya	Mahasiswa mampu: 1. Memahami dan menjelaskan konsep stream cipher 2. Menganalisa perbedaan stream cipher dibandingkan teknik sebelumnya 3. Mengetahui	Teknik Stream Cipher a. Konsep Stream Cipher b. Operasi pada mode Bit String c. Synchronous Stream Cipher d. Self Synchronous Stream Cipher e. Contoh aplikasi pada stream cipher	1. Menjelaskan konsep dasar Stream Cipher 2. Menjelaskan langkah metode operasi pada Bit String 3. Menjelaskan metode Synchronous dan Self Synchronous Cipher	150 menit	1, 3, 4	a. Melakukan tanya jawab pemahaman mahasiswa b. Memberi latihan di kelas. c. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.

Kompetensi Dasar	Indikator	Pokok Bahasan/Materi	Strategi Pembelajaran	Alokasi Waktu	Referensi	Evaluasi
	jenis-jenis enkripsi pada stream cipher					
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memahami dan menjelaskan perbedaan kriptografi klasik dan modern Menerapkan metode Vigenere dan Hill untuk menyelesaikan persoalan yang diberikan 	Mahasiswa mampu: <ol style="list-style-type: none"> Memahami dan menjelaskan konsep dasar teknik block cipher Mengetahui jenis-jenis block cipher 	Teknik Block Cipher <ol style="list-style-type: none"> Mode Electronic Code Block Mode Cipher Block Chaining Mode Cipher Feed Back Mode Output Feed Back 	<ol style="list-style-type: none"> Menjelaskan konsep dasar teknik block Cipher Menjelaskan berbagai jenis teknik dan metode block Cipher 	150 menit	1, 2, 3	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.
Setelah mengikuti kuliah ini mahasiswa dapat memahami langkah-langkah enkripsi DES	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan konsep DES Mengetahui langkah-langkah pada enkripsi DES 	Data Ecrption Standar (DES) <ol style="list-style-type: none"> Konsep dasar DES Algoritma DES Langkah-langkah enkripsi DES 	<ol style="list-style-type: none"> Menjelaskan konsep DES Menjelaskan langkah-langkah enkripsi DES 	150 menit	1, 3	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memahami dan menjelaskan kelebihan dibandingkan algortima DES 	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan konsep AES Mengetahui langkah-langkah AES 	Advanced Ecrption Standar (AES) <ol style="list-style-type: none"> Konsep dasar AES Algoritma AES Langkah-langkah enkripsi AES 	<ol style="list-style-type: none"> Menjelaskan konsep AES Menjelaskan perbedaan DES dan AES Menjelaskan langkah-langkah AES 	150 menit	1, 3	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.

Kompetensi Dasar	Indikator	Pokok Bahasan/Materi	Strategi Pembelajaran	Alokasi Waktu	Referensi	Evaluasi
<ul style="list-style-type: none"> Memahami langkah-langkah enkripsi AES 						
Setelah mengikuti kuliah ini mahasiswa dapat memahami dan menjelaskan enkripsi RSA dan MD5	Mahasiswa mampu: <ol style="list-style-type: none"> Menjelaskan dan memahami algoritma RSA dan MD5 Mengetahui langkah-langkah enkripsi RSA dan MD5 	RSA dan MD5 <ol style="list-style-type: none"> Algoritma RSA Enkripsi dan dekripsi RSA Algoritma MD5 Enkripsi MD5 	<ol style="list-style-type: none"> Menjelaskan sejarah dan konsep RSA Menjelaskan langkah-langkah enkripsi RSA Menjelaskan sejarah dan konsep MD5 Menjelaskan langkah-langkah enkripsi MD5 	150 menit	1, 2, 3, 4	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.
Setelah mengikuti kuliah ini mahasiswa dapat: <ul style="list-style-type: none"> Memahami dan menjelaskan perbedaan steganografi dan watermarking Menyebutkan berbagai contoh aplikasi yang menerapkan teknik steganografi dan watermarking 	Mahasiswa mampu: <ol style="list-style-type: none"> Memahami konsep Steganografi dan Watermarking Menganalisa dan menjelaskan perbedaan Steganografi dan Watermarking Menyebutkan dan menjelaskan contoh aplikasi yang menerapkan metode 	Steganografi dan Watermarking <ol style="list-style-type: none"> Sejarah Steganografi Digital Watermarking Aplikasi Steganografi Digital Signature Digital Certificate Pretty Good Privacy 	<ol style="list-style-type: none"> Menjelaskan konsep dan perbedaan steganografi dan watermarking Memberi contoh aplikasi steganografi dan watermarking 	150 menit	1, 3, 4	<ol style="list-style-type: none"> Melakukan tanya jawab pemahaman mahasiswa Memberi latihan di kelas. Memberi tugas kepada mahasiswa untuk dikerjakan di rumah.

Kompetensi Dasar	Indikator	Pokok Bahasan/Materi	Strategi Pembelajaran	Alokasi Waktu	Referensi	Evaluasi
	tersebut.					
Ujian Akhir Semester						

Daftar Referensi
Buku Utama:

1. Bruce Scheier, (2001), Applied Cryptography, John Willey & Sons Inc, Canada
2. Cobb, Chey, (2004), Cryptography for Dummies, John Willey & Sons Inc, Canada
3. Stalling William, (2003), Cryptography and Network Security, Prentice Hall, USA

Buku Tambahan :

4. Ariyus Doni, (2006), Kriptografi, Keamanan Data dan Komunikasi, Graha Ilmu, Yogyakarta

Disusun oleh :	Diperiksa oleh :		Disahkan oleh :
Dosen Pengampu	Penanggungjawab Keilmuan	Program Studi	Dekan
Aisyatul Karima, S.Kom, M.CS	Elkaf Rahmawan P.,M.Kom	Heru Agus Santoso , Ph. D	DR. Drs. Abdul Syukur, MM