	UIN SUNAN KALIJAGA **PROGRAM STUDI: MATEMATIKA**

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH:	KODE MATA KULIAH:	RUMPUN MATA KULIAH:	BOBOT (SKS):	SEMESTER:	TANGGAL PENYUSUNAN:
Kriptografi	**MAT415030**	**Aljabar**	**3 SKS**	**IV**	13 Januari 2021
OTORISASI Ketua Prodi	DOSEN PENGEMBANG RPS: **Muhamad Zaki Riyanto, M.Sc.**	KOORDINATOR RMK:			Kaprodi **Muchammad Abrori, S.Si, M.Kom.**
CAPAIAN PEMBELAJARAN	CAPAIAN PEMBELAJARAN PRODI	1. Menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan/atau teknologi sesuai dengan bidang matematika. 2. Memecahkan masalah melalui pendekatan dan pemikiran matematis serta mengembangkannya dengan atau tanpa bantuan piranti lunak, baik dalam bidang matematika maupun bidang lainnya yang relevan.			
	CAPAIAN PEMBELAJARAN MATA KULIAH	Setelah mengikuti perkuliahan ini selama satu semester, mahasiswa mampu menganalisis salah satu algoritma kriptografi dan penerapannya untuk menyelesaikan sebuah masalah yang dihadapi oleh pihak yang ingin berkomunikasi secaa aman, serta menuangkannya dalam bentuk makalah sebanyak 10-15 halaman.			

DESKRIPSI SINGKAT MATA KULIAH:	Mata kuliah kriptografi mempelajari tentang penerapan matematika untuk menyelesaikan beberapa permasalahan pada keamanan informasi, seperti kerahasiaan informasi, keutuhan informasi dan otentikasi identitas digital. Beberapa konsep yang dibahas yaitu sejarah kriptografi klasik, pengantar kriptanalisis atau teknik pemecahan sandi rahasia, kriptografi modern, Block Cipher DES dan AES, Stream Cipher, Fungsi Hash, Pertukaran Kunci Diffie-Hellman, kriptografi kunci publik RSA dan ElGamal, Kriptografi Kurva Elliptik, serta tanda tangan digital RSA, ElGamal dan DSA.

MATERI PEMBELAJARAN/POKOK BAHASAN	1. Kriptografi Klasik 2. Teknik Pemecahan Sistem Kriptografi 3. Kriptografi Modern: Block Cipher dan Stream Cipher 4. Kriptografi Kunci Publik 5. Kriptografi Kurva Eliptik 6. Fungsi Hash dan Tanda Tangan Digital 7. Pengantar Kriptografi Post-Quantum
PUSTAKA	UTAMA
	1. Stinson Douglas R., 2019, Cryptography Theory and Practice, Fourth Edition, CRC Press. 2. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, 2014, Introduction to Mathematical Cryptography 2nd Edition, Springer.
	PENDUKUNG
	1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 1996, Handbook of Applied Cryptography, CRC Press. 2. Tim Lemsaneg, 2007, Jelajah Kriptologi, Lembaga Sandi Negara, Jakarta
MEDIA PEMBELAJARAN	White Board, Slide Presentasi, Video, Software CrypTool
TEAM TEACHING	1. Muhamad Zaki Riyanto, M.Sc.
MATA KULIAH SYARAT	

MINGGU KE	SUB CP MK (SEBAGAI KEMAMPUAN AKHIR YANG DIHARAPKAN)	INDIKATOR	KRITERIA DAN BENTUK PENILAIAN	METODE PEMBELAJARAN	MATERI PEMBELAJARAN	BOBOT PENILAIAN
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1	Mampu mengidentifikasi masalah dalam pengiriman pesan	Mahasiswa dapat mengetahui ancaman keamanan informasi/pesan rahasia, sejarah kriptografi, dan menjelaskan pengertian,	Penugasan Mandiri dan Latihan Soal	Ball Throw	Pendahulaun 1. Ancaman keamanan informasi/pesan rahasia 2. Sejarah dan perkembangan	8%

MINGGU KE	SUB CP MK (SEBAGAI KEMAMPUAN AKHIR YANG DIHARAPKAN)	INDIKATOR	KRITERIA DAN BENTUK PENILAIAN	METODE PEMBELAJARAN	MATERI PEMBELAJARAN	BOBOT PENILAIAN
(1)	(2)	(3)	(4)	(5)	(6)	(7)
	rahasia melalui jalur komunikasi yang tidak aman, yaitu masalah kerahasiaan, masalah integritas data, masalah otentikasi dan masalah nir-penyangkalan.	istilah-istilah dasar dan ruang lingkup kriptografi dan kaitannya dengan matematika.			kriptografi 3. Pengertian kriptografi, enkripsi, dekripsi dan kunci rahasia 4. Kaitan antara kriptografi dan matematika, khususnya aljabar dan teori bilangan	
2	Mampu menjelaskan konsep dasar dan jenis-jenis kriptografi yang meliputi konsep enkripsi dan dekripsi. Mahasiswa memiliki pengetahuan dan pemahaman tentang kriptografi klasik, yaitu proses enkripsi-dekripsi dilakukan secara manual	Mahasiswa dapat menyelesaikan enkripsi dan dekripsi suatu pesan rahasia menggunakan sistem kriptografi klasik, yaitu sandi Caesar, sandi affine, sandi permutasi dan sandi substitusi, serta sandi yang digunakan di perang dunia, seperti sandi Playfair dan ADFGVX.	Penugasan Mandiri dan Latihan Soal	Do it your self dan The power of two	Kriptografi Klasik I 1. Sandi Caesar 2. Sandi Affine 3. Sandi Permutasi 4. Sandi Substitusi 5. Sandi Playfair 6. Sandi ADFGVX	7%
3	Mampu menjelaskan konsep dasar dan	Mahasiswa dapat menyelesaikan enkripsi dan dekripsi suatu pesan rahasia	Penugasan Mandiri dan Latihan Soal	Do it your self dan The power of two	Kriptografi Klasik II 1. Sandi Hill 2. Sandi Vigenere	7%

MINGGU KE	SUB CP MK (SEBAGAI KEMAMPUAN AKHIR YANG DIHARAPKAN)	INDIKATOR	KRITERIA DAN BENTUK PENILAIAN	METODE PEMBELAJARAN	MATERI PEMBELAJARAN	BOBOT PENILAIAN
(1)	(2)	(3)	(4)	(5)	(6)	(7)
	jenis-jenis kriptografi yang meliputi konsep enkripsi dan dekripsi. Mahasiswa memiliki pengetahuan dan pemahaman tentang kriptografi klasik, yaitu proses enkripsi-dekripsi dilakukan secara manual	menggunakan sistem kriptografi klasik, yaitu sandi Hill, sandi Vigenere dan Auto Key Cipher. Mahasiswa dapat memahami konsep sandi aliran (stream cipher) .			3. Auto Key Cipher 4. LFSR key stream generator 5. One-Time Pad	
4	Mahasiswa memiliki pengetahuan dan pemahaman tentang kriptanalisis, yaitu cara memecahkan algoritma kriptografi	Mahasiswa dapat memahami konsep pemecahan sandi rahasia. Mahasiswa dapat melakukan pemecahan sandi Caesar, sandi Hill dan Sandi Substitusi melalui teknik analisis frekuensi dalam bahasa Inggris dan bahasa Indonesia.	Penugasan Mandiri dan Latihan Soal	Brain storming	Kriptanalisis I 1. Pengertian konsep kriptanalisis/ pemecahan sandi rahasia 2. Kriptanalisis Shift Cipher dan Affine Cipher 3. Analisis Frekuensi untuk kriptanalisis sandi substitusi	7%
5	Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan informasi rahasia, yaitu algoritma kriptografi klasik	Mahasiswa dapat melakukan pemecahan sandi Vigenere menggunakan teknik analisis frekusensi dan Index of Coincidence dalam bahasa Inggris dan bahasa Indonesia.	Penugasan Mandiri dan Latihan Soal	Team inversigation	Kriptanalisis II 1. Index of Coincidence 2. Kriptanalisis sandi Vigenere	7%

MINGGU KE	SUB CP MK (SEBAGAI KEMAMPUAN AKHIR YANG DIHARAPKAN)	INDIKATOR	KRITERIA DAN BENTUK PENILAIAN	METODE PEMBELAJARAN	MATERI PEMBELAJARAN	BOBOT PENILAIAN
(1)	(2)	(3)	(4)	(5)	(6)	(7)
6	Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan informasi rahasia, yaitu algoritma DES dan AES	Mahasiswa dapat menentukan penjadwalan kunci dan melakukan proses enkripsi berbasis jaringan substitusi permutasi. Selain itu, dapat menentukan fungsi dekripsi melalui invers permutasi dan invers substitusi.	Penugasan Mandiri dan Latihan Soal	Team investigation	Sandi Blok Berbasis SPN 1. Pendahuluan Kriptografi Modern 2. Produk Sistem Kriptografi 3. Enkripsi-derkipsi berbasis Jaringan Substitusi-Permutasi/ Substitution-Permutation Network (SPN)	7%
7	Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan informasi rahasia, yaitu algoritma DES dan AES	Mahasiswa dapat memahami proses enkripsi-dekripsi algoritma sandi blok DES dan AES yang bertipe jaringan substitusi-permutasi.	Penugasan Mandiri dan Latihan Soal	Gallery session	Kriptografi Modern: Sandi Blok 1. Algoritma DES 2. Algoritma AES 3. Mode Operasi	7%
Evaluasi Tengah Semester: Melakukan validasi hasil penilaian dan evaluasi						
8	Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan informasi rahasia, yaitu protokol pertukaran kunci Diffie-Hellman	Mahasiswa dapat menjelaskan solusi dari masalah distribusi kunci yang dihadapi oleh sistem kriptografi kunci rahasia (simetris) menggunakan protokol perjanjian kunci dan menghitung proses perjanjian kunci Diffie-Hellman.	Penugasan Mandiri dan Latihan Soal	Guided teaching	Protokol Perjanjian Kunci 1. Masalah distribusi kunci 2. Grup Siklik Zp* 3. Masalah logaritma diskrit 4. Perjanjian Kunci Diffie-Hellman	8%
9	Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan	Mahasiswa dapat menjelaskan solusi dari masalah distribusi kunci yang dihadapi oleh sistem kriptografi kunci rahasia (simetris) menggunakan	Penugasan Mandiri dan Latihan Soal	Gallery session	Algoritma RSA 1. Masalah distribusi kunci 2. Masalah faktorisasi 3. Penerapan masalah faktorisasi	7%

MINGGU KE	SUB CP MK (SEBAGAI KEMAMPUAN AKHIR YANG DIHARAPKAN)	INDIKATOR	KRITERIA DAN BENTUK PENILAIAN	METODE PEMBELAJARAN	MATERI PEMBELAJARAN	BOBOT PENILAIAN
(1)	(2)	(3)	(4)	(5)	(6)	(7)
	informasi rahasia, yaitu algoritma kriptografi RSA	enkripsi kunci publik, dan memahami masalah faktorisasi yang digunakan oleh algoritma RSA.			pada enkripsi kunci publik 4. Algoritma kriptografi kunci publik RSA	
10	Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan informasi rahasia, yaitu algoritma kriptografi ElGamal	Mahasiswa dapat memahami masalah logaritma diskrit dan penerapannya pada algoritma kunci publik ElGamal untuk proses enkripsi-dekripsinya.	Penugasan Mandiri dan Latihan Soal	Gallery session	Algoritma ElGamal 1. Penerapan masalah logaritma diskrit pada enkripsi kunci publik 2. Algoritma kriptografi kunci publik ElGamal	7%
11	Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan informasi rahasia, yaitu algoritma kriptografi kurva elliptik	Mahasiswa dapat melakukan operasi penjumlahan dan perkalian skalar pada grup kurva elliptik, kemudian menerapkannya pada algoritma ElGamal	Penugasan Mandiri dan Latihan Soal	Metaplano session	Kriptografi Kurva Elliptik 1. Masalah logaritma diskrit atas grup kurva elliptik 2. Algoritma ElGamal menggunakan grup kurva elliptik	7%
12	Mampu menguji integritas data menggunakan fungsi hash, dan menerapkannya untuk mendeteksi	Mahasiswa dapat menerapankan fungsi hash dan tanda tangan digital untuk proses integritas autentikasi data	Penugasan Mandiri dan Latihan Soal	Information search	Fungsi Hash, Tandatangan Digital RSA dan ElGamal 1. Keamanan informasi yang berkaitan dengan keaslian pesan dan otentikasi pihak pengirim	7%

MINGGU KE	SUB CP MK (SEBAGAI KEMAMPUAN AKHIR YANG DIHARAPKAN)	INDIKATOR	KRITERIA DAN BENTUK PENILAIAN	METODE PEMBELAJARAN	MATERI PEMBELAJARAN	BOBOT PENILAIAN
(1)	(2)	(3)	(4)	(5)	(6)	(7)
	kesalahan penulisan ayat Al-Qur'an. Mampu menganalisis dan menerapkan algoritma kriptografi untuk pengamanan informasi rahasia, yaitu algoritma tandatangan digital RSA dan ElGamal. Mampu mengidentifikasi algoritma kriptografi yang tepat untuk menyelesaikan beberapa masalah tertentu terkait dengan pengamanan informasi rahasia				2. Fungsi hash dan aplikasinya 3. Konsep tandatangan digital 4. Tandatangan Digital RSA 5. Tandatangan Digital ElGamal	
13	Mampu menjelaskan perkembangan post-quantum cryptography untuk non-commutative cryptography, lattice-based cryptography dan code-based cryptography.	Mahasiswa dapat menyebutkan sejarah dan perkembangan serangan pada kriptografi menggunakan komputer kuantum	Penugasan Mandiri dan Latihan Soal	Information search	Post-Quantum Cryptography 1. Sejarah dan perkembangan komputer kuantum dan serangannya 2. Protokol pertukaran kunci berbasis masalah pada struktur aljabar non-komutatif	7%

MINGGU KE	SUB CP MK (SEBAGAI KEMAMPUAN AKHIR YANG DIHARAPKAN)	INDIKATOR	KRITERIA DAN BENTUK PENILAIAN	METODE PEMBELAJARAN	MATERI PEMBELAJARAN	BOBOT PENILAIAN
(1)	(2)	(3)	(4)	(5)	(6)	(7)
14	Mampu menjelaskan perkembangan post-quantum cryptography untuk non-commutative cryptography, lattice-based cryptography dan code-based cryptography.	Mahasiswa dapat memahami sejarah dan perkembangan sistem kriptografi asimetris yang tahan terhadap serangan komputer kuantum	Penugasan Mandiri dan Latihan Soal	Gallery session	Perkembangan Sistem Kriptografi Asimetris pada Post-Quantum Cryptogoraphy 1. Sejarah dan perkembangan lattice-based cryptography 2. Sejarah dan perkembangan code-based cryptography	7%
Evaluasi Akhir Semester: Melakukan validasi hasil penilaian akhir dan menentukan kelulusan mahasiswa						

Integrasi-Interkoneksi

1. Matakuliah pendukung integrasi-interkoneksi:
2. Level integrasi-interkoneksi
   a. Materi
   b. Metodologi
3. Proses integrasi-interkoneksi:

Disusun oleh:	Diperiksa oleh:		Disahkan oleh:
Dosen Pengampu	Penanggungjawab Keilmuan	Ketua Program Studi	Dekan
Muhamad Zaki Riyanto, M.Sc	Muhamad Zaki Riyanto, M.Sc.	Muchammad Abrori, S.Si, M.Kom.	Dr. Hj. Khurul Wardati, M.Si.