RENCANA PEMBELAJARAN SEMESTER

(BERDASARKAN PERMENRISTEKDIKTI NO. 44/2015 SNPT PASAL 12)

MATA KULIAH : KRIPTOGRAFI
SKS : 2 (DUA) SKS
KODE : 1761332
PROGRAM STUDI : MATEMATIKA
SEMESTER : 7 (TUJUH)
NAMA DOSEN PENGAMPU : MUHAMMAD KHUDZAIFAH, M.Si
CAPAIAN PEMBELAJARAN MATA KULIAH :

1. Memiliki motivasi dan keinginan yang tinggi disertai kesadaran akan pentingnya memahami, mempelajari, dan mengembangkan Kriptografi.
2. Memiliki dan mengembangkan pengetahuan dan mengetahui dan menggali sumber-sumber pengetahuan beserta obyek, alat dan metode pembenarannya dalam memahami, mempelajari, dan mengembangkan Kriptografi.
3. Memiliki dan mengembangkan keterampilan dalam memahami, mempelajari, dan mengembangkan E Kriptografi.
4. Memiliki dan mengembangkan pengalaman untuk merefleksikan diri dalam komunitas sosialnya dalam mengembangkan Kriptografi.

Pertemuan Ke-	Kemampuan yang Diharapkan pada Setiap Pertemuan	Bahan Kajian	Metode Pembelajaran	Waktu Belajar (Menit)	Pengalaman Belajar Mahasiswa (Deskripsi Tugas)	Kriteria, Indikator dan Bobot Penilaian	Daftar Referensi yang digunakan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Ke-1	Mahasiswa memahami rencana pembelajaran semester dan deskripsi tugas yang harus diselesaikan.	Kontrak Perkuliahan dan Pengenalan Materi	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan dan terlibat aktif dalam tanya jawab.	1. Tugas mandiri dan kelompok, bobot:20% 2. Keaktifan dalam tanya jawab, bobot: 10%	
Ke-2	Mahasiswa mengetahui dan memahami pengantar dan dasar-dasar kriptografi	1. Definisi Kriptografi 2. Sejarah Kriptografi 3. Kriptanalisis 4. Kriptografi simetri dan kriptografi nirsimetri 5. Fungsi Hash 6. Kriptografi di Indonesia	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, dan terlibat aktif dalam tanya jawab.	1. Tugas mandiri dan kelompok, bobot:20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan

Pertemuan Ke-	Kemampuan yang Diharapkan pada Setiap Pertemuan	Bahan Kajian	Metode Pembelajaran	Waktu Belajar (Menit)	Pengalaman Belajar Mahasiswa (Deskripsi Tugas)	Kriteria, Indikator dan Bobot Penilaian	Daftar Referensi yang digunakan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Ke-3	Mahasiswa mengetahui, memahami dan terampil menggunakan ilmu matematika dalam kriptografi	1. Fungsi 2. Kombinatorial 3. Teori Peluang 4. Teori Informasi 5. Teori Bilangan 6. Aljabar Abstrak	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, dan terlibat aktif dalam tanya jawab.	1. Tugas mandiri, bobot:20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-4	Mahasiswa mengetahui dan memahami serangan terhadap kriptografi	1. Jenis serangan pada kriptografi 2. Keamanan algoritma kriptografi 3. Kompleksitas serangan	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, dan terlibat aktif dalam tanya jawab.	1. Tugas mandiri, bobot:20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-5	Mahasiswa mengetahui dan memahami kriptografi klasik	1. Cipher subtitusi 2. Jenis-jenis cipher substitusi 3. Cipher transposisi 4. Super enkripsi 5. Metode analisis frekuensi 6. Vigenere cipher 7. Playfair cipher 8. Hill cipher 9. Enigma cipher 10. One-Time Pad	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab.	1. Tugas mandiri, bobot:20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-6	Mahasiswa mengetahui dan memahami Kriptografi modern	1. Rangkaian bit dan operasinya 2. Kategori cipher untuk data digital 3. Cipher alir 4. Linear feedback shift register 5. Electronic code book 6. Cipher block chaining 7. Cipher feedback 8. Output feedback 9. Counter mode 10. Prinsip-prinsip perancangan cipher blok	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan

Pertemuan Ke-	Kemampuan yang Diharapkan pada Setiap Pertemuan	Bahan Kajian	Metode Pembelajaran	Waktu Belajar (Menit)	Pengalaman Belajar Mahasiswa (Deskripsi Tugas)	Kriteria, Indikator dan Bobot Penilaian	Daftar Referensi yang digunakan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Ke-7	Mahasiswa mengetahui dan memahami review beberapa cipher alir dan cipher blok	1. RC4 2. A5 3. DES 4. Double DES dan Triple DES 5. GOST 6. RC5 7. RC6 8. Advance Encryption Standard (AES)	Ekspositori dan Tanya Jawab	100 Menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-8	UJIAN TENGAH SEMESTER	Pertemuan ke-2 s/d ke-7	Tes tulis	60 menit	Mengerjakan soal tes	Bobot: 25%	
Ke-9	Mahasiswa mengetahui dan memahami Kriptografi kunci-publik	1. Konsep kriptografi kunci-publik 2. Aplikasi kriptografi kunci-publik 3. Algoritma RSA 4. Algoritma pertukaran kunci differ-hellman 5. Algoritma elgamal 6. Algoritma knapsack 7. Algoritma untuk perpangkatan modulo 8. Pembangkitan bilangan prima	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-10	Mahasiswa mengetahui dan memahami pembangkitan bilangan acak	1. Linear congruential generator (LCG) 2. Blum-blum shub 3. CSPRNG berbasis algoritma RSA 4. CSPRNG berbasis chaos	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab.	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-11	Mahasiswa mengetahui dan memahami fungsi hash satu arah	1. Fungsi hash satu arah 2. Algoritma MD5 3. Secure Hash Algorithm 4. Message Authentication Code 5. Algoritma MAC	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan

Pertemuan Ke-	Kemampuan yang Diharapkan pada Setiap Pertemuan	Bahan Kajian	Metode Pembelajaran	Waktu Belajar (Menit)	Pengalaman Belajar Mahasiswa (Deskripsi Tugas)	Kriteria, Indikator dan Bobot Penilaian	Daftar Referensi yang digunakan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Ke-12	Mahasiswa mengetahui dan memahami tanda tangan digital	1. Penandatanganan dengan cara mengenkripsi pesan 2. Tanda tangan digital dengan kombinasi fungsi hash dan kriptografi kunci-publik 3. Digital standard algorithm (DSA)	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-13	Mahasiswa mengetahui dan memahami kriptografi kurva eliptik di dalam kriptografi	1. Kurva eliptik 2. Elliptic curve Diffie-Hellman 3. Elliptic curve ElGamal Cryptosystem 4. Elliptic curve Digital Signature Algorithm 5. Pengkodean pesan menjadi titik di dalam kurva eliptik	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-14	Mahasiswa mengetahui dan memahami manajemen kunci	1. Pembangkitan kunci 2. Penyebaran kunci 3. Penyimpanan kunci 4. Penggunaan kunci 5. Perubahan kunci 6. Penghancuran kunci	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-15	Mahasiswa mengetahui dan memahami steganografi	1. Sejarah steganografi 2. Konsep dan terminology 3. Metode LSB 4. Kombinasi steganografi dengan kriptografi 5. Steganalysis 6. Watermarking 7. Noiseless steganography	Ekspositori dan Tanya Jawab	100 menit	Menyimak penjelasan, mengerjakan latihan soal, membaca buku dari literatur, melakukan percobaan secara berkelompok dan terlibat aktif dalam tanya jawab	1. Tugas mandiri, bobot: 20% 2. Keaktifan dalam tanya jawab, bobot: 10%	Munir, Rinaldi. 2019. KRIPTOGRAFI Edisi kedua. Bandung: Informatika dan referensi lain yang relevan
Ke-16	UJIAN AKHIR SEMESTER	Pertemuan ke-9 s/d ke-15	Tes tulis	60 menit	Mengerjakan soal tes	Bobot: 25%	

Malang,_____
Dosen Pengampu Mata Kuliah

MUHAMMAD KHUDZAIFAH, MSi