

RENCANA PEMBELAJARAN SEMESTER (RPS)  
MATA KULIAH : KRIPTOGRAFI  
PROGRAM STUDI TEKNOLOGI INFORMASI  
FAKULTAS SAINS DAN TEKNOLOGI UIN AR-RANIRY BANDA ACEH

**A IDENTITAS**

1	Prodi	Teknologi Informasi
2	Kode Mata kuliah	2032TI046
3	Nama Mata kuliah	KRIPTOGRAFI
4	Semester/SKS	6 / 3 sks
5	Jenis Mata Kuliah	MK KEAHLIAN DAN KETRAMPILAN (MKK)
6	Koordinator Mata Kuliah	2027018303   Malahayati, M.T.
7	Dosen Pengampu	Malahayati, M.T

**B CAPAIAN PEMBELAJARAN LULUSAN (CPL-Prodi)**

- 1 Sikap
  - a Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religious (S1)
  - b Mampu menginternalisasi dan Mengaktualisasi nilai, norma, etika dan Integritas akademik (S7)
- 2 Pengetahuan
  - a Menguasai substansi materi, struktur, dan pola pikir keilmuan Teknologi Informasi (P1)
  - b Mengetahui metode identifikasi, memformulasi, memecahkan masalah dan menemukan solusi dalam teknologi teknologi informasi (P4)
  - c Menguasai teori dan konsep-konsep dasar yang mendasari keilmuan teknologi Informasi (P9)
  - d Menguasai bidang bidang yang berfokus pada keilmuan teknologi informasi serta mampu beradaptasi dengan perkembangan ilmu pengetahuan dan teknologi terkini (P12)
  - e Memiliki latar belakang untuk meneruskan pendidikan pada tahap selanjutnya (P13)
- 3 Keterampilan Umum
  - a Mampu mengkaji implikasi pengembangan dan implementasi ilmu pengetahuan dan teknologi berdasarkan kaidah, tata cara dan etika ilmiah dalam rangka menghasilkan solusi, gagasan, dan desain (KU2)
  - b Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahlian Teknologi Informasi, berdasarkan hasil analisis informasi dan data (KU4)
- 4 Keterampilan Khusus

**C CAPAIAN PEMBELAJARAN MATA KULIAH (CPMK)**

- 1 Mahasiswa dapat mengemukakan beberapa terminologi dalam kriptografi dan sejarah kriptografi
- 2 Mahasiswa dapat menganalisis landasan matematika terkait kriptografi
- 3 mahasiswa dapat menganalisis jenis serangan dalam kriptografi
- 4 Mahasiswa dapat mengenal beberapa jenis algoritma klasik dan modern
- 5 Mahasiswa dapat mengaplikasikan beberapa jenis algoritma kriptografi terkait permasalahan sehari-hari

**D DESKRIPSI MATA KULIAH**

Mata kuliah kriptografi merupakan salah satu mata kuliah yang wajib diikuti oleh seluruh mahasiswa prodi Teknologi Informasi. Mata kuliah ini disampaikan melalui materi: Pengantar kriptografi; Landasan Matematika terkait kriptografi; Serangan pada kriptografi, Kriptografi Klasik; Kriptografi Modern; dan Metode Analisis Frekuensi pada Kriptografi. Proses pembelajaran matakuliah ini dilakukan dalam bentuk kuliah dan praktek. Pembelajaran mata kuliah ini akan dievaluasi melalui sikap dan tata nilai, kognitif dan ketrampilan yang ditunjukkan oleh mahasiswa melalui keaktifan selama dalam pendidikan serta penyelesaian tugas yang diberikan.

**E MATRIKS KEGIATAN PEMBELAJARAN**

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
1	Mahasiswa mampu menunjukkan sikap menerima kontrak perkuliahan dengan baik dan tanggung jawab	Pendahuluan <ul style="list-style-type: none"> <li>Rencana Pembelajaran Semester</li> <li>Kontrak Kuliah</li> <li>Aturan Penilaian</li> </ul>	X			Kuliah <ul style="list-style-type: none"> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3x50" TKT 3x60" TKM 3x60"	PTM <ul style="list-style-type: none"> <li>Mendapatkan penjelasan tentang kontrak kuliah</li> <li>Mendapatkan penjelasan tentang materi yang akan dipelajari dalam perkuliahan kriptografi</li> </ul> TKT Tugas 1: Menyusun ringkasan materi TKM Tugas 2: Membaca referensi lain yang berkaitan dengan materi ajar dan membuat beberapa catatan penting	Bentuk penilaian <ul style="list-style-type: none"> <li>Sikap (komunikasi dan santun)</li> <li>Keaktifan dalam menjawab</li> <li>Ketepatan menjelaskan pengertian materi yang ditanyakan</li> </ul>	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London
2	<ul style="list-style-type: none"> <li>Mahasiswa mampu mengartikan beberapa terminologi dalam kriptografi</li> <li>Mahasiswa mampu mengemukakan sejarah dan aplikasi kriptografi dalam kehidupan sehari-hari</li> </ul>	Pengantar Kriptografi <ul style="list-style-type: none"> <li>Beberapa termonilogy: sender, receiver, plaintext, ciphertext, cryptogram, enkripsi, dekripsi, kunci</li> <li>Sejarah dan aplikasi kriptografi, kegunaan kriptografi</li> <li>Kriptografi dalam kehidupan sehari-hari</li> </ul>	X			PTM <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan definisi atau terminologi dalam kriptografi</li> <li>Mahasiswa dapat menjelaskan sejarah dan aplikasi kriptografi</li> <li>Mahasiswa dapat menjelaskan penggunaan Kriptografi dalam kehidupan sehari-hari</li> </ul> TKT Tugas 3: Menyelesaikan soal latihan terkait Terminologi dalam Kriptografi TKM Tugas 4: Menyelesaikan soal tugas yang diberikan oleh dosen terkait aplikasi kriptografi dalam kehidupan sehari-hari	PTM 3x50" TKT 3x60" TKM 3x60"	PTM <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan definisi atau terminologi dalam kriptografi</li> <li>Mahasiswa dapat menjelaskan sejarah dan aplikasi kriptografi</li> <li>Mahasiswa dapat menjelaskan penggunaan Kriptografi dalam kehidupan sehari-hari</li> </ul> TKT Tugas 3: Menyelesaikan soal latihan terkait Terminologi dalam Kriptografi TKM Tugas 4: Menyelesaikan soal tugas yang diberikan oleh dosen terkait aplikasi kriptografi dalam kehidupan sehari-hari	Bentuk Penilaian: <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa: <ul style="list-style-type: none"> <li>Ketepatan dalam menjelaskan beberapa terminologi dalam kriptografi</li> <li>Ketepatan dalam menjelaskan pemakaian aturan pembuatan distribusi frekuensi</li> <li>Mampu menyelesaikan soal sesuai langkah-langkah sistematis</li> </ul> Menguasai materi yang dijelaskan minimal 80 %	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
3	Mahasiswa mampu menghitung serta menerapkan teori bilangan dan aljabar abstrak	Landasan Matematika <ul style="list-style-type: none"> <li>Fungsi, kombinatorial dan teori peluang</li> <li>Teori Informasi</li> <li>Teori Bilangan</li> <li>Aljabar Abstrak</li> </ul>	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3x50" TKT 3x60" TKM 3x60"	<p>PTM</p> <ul style="list-style-type: none"> <li>Mahasiswa mendapatkan penjelasan tentang materi ajar</li> <li>Mahasiswa berdiskusi terhadap materi ajar</li> <li>Mahasiswa menyelesaikan beberapa contoh soal yang diberikan oleh dosen</li> </ul> <p>TKT</p> <p>Tugas 5: Menyelesaikan soal latihan tentang fungsi, kombinatorial, teori peluang dan teori informasi</p> <p>TKM</p> <p>Tugas 6: Menyelesaikan soal tugas yang diberikan oleh dosen tentang fungsi, kombinatorial, teori peluang dan teori informasi</p>	<p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> <p>Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa:</p> <ul style="list-style-type: none"> <li>Ketepatan dalam menggunakan dan menghitung fungsi, kombinatorial dan teori peluang</li> <li>Ketepatan dalam menggunakan dan menghitung teori informasi</li> </ul> <p>Menguasai materi yang dijelaskan minimal 80 %</p>	<ol style="list-style-type: none"> <li>Munir, R., Kriptografi, Penerbit Informatika, 2019.</li> <li>Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London</li> </ol>
4	Mahasiswa mampu menghitung serta menerapkan teori bilangan dan aljabar abstrak	Landasan Matematika <ul style="list-style-type: none"> <li>Fungsi, kombinatorial dan teori peluang</li> <li>Teori Informasi</li> <li>Teori Bilangan</li> <li>Aljabar Abstrak</li> </ul>	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3x50" TKT 3x60" TKM 3x60"	<p>PTM</p> <ul style="list-style-type: none"> <li>Mahasiswa mendapatkan penjelasan tentang materi ajar</li> <li>Mahasiswa berdiskusi terhadap materi ajar</li> <li>Mahasiswa menyelesaikan beberapa contoh soal yang diberikan oleh dosen</li> </ul> <p>TKT</p> <p>Tugas 5: Menyelesaikan soal latihan tentang teori bilangan dan aljabar abstrak</p> <p>TKM</p> <p>Tugas 6: Menyelesaikan soal tugas yang diberikan oleh dosen tentang teori bilangan dan aljabar abstrak</p>	<p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> <p>Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa</p> <ul style="list-style-type: none"> <li>Ketepatan dalam menggunakan dan menghitung teori bilangan</li> <li>Ketepatan dalam menggunakan dan menghitung kaidah aljabar abstrak</li> </ul> <p>Menguasai materi yang dijelaskan minimal 80 %</p>	<ol style="list-style-type: none"> <li>Munir, R., Kriptografi, Penerbit Informatika, 2019.</li> <li>Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London</li> </ol>

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
5	<ul style="list-style-type: none"> <li>Mahasiswa mampu mengemukakan jenis-jenis serangan terhadap kriptografi dan metode penyadapan</li> <li>Mahasiswa mampu mengklasifikasi kompleksitas serangan serta pentingnya keamanan algoritma kriptografi</li> </ul>	<b>Serangan Pada Kriptografi</b> <ul style="list-style-type: none"> <li>Beberapa jenis serangan terhadap kriptografi: exhaustive attack dan analytical attack</li> <li>Metode penyadapan, kompleksitas serangan</li> <li>Keamanan algoritma kriptografi</li> </ul>	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3 x 50" TKT 3x60" TKM 3x60"	<b>PTM</b> <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan exhaustive attack</li> <li>Mahasiswa dapat menjelaskan analytical attack</li> </ul> <b>TKT</b> Tugas 7: Menyelesaikan soal latihan tentang metode penyadapan TKM Tugas 8: Menyelesaikan soal tugas yang diberikan dosen tentang keamanan algoritma kriptografi	Bentuk Penilaian: <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa <ul style="list-style-type: none"> <li>Ketepatan dalam menjelaskan exhaustive attack</li> <li>Ketepatan dalam menjelaskan analytical attack</li> </ul> Menguasai materi yang dijelaskan minimal 80 %	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London
6	Mahasiswa mampu mengkonsepkan algoritma kriptografi klasik, yaitu: cipher substitusi dan cipher transposisi	<b>Kriptografi Klasik</b> <ul style="list-style-type: none"> <li>Cipher substitusi (caesar cipher dan kriptanalisis terhadap caesar cipher)</li> <li>Jenis-jenis cipher substitusi (abjad tunggal, abjad banyak, substitusi homofonik, substitusi poligram)</li> <li>Cipher transposisi</li> </ul>	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3x50" TKT 3x60" TKM 3x60"	<b>PTM</b> <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan beberapa jenis algoritma kriptografi klasik</li> <li>Mahasiswa dapat menyelesaikan soal tentang plainteks dari cipherteks</li> </ul> <b>TKT</b> Tugas 9: Menyelesaikan soal latihan tentang algoritma cipher substitusi dan cipher transposisi	Bentuk Penilaian: <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa: <ul style="list-style-type: none"> <li>Ketepatan dalam menjelaskan jenis algoritma kriptografi klasik</li> <li>Ketepatan pendugaan plainteks dari cipherteks</li> <li>Mampu menyelesaikan soal sesuai langkah-langkah sistematis</li> </ul> Menguasai materi yang dijelaskan minimal 80 %	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
7	Mahasiswa mampu mengkonsepkan dan mensimulasikan vigenere cipher dan playfair cipher	Kriptografi Klasik <ul style="list-style-type: none"> <li>Vigenere cipher</li> <li>Playfair cipher</li> </ul>	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3x50" TKT 3x60" TKM 3x60"	PTM <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan beberapa jenis algoritma kriptografi klasik</li> <li>Mahasiswa dapat menyelesaikan soal tentang plainteks dari cipherteks</li> </ul> TKT Tugas 9: Menyelesaikan soal latihan tentang vigenere cipher dan playfair cipher TKM Tugas 10: Menyelesaikan soal tugas yang diberikan dosen tentang vigenere cipher dan playfair cipher	Bentuk Penilaian: <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa: <ul style="list-style-type: none"> <li>Ketepatan dalam menjelaskan jenis algoritma kriptografi klasik</li> <li>Ketepatan pendugaan plainteks dari cipherteks</li> <li>Mampu menyelesaikan soal sesuai langkah-langkah sistematis</li> </ul> Menguasai materi yang dijelaskan minimal 80 %	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London
8	Mahasiswa mampu menyelesaikan soal ujian terhadap materi yang diajarkan minimal 85%	Materi ajar 1-7	X				PTM 3x50" Pengayaan Terstruktur 3x60" Pengayaan Mandiri 3x60"	PTM <ul style="list-style-type: none"> <li>Mahasiswa menjawab soal-soal yang diujikan secara tertulis</li> <li>Mahasiswa mengumpulkan kertas jawaban</li> </ul> KT Mahasiswa membahas soal UTS yang diujikan dengan berpedoman pada bahan ajar KM Menyelesaikan soal ujian tambahan yang diberikan dosen	Ketepatan dalam menemukan jawaban pada contoh soal	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
9	Mahasiswa mampu menentukan plainteks dari chiperteks	Metode Analisis Frekuensi pada Kriptografi	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3 x 50" TKT 3x60" TKM 3x60"	<p>PTM</p> <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan prinsip metode analisis frekuensi pada kriptografi</li> </ul> <p>TKT</p> <p>Tugas 11: Menyelesaikan soal latihan tentang metode analisis frekuensi pada kriptografi TKM</p> <p>Tugas 12: Menyelesaikan soal tugas yang diberikan dosen tentang metode analisis frekuensi pada kriptografi</p>	<p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> <p>Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa:</p> <ul style="list-style-type: none"> <li>Ketepatan dalam menjelaskan tentang metode analisis frekuensi pada kriptografi</li> <li>Mampu menyelesaikan soal sesuai langkah-langkah sistematis</li> </ul> <p>Menguasai materi yang dijelaskan minimal 80 %</p>	<ol style="list-style-type: none"> <li>Munir, R., Kriptografi, Penerbit Informatika, 2019.</li> <li>Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London</li> </ol>
10	Mahasiswa mampu mengkonsepkan algoritma kriptografi modern, yaitu cipher alir dan mengemukakan beberapa serangan terhadap cipher alir	<p>Kriptografi Modern</p> <ul style="list-style-type: none"> <li>Algoritma kriptografi modern yakni cipher alir dan beberapa serangan terhadap cipher alir</li> </ul>	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3 x 50" TKT 3x60" TKM 3x60"	<p>PTM</p> <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan prinsip algoritma kriptografi modern</li> <li>Mahasiswa dapat menjelaskan cipher alir dan cipher blok</li> <li>Mahasiswa dapat menjelaskan terkait mode operasi cipher blok</li> </ul> <p>TKT</p> <p>Tugas 13: Menyelesaikan soal latihan tentang teknik kriptografi dalam cipher alir</p> <p>TKM</p> <p>Tugas 14: Menyelesaikan soal tugas yang diberikan dosen tentang cipher alir</p>	<p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> <p>Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa</p> <ul style="list-style-type: none"> <li>Ketepatan dalam menjelaskan tentang cipher alir</li> <li>Mampu menyelesaikan soal sesuai langkah-langkah sistematis</li> </ul> <p>Menguasai materi yang dijelaskan minimal 80 %</p>	

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
11	Mahasiswa mampu mengkonsepkan algoritma kriptografi modern, yaitu cipher blok dan mengemukakan teknik kriptografi modern yang digunakan dalam cipher blok	Kriptografi Modern <ul style="list-style-type: none"> <li>Algoritma cipher block dan teknik kriptografi modern yang digunakan dalam cipher blok</li> </ul>	X			<ul style="list-style-type: none"> <li>Kuliah</li> <li>Diskusi</li> <li>Tanya jawab</li> <li>Penugasan</li> </ul>	PTM 3 x 50 " TKT 3x60" TKM 3x60"	<p>PTM</p> <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan prinsip algoritma kriptografi modern</li> <li>Mahasiswa dapat menjelaskan cipher alir dan cipher blok</li> <li>Mahasiswa dapat menjelaskan terkait mode operasi cipher blok</li> </ul> <p>TKT</p> <p>Tugas 13: Menyelesaikan soal latihan tentang teknik kriptografi dalam cipher blok</p> <p>TKM</p> <p>Tugas 14: Menyelesaikan soal tugas yang diberikan dosen tentang cipher blok</p>	<p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> <p>Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa:</p> <ul style="list-style-type: none"> <li>Ketepatan dalam menjelaskan cipher blok</li> <li>Mampu menyelesaikan soal sesuai langkah-langkah sistematis</li> </ul> <p>Menguasai materi yang dijelaskan minimal 80 %</p>	<ol style="list-style-type: none"> <li>Munir, R., Kriptografi, Penerbit Informatika, 2019.</li> <li>Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London</li> </ol>
12	Mahasiswa mampu mensimulasikan proses enkripsi dan dekripsi menggunakan algoritma caesar cipher	Modul 1 Kriptografi klasik (caesar cipher)	X			<ul style="list-style-type: none"> <li>Praktik</li> <li>Penugasan</li> </ul>	PTM 3 x 50" TKT 3x60" TKM 3x60"	<p>PTM</p> <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan prinsip caesar cipher</li> <li>Mahasiswa dapat menerjemahkan algoritma caesar cipher ke dalam bahasa pemrograman</li> </ul> <p>TKT</p> <p>Tugas 17: Menyelesaikan pemrograman menggunakan caesar cipher</p> <p>TKM</p> <p>Tugas 18:</p> <ul style="list-style-type: none"> <li>Melakukan uji coba program dengan beberapa variasi plainteks untuk proses enkripsi</li> <li>Melakukan uji coba program dengan chiperteks yang diperoleh untuk proses dekripsi</li> </ul>	<p>Bentuk Penilaian:</p> <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> <p>Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa</p> <ul style="list-style-type: none"> <li>Ketepatan melakukan proses enkripsi dan dekripsi menggunakan caesar cipher</li> <li>Mampu menyelesaikan soal sesuai langkah-langkah sistematis</li> </ul> <p>Menguasai materi yang dijelaskan minimal 80 %</p>	<ol style="list-style-type: none"> <li>Munir, R., Kriptografi, Penerbit Informatika, 2019.</li> <li>Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London</li> </ol>

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
13	Mahasiswa mampu mensimulasikan proses enkripsi dan dekripsi menggunakan algoritma vigenere cipher	Modul 2 Kriptografi klasik (vigenere cipher)	X			<ul style="list-style-type: none"> <li>Praktik</li> <li>Penugasan</li> </ul>	PTM 3 x 50" TKT 3x60" TKM 3x60"	PTM <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan prinsip vigenere cipher</li> <li>Mahasiswa dapat menerjemahkan algoritma vigenere cipher ke dalam bahasa pemrograman</li> </ul> TKT Tugas 19: Menyelesaikan pemrograman menggunakan vigenere cipher TKM Tugas 20: <ul style="list-style-type: none"> <li>Melakukan uji coba program dengan beberapa variasi plainteks untuk proses enkripsi</li> <li>Melakukan uji coba program dengan chiperteks yang diperoleh untuk proses dekripsi</li> </ul>	Bentuk Penilaian: <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa ketepatan melakukan proses enkripsi dan dekripsi menggunakan vigenere cipher Menguasai materi yang dijelaskan minimal 80 %	

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
14	Mahasiswa mampu mensimulasikan proses enkripsi dan dekripsi menggunakan algoritma XOR	Modul 3 Kriptografi modern (Algoritma XOR)	X			<ul style="list-style-type: none"> <li>Praktik</li> <li>Penugasan</li> </ul>	PTM 3 x 50" TKT 3x60" TKM 3x60"	PTM <ul style="list-style-type: none"> <li>Mahasiswa dapat menjelaskan prinsip caesar cipher</li> <li>Mahasiswa dapat menerjemahkan algoritma XOR ke dalam bahasa pemrograman</li> </ul> TKT Tugas 21: <ul style="list-style-type: none"> <li>Menyelesaikan pemrograman menggunakan algoritma XOR</li> </ul> TKM Tugas 22: <ul style="list-style-type: none"> <li>Melakukan uji coba program dengan beberapa variasi plainteks untuk proses enkripsi</li> <li>Melakukan uji coba program dengan chiperteks yang diperoleh untuk proses dekripsi</li> </ul>	Bentuk Penilaian: <ul style="list-style-type: none"> <li>Sikap (Komunikasi dan santun),</li> <li>Keaktifan dalam menjawab</li> </ul> Kriteria dan Indikator penilaian adalah ketepatan dan sistematis berupa ketepatan melakukan proses enkripsi dan dekripsi menggunakan algoritma XOR Menguasai materi yang dijelaskan minimal 80 %	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London
15	Mahasiswa mampu menciptakan project enkripsi dan dekripsi	Membuat project enkripsi dan dekripsi menggunakan algoritma apa saja yang telah dipelajari	X				PTM 3 x 50" TKT 3x60" TKM 3x60"	Mahasiswa menjalankan program dengan baik dan benar	Ketepatan dalam memperoleh chiperteks dan menemukan kembali plainteks Menguasai materi yang dijelaskan minimal 80 %	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London
16	Mahasiswa mampu menjawab soal ujian terhadap materi ujian yang sudah diajarkan minimal 85%	Semua materi yang telah dipelajari	X			UAS teori	PTM 3x50" Pengayaan Terstruktur 3x60" Pengayaan Mandiri 3x60	Mahasiswa menjawab soal-soal yang diujikan dengan baik dan benar	Ketepatan dalam menemukan jawaban pada contoh soal	1. Munir, R., Kriptografi, Penerbit Informatika, 2019. 2. Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London
17										
18										
19										
20										

## F REFERENSI

1 Wajib

- a Munir, R., Kriptografi, Penerbit Informatika, 2019.
- b Stinson, R., Cryptography, Theory and Practice, 3rd ed, Chapman and Hall, London

2 Pendukung

Mengetahui:  
Ketua Prodi Teknologi Informasi

Banda Aceh, 19 Januari 2024  
Koordinator/Dosen Mata Kuliah

Ima Dwitawati, M.B.A.  
NIDN : 0113108204

Malahayati, M.T.  
NIDN : 2027018303

## TUGAS KEGIATAN TERSTRUKTUR (TKT)

Nama Mata Kuliah            KRIPTOGRAFI  
Kode mata Kuliah            2032TI046  
Semester/SKS                6/3 sks

1 Tujuan Tugas            Mahasiswa mampu menguasai materi Kriptografi dan mampu menyelesaikan permasalahan/ccontoh soal yang terdapat pada materi Kriptografi

2 Uraian Tugas

- |                                                     |                                                                         |
|-----------------------------------------------------|-------------------------------------------------------------------------|
| a Obyek garapan                                     | Materi perkuliahan yang terdapat dalam RPS                              |
| b Yang harus dikerjakan dan batasan-batasan         | Menyelesaikan soal latihan                                              |
| c Metode/cara pengerjaan, acuan yang digunakan      | Menuliskan jawaban di buku catatan, handbook dan catatan yang diberikan |
| d Deskripsi luaran tugas yang dihasilkan/dikerjakan | Adanya catatan yang lebih banyak soal dan pembahasan                    |

3 Kriteria Penilaian

- |                                    |      |
|------------------------------------|------|
| a Ketepatan penyerahan tugas       | 50 % |
| b Kesempurnaan substansi/isi tugas | 50%  |
| c Desain tugas                     |      |

Mengetahui:  
Ketua Prodi Teknologi Informasi

Banda Aceh, 19 Januari 2024  
Koordinator/Dosen Mata Kuliah

Ima Dwitawati, M.B.A.  
NIDN : 0113108204

Malahayati, M.T.  
NIDN : 2027018303

## TUGAS KEGIATAN MANDIRI (TKM)

Nama Mata Kuliah            KRIPTOGRAFI  
Kode mata Kuliah            2032TI046  
Semester/SKS                6/3 sks

## Capaian Pembelajaran Mata Kuliah (CPMK)

- 1 Mahasiswa dapat mengemukakan beberapa terminologi dalam kriptografi dan sejarah kriptografi
- 2 Mahasiswa dapat menganalisis landasan matematika terkait kriptografi
- 3 mahasiswa dapat menganalisis jenis serangan dalam kriptografi
- 4 Mahasiswa dapat mengenal beberapa jenis algoritma klasik dan modern
- 5 Mahasiswa dapat mengaplikasikan beberapa jenis algoritma kriptografi terkait permasalahan sehari-hari

## Jenis Tugas :

Pengayaan/remedial mata kuliah secara mandiri: Menjawab soal dari handbook atau dari referensi lain

Mengetahui:  
Ketua Prodi Teknologi Informasi

Ima Dwitawati, M.B.A.  
NIDN : 0113108204

Banda Aceh, 19 Januari 2024  
Koordinator/Dosen Mata Kuliah

Malahayati, M.T.  
NIDN : 2027018303

## PENILAIAN SIKAP, PENGETAHUAN DAN KETERAMPILAN

## A. PENILAIAN SIKAP (RUBRIK)

Prediket	Skor Angka	Deskripsi Perilaku
-	-	Menunjukkan sikap religious dalam proses pembelajaran
-	-	Menunjukkan sikap jujur dalam proses pembelajaran
-	-	Menunjukkan sikap disiplin dalam proses pembelajaran
-	-	Menunjukkan sikap bertanggung jawab terhadap tugas yang diberikan dalam proses pembelajaran

Keterangan :

Prediket :

Diisi dengan deskripsi tingkatan nilai, dengan jumlah tingkat yang kerinciannya sesuai dengan yang dikehendaki (sangat baik, baik, cukup, kurang, gagal).

Skor Angka :

Diisi dengan rentang angka yang sesuai dengan tingkat nilai pada kolom jenjang.

## B. KRITERIA PENILAIAN PENGETAHUAN DAN KETERAMPILAN

Nilai Huruf (NH)	Nilai Bobot (NB)	Nilai Angka (NA)	Predikat
A	4.00	90-100	Sangat Baik Sekali
A-	3.67	85-89	Sangat Baik
B+	3.33	78-84	Baik
B	3.00	72-77	Agak Baik
B-	2.67	68-71	Cukup
C+	2.33	65-67	Agak Kurang Baik
C	2.00	60-64	Kurang Baik
D	1.00	50-59	Sangat Kurang Baik
E	0	0-49	Gagal

Mengetahui:  
Ketua Prodi Teknologi Informasi

Banda Aceh, 19 Januari 2024  
Koordinator/Dosen Mata Kuliah

Ima Dwitawati, M.B.A.  
NIDN : 0113108204

Malahayati, M.T.  
NIDN : 2027018303