

**II4031 Kriptografi dan Koding
(Semester II Tahun Ajaran 2023/2024)**

<i>Bobot SKS</i>	: 2
<i>Dosen</i>	: Dr. Rinaldi Munir, M.T
<i>E-mail</i>	: rinaldi@informatika.org
<i>URL kuliah</i>	: http://informatika.stei.itb.ac.id/~rinaldi.munir
<i>Asisten</i>	: Tri Sulthon dan Kinantan Arya Bagaspati
<i>Jadwal kuliah</i>	: Rabu, 13.00 – 15.40

Tujuan Umum Kuliah:

Setelah mengikuti kuliah Kriptografi dan Koding, mahasiswa memahami berbagai teknik pengamanan pesan (*message security*) dengan menggunakan kriptografi. Keamanan pesan meliputi kerahasiaan, otentikasi, integritas, dan nir-penyangkalan (*non-repudiation*). Mahasiswa dapat mengimplementasikan berbagai teknik pengamanan pesan menjadi program komputer.

Tujuan Khusus:

1. Mahasiswa mengerti dasar-dasar kriptografi untuk keamanan pesan.
2. Mahasiswa memahami bermacam-macam algoritma kriptografi dari berbagai jenis (simetri, nirsimetri, fungsi hash)
3. Mahasiswa juga memahami teknik-teknik mengamankan pesan selain kriptografi seperti steganografi.
4. Mahasiswa mampu memilih algoritma kriptografi yang sesuai untuk mengamankan pesan, baik pesan yang terkirim maupun pesan tersimpan (dokumen)
5. Mahasiswa mampu membuat program aplikasi (*coding*) menggunakan kriptografi untuk keamanan pesan.

Prasyarat Kuliah:

1. II2110 Matematika STI
2. II2111 Algoritma dan Struktur Data STI

Lingkup Bahasan:

1. Pengantar kriptografi
2. Ragam cipher klasik

3. Kriptografi modern
4. Kriptografi simetri (stream cipher dan block cipher)
5. Kriptografi asimetri
6. Fungsi hash
7. Tanda-tangan digital
8. Protokol kriptografi
9. Public Key Infrastructure
10. Miscellaneous topics in information security (steganography, watermarking, etc)

Referensi kuliah:

1. Ferguson, Niels, and Schneier, Bruce, *Practical Cryptography*, Wiley, 2003
2. William Stallng, *Cryptography and Network Security, Principle and Practice 5rd Edition*, Pearson Education, Inc., 2015
3. Hans Delfs, Helmut Knebl, *Introduction to Cryptography Principles and Applications*, Second Edition, Springer
4. Douglas R. Stinson, Maura B. Paterson, *Cryptography Theory and Practice*, Fourth Edition
5. Rinaldi Munir, *Kriptografi*, Edisi Kedua, Penerbit Informatika
6. Menezes, Alfred J., Paul C van Oorschot, dan Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. (e-book)
7. Schneier, Bruce, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996

Penilaian :

- | | | |
|--------------------------------|-----------------|--------|
| 1. Ujian Tengah Semester (UTS) | – 1 kali | (25%) |
| 2. Tugas pemrograman | – 3 atau 4 kali | (40%) |
| 3. Ujian Akhir | – 1 kali | (25%) |
| 4. Makalah | – 1 buah | (7,5%) |
| 5. Kehadiran | | (2,5%) |

Lain-lain :

Tugas pemrograman adalah tugas perorangan atau berdua orang (jika cukup kompleks).