

**II4031 Kriptografi dan Koding
(Semester II Tahun Ajaran 2020/2021)**

Bobot SKS : 2
Dosen : Dr. Rinaldi Munir, M.T
E-mail : rinaldi@informatika.org
URL kuliah : <http://informatika.stei.itb.ac.id/~rinaldi.munir>
Asisten : (belum ditentukan)
Jadwal kuliah : Jumat, 9.00 – 10.40

Tujuan Umum Kuliah:

Mahasiswa memahami berbagai penyandian data dan mengkodekannya untuk kebutuhan keamanan data atau informasi.

Tujuan Khusus:

Mahasiswa mampu:

1. Memilih teknik kriptografi yang sesuai untuk mengamankan pesan, baik pesan yang terkirim maupun pesan tersimpan (dokumen)
2. Membuat program aplikasi (coding) untuk tujuan keamanan pesan.

Prasyarat Kuliah:

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

Lingkup Bahasan:

1. Pengantar kriptografi
2. Ragam algoritma kriptografi klasik
3. Kriptografi modern
4. Kriptografi simetri
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 Stallings, *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 | (30%) |
| 2. Ujian Akhir Semester (UAS) | – 1 kali | (30%) |
| 3. Tugas kecil | – 3 buah | (20%) |
| 4. Tugas besar | – 1 buah | (12,5%) |
| 4. Makalah (di akhir semester) | – 1 buah | (5%) |
| 5. Kehadiran | | (2,5%) |

Lain-lain :

Tugas kecil adalah tugas perorangan atau berdua orang. Tugas besar adalah tugas berkelompok. Bahasa pemrograman yang digunakan bebas.