

IF4020 Kriptografi
(Semester II Tahun Ajaran 2022/2023)

<i>Bobot SKS</i>	: 3
<i>Dosen</i>	: Dr. Rinaldi Munir
<i>E-mail</i>	: rinaldi@informatika.org
<i>URL kuliah</i>	: http://informatika.stei.itb.ac.id/~rinaldi.munir
<i>Asisten</i>	: (belum ditentukan)
<i>Jadwal kuliah</i>	: Senin, 13.00 – 15.00, R. 7606 Rabu, 15.00 – 16.00, R. Multimedia

Tujuan Umum Kuliah:

Setelah mengikuti kuliah Kriptografi, mahasiswa memahami berbagai teknik pengamanan pesan (*message security*) dengan menggunakan kriptografi. Keamanan pesan meliputi kerahasiaan, otentikasi, integritas, dan anti-penyangkalan (*non-repudiation*) dan dapat mengimplementasikannya.

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, *watermarking*, *noise-stega*, *secret sharing scheme*, dan kriptografi visual.
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. IF2120 Matematika Diskrit
2. IF2110 Algoritma dan Struktur Data

Lingkup Bahasan:

1. Pengantar kriptografi
2. Landasan matematika untuk kriptografi
3. Ragam cipher klasik

4. Steganografi dan watermarking
3. Kriptografi modern (block cipher dan stream cipher)
4. Kriptografi kunci-simetri
5. Kriptografi kunci-nirsimetri
6. Fungsi hash dan MAC
7. Tanda-tangan digital
8. Protokol kriptografi
9. Public Key Infrastructure (PKI)
10. Pembangkit bilangan acak
11. Kriptografi visual
12. Skema pembagian data rahasia (*secret sharing*)
13. Enkripsi homomorfik

Referensi kuliah:

1. Ferguson, Niels, and Schneier, Bruce, *Practical Cryptography*, Wiley, 2003
2. William Stalling, *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 | (27,5 %) |
| 2. Ujian Akhir Semester (UAS) | – 1 kali | (27,5%) |
| 3. Tugas kecil dan tugas besar | – 3 + 2 kali | (35 %) |
| 4. Tugas membuat makalah | – 1 kali | (7,5 %) |
| 4. Kehadiran (minimal 80% kehadiran agar bisa ikut UAS) | | (2,5%) |

*) Masih tentatif

Lain-lain :

Tugas pemrograman ada yang per orang/dua orang dan ada yang per kelompok (Tucil dan Tubes). Bahasa pemrograman yang digunakan bebas.