Departemen Teknik Informatika
Fakultas Teknologi Industri
Institut Teknologi Bandung

IF5054 Kriptografi
(Semester I Tahun Ajaran 2005/2006)

Silabus Ringkas

Bobot SKS : 3
Dosen : Ir. Rinaldi Munir, MT
E-mail : rinaldi@informatika.org
URL : www.informatika.org/~rinaldi
Asisten : Anugerah Redja Kusuma (IF 2001)
Jadwal kuliah :
1. Kamis, 15.00 - 17.00 di Ruang 7606
2. Jumat, 15.00 – 16.00 di Ruang 7610

Penilaian :
1. Ujian Akhir Semester (UAS)
2. Tugas pemrograman aplikasi (2 kali)
3. Tugas kriptanalisis sederhana (1 kali)
4. Makalah
5. Kehadiran

Bahan Kuliah:
1. Pengantar kriptografi
2. Jenis-jenis serangan (*attack*) pada kriptografi
3. Teori bilangan
4. Algoritma kriptografi klasik
5. Algoritma kriptografi modern
6. *Stream cipher* dan *block cipher*.
7. *Data Encryption Standard* dan *Advanced Encryption Standard*
8. Sistem kriptografi kunci publik
9. Algoritma-algoritma kriptografi kunci-publik (RAS, Elgamal, Knapsack).
10. Fungsi *hash*
11. Otentikasi dan sidik digital (*digital signature*)
12. Protokol kriptografi
13. Manajemen kunci
14. Steganografi dan *watermarking*
15. *Public Key Infrastructure* (*PKI*)
16. Kriptografi dalam kehidupan sehari-hari

Buku teks pegangan kuliah:
1. Schneier, Bruce, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996
2. Menezes, Alfred J., Paul C van Oorschot, dan Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
3. Stalling, W., *Cryptography and Network Security, Principle and Practice 3rd Edition*, Pearson Education, Inc., 2003
4. Rhee, Man Young, *Cryptography and Secure Communications*, McGraw-Hill, 1994
5. Meyer, Carl H. & Matyas, Stephen M., *Cryptography, A New Dimension in Computer Data Security*, John Wiley & Sons, 1982.