Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

IF5054 Kriptografi (3 SKS)

(Semester I Tahun Ajaran 2007/2008)

Dosen : Ir. Rinaldi Munir, MT
E-mail : rinaldi@informatika.org
URL : www.informatika.org/~rinaldi
Asisten : ??
Jadwal kuliah : 1. Senin, 10.00 - 11.00 di Ruang 7602
2. Kamis, 13.00 – 15.00 di Ruang 7602

Penilaian : 1. Tugas pemrograman aplikasi (2 kali) – perkelompok @ 3 orang
2. Tugas kriptanalisis sederhana (1 kali) – per kelompok @ 2 orang
3. Makalah pengganti UTS (1 kali) – per orang
4. Makalah pengganti UAS (1 kali) – per orang
5. Kehadiran

Bahan Kuliah:

1. Pengantar kriptografi
2. Jenis-jenis serangan (*attack*) pada kriptografi
3. Landasan matematika untuk kriptografi
4. Algoritma kriptografi klasik (*Caesar cipher*, Vigenere, Playfair)
5. Teknik analisis frekuensi
6. Algoritma kriptografi modern
7. *Stream cipher* dan *block cipher*.
8. Beberapa algoritma *cipher* blok (*DES*, *TDES*, *GOST*, *RC5*, *AES*)
9. Steganografi dan *watermarking*

---------- **Batas materi untuk makalah I**

10. Kriptografi kunci publik
11. Algoritma-algoritma kriptografi kunci-publik (RSA, ElGamal, Diffie-Hellman, Knapsack).
12. Fungsi *hash* da *MAC*
13. Tanda-tangan digital (*digital signature*)
14. Protokol kriptografi
15. *Public Key Infrastructure* (*PKI*)
16. Manajemen kunci
17. Kriptografi dalam kehidupan sehari-hari

---------- **Batas materi untuk makalah II**

Buku teks pegangan kuliah:

1. Diktat kuliah IF5054 Kriptografi oleh Rinaldi Munir, Prodi IF – STEI 2006
2. Schneier, Bruce, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996
3. Menezes, Alfred J., Paul C van Oorschot, dan Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
4. Stalling, W., *Cryptography and Network Security, Principle and Practice 3rd Edition*, Pearson Education, Inc., 2003
5. Rhee, Man Young, *Cryptography and Secure Communications*, McGraw-Hill, 1994
6. Meyer, Carl H. & Matyas, Stephen M., *Cryptography, A New Dimension in Computer Data Security*, John Wiley & Sons, 1982.