IF4020 Kriptografi

Oleh: Rinaldi Munir
Program Studi Teknik Informatika ITB

Sekolah Teknik Elektro dan Informatika ITB
2019

Tujuan Umum Kuliah IF4020

- Mahasiswa memahami berbagai teknik pengamanan pesan (*message security*) dengan menggunakan nkriptografi

- Keamanan pesan meliputi kerahasiaan, otentikasi, integritas, dan anti-penyangkalan (*non-repudiation*).

Luaran (*outcomes*)

Mahasiswa diharapkan mampu:

1. Memilih teknik kriptografi yang sesuai untuk mengamankan pesan, baik pesan yang terkirim maupun pesan tersimpan (dokumen)

2. Membuat program aplikasi untuk tujuan keamanan pesan.

Prasyarat

1. IF2120 Matematika Diskrit
2. IF2110 Algoritma dan Struktur Data

Penilaian

1. Tubes besar: Tugas pemrograman aplikasi (dua kali) – perkelompok @ 3 orang
2. Tugas kecil (Tucil) (3 sampai 4 kali)
3. UTS
4. Makalah pengganti UAS – per orang
5. Kehadiran (minimal 80%), kurang 80% nilai dikurangi satu tingkat.

Makalah

- Makalah tidak boleh berupa studi literatur, tetapi harus hasil karya nyata (riset skala lab).

- Makalah pengganti UAS topiknya bebas, namun harus berupa hasil riset mandiri tentang aplikasi kriptografi di berbagai bidang.

Silabus Ringkas (*keywords*)

Pengantar, serangan pada kriptografi, algoritma kriptografi klasik, kriptanalisis, s*tream cipher* dan *block cipher*, sistem kriptografi kunci-publik, fungsi *hash* dan *MAC*, tanda tangan digital, protokol kriptografi, infrastruktur kunci publik, manajemen kunci, steganografi dan *watermarking*, kriptografi visual.

Materi 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. Kriptanalisis
6. Algoritma kriptografi modern
7. *Stream cipher* dan *block cipher*.
8. Beberapa algoritma *stream cipher* dan block *cipher* (RC4, A5, *DES*, *TDES*, *GOST*, *RC5*, *AES*)
9. Steganografi dan *watermarking*

10. Kriptografi kunci publik
11. Algoritma-algoritma kriptografi kunci-publik (RSA, ElGamal, Diffie-Hellman, Knapsack).
12. Fungsi *hash* dan *MAC*
13. Tanda-tangan digital (*digital signature*)
14. *Elliptic Curve Cryptography (ECC)*
15. Protokol kriptografi
16. *Public Key Infrastructure* (*PKI*)
17. Pembangkitan bilangan acak
18. Skema pembagian data rahasia
19. Kriptografi visual

Buku Acuan Kuliah

1. William Stalling, *Cryptography and Network Security, Principle and Practice 5rd Edition*, Pearson Education, Inc., 2015
2. Diktat kuliah IF5054 Kriptografi oleh Rinaldi Munir, Prodi IF – STEI 2006 (Sudah diterbitkan nenjadi buku isi kedua oleh Penerbit Informatika)
3. Menezes, Alfred J., Paul C van Oorschot, dan Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. (*e-book*)
4. Schneier, Bruce, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996
5. dll