IF4020 Kriptografi

Oleh: Rinaldi Munir
Program Studi Teknik Informatika ITB

Sekolah Teknik Elektro dan Informatika ITB

Tujuan Umum Kuliah IF4020

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

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

Luaran (*outcomes*)

Mahasiswa diharapkan mampu:

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

2. Membuat program aplikasi untuk tujuan keamanan pesan.

Prasyarat

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

Penilaian

1. Tubes: Tugas pemrograman aplikasi (2 kali) – perkelompok @ 3 orang

   a. Tubes 1: steganografi/watermarking + enkripsi

   b. Tubes 2: Aplikasi *asymmetric cryptography*
2. Tucil (3 atau 4 kali): *Vigenere cipher*, kriptanalisis, *asymmetric cryptography*
3. Makalah pengganti UTS (1 kali) – per orang
4. Makalah pengganti UAS (1 kali) – 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 UTS berupa hasil riset pengembangan sebuah *block cipher* "baru".
- 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. 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* dan *MAC*
13. Tanda-tangan digital (*digital signature*)
14. Protokol kriptografi
15. *Public Key Infrastructure* (*PKI*)
16. Manajemen kunci
17. Kriptografi dalam kehidupan sehari-hari
18. Kriptografi visual

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

Buku Acuan Kuliah

1. Diktat kuliah IF5054 Kriptografi oleh Rinaldi Munir, Prodi IF – STEI 2006 (Saudah diterbitkan nenjaid buku oleh Penerbit Informatika)
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. (*e-book*)
4. Stalling, W., *Cryptography and Network Security, Principle and Practice 3rd Edition*, Pearson Education, Inc., 2003
5. David Bishop, *Introduction to Cryptography with Java Applets* (*e-book*)
6. dll