Tugas Membuat Makalah Mata Kuliah IF5054 Kriptografi Departemen Teknik Informatika ITB

Rinaldi Munir[1] dan Anugerah Redja Kusuma[2]

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : rinaldi@informatika.org[1], *anugerah@students.if.itb.ac.id*[2]

Abstrak

Mahasiswa Teknik Informatika sebaiknya tidak hanya mampu membangun program aplikasi, tetapi juga diharapkan mampu menulis karya ilmiah. Dengan membuat tulisan, maka berbagai pemikiran, karya, maupun, penelitian di bidang Informatika dapat dikomunikasikan ke tengah masyarakat. Salah satu bidang ilmu di Informatika adalah Kriptografi. Mahasiswa yang mengambil mata kuliah IF5054 diwajibkan menulis sebuah makalah ilmiah dengan memilih salah satu topik di bidang kriptografi (lihat penjelasan tugas di bawah ini). Manfat menulis makalah ini, selain manfaat yang sudah disebutkan di atas, juga memicu mahasiswa untuk me-*review* kembali semua bahan kuliah yang sudah pernah diberikan, ternasuk referensi lain dari berbagai sumber (buku teks, Internet, jurnal, dsb), sebagai persiapan Ujian Akhir Semester. Makalah yang bagus mungkin saja akan diikutsertakan pada seminar-seminar tentang teknologi informasi, keamanan komputer, dan alin-lain.

***Kata kunci**: makalah, kriptografi, tugas*

1. Pendahuluan

Buatlah makalah ilmiah berupa *technical report* di bidang kriptografi dengan memilih salah satu dari topik berikut:

a. *Public-Key Cryptography*
b. *Symmetric Cryptography*
c. *Hash Function*
d. *Cryptography Protocols*
e. *Key Management*
f. *Cryptanalysis Technique*
g. *Digital Signature*
h. *Public Key Infrastructures*
i. *Crypto Policy*
j. *Cryptography Applications*

Pada dasarnya, topik-topik tentang bidang teknologi informasi dan topik lain yang terkait dengan bidang kriptografi tetap dipertimbangkan untuk dinilai.

Dokumen ini memperlihatkan contoh format penulisan makalah. Aturan penulisan naskah dapat dilihat pada bagian 4 dari dokumen ini.

2. Ruang lingkup

Makalah dapat berisi berbagai pemikiran, usulan, konsep, pengembangan, atau kajian dari berbagai literatur tentang topik kriptografi yang dipilih. Makalah harus asli, tidak boleh berupa jiplakan, saduran atau terjemahan dari makalah lain yang pernah ada. Tulisan berupa survey dari berbagai literartur lain diperbolehkan.

3. Pengumpulan Tugas

Makalah ini dibuat per kelompok, sesuai dengan kelompok tugas-tugas sebelumnya.

Makalah diserahkan paling lambat tanggal 6 Januari 2006 ke meja Dosen IF5054 dalam dua bentuk:

1. *Hardcopy*: *print out* dari makalah.
2. *Softcopy*: dalam format PDF, dikirim langsung ke alamat *e-mail*: **rinaldi@informatika.org**

Semua makalah akan di-*publish* di dalam **http://www.informatika.org/rinaldi**.

4. Aturan Penulisan Naskah

Naskah dapat ditulis dalam Bahasa Indonesia atau Bahasa Inggris dengan susunan penulisan yang terdiri dari: judul, nama penulis dan instansi, abstrak (maksimal 200 kata), kata kunci, isi makalah, apendiks (jika ada), dan daftar pustaka. Contoh tulisan beserta template-nya dengan menggunakan MS Words dapat juga dilihat di http://www.informatika.org/rinaldi.

Naskah harus ditulis rapi pada kertas berukuran 20x26 cm (satu sisi) dan setiap lembar tulisan harus diberi nomor halaman. Format penulisan satu kolom, model huruf *Times New Roman*, ukuran huruf 11 point, dan 1 spasi. Gunakan margin kanan 2 cm, margin kiri 2,5 cm, margin atas 2,5 cm, dan margin bawah 3,5 cm. Judul harus ditulis secara ringkas, tetapi cukup informatif untuk menggambarkan isi makalah. Jika memungkinkan hindari penggunaan singkatan. Huruf awal setiap kata pada judul berupa huruf kapital, kecuali kata sandang, kata depan, dan kata sambung.

Nama-nama penulis harus tertulis jelas. Jika seorang penulis mempunyai institusi yang berbeda dengan yang lainnya, setiap nama penulis harus diikuti dengan nomor urut superscript dan institusinya dengan nomor *superscript* yang sama. Nama institusi penulis beserta alamat pos institusi tidak boleh disingkat.

Abstrak berisi penjelasan isi makalah secara umum dan kesimpulan utama. Abstrak haruslah bisa berdiri sendiri, tidak mencantumkan nomor tabel, nomor gambar, atau referensi. Panjang abstrak tidak boleh lebih dari 200 kata untuk makalah biasa, dan 150 kata untuk komunikasi singkat.

Kata kunci harus dipilih untuk menggambarkan isi makalah. Pada umumnya, kata-kata ini dapat diambil dari judul dan abstrak.

Isi makalah harus diawali dengan bagian "1. Pendahuluan" dan diakhiri dengan bagian "Kesimpulan". Judul subbagian diberi nomor (contoh: 2.2, 2.3) dengan nomor pertama adalah nomor bagian. Demikian juga halnya dengan judul subbagian.

Rumus-rumus harus diketik rapi dan dapat dibaca serta diberi nomor dalam tanda kurung pada tepi kanan halaman. Satuan sebaiknya menggunakan Sistem Internasional (SI).

Referensi harus dinyatakan di dalam teks dengan nomor *superscript* yang diikuti oleh tanda kurung, seperti 1), 2,3), dan 4-8,11). Rujukan ke penulis cukup dengan hanya menuliskan nama belakangnya saja. Jika ada 2 atau lebih penulis, hanya penulis pertama saja yang disebutkan dan diikuti dengan *et al*.

Daftar pustaka diberi nomor urut berdasarkan abjad nama belakang penulis dan ditulis pada akhir makalah setelah *acknowledgement* dan apendiks (jika ada). Setiap nomor referensi berhubungan dengan satu referensi. Referensi yang berbeda dengan penulis yang sama harus ditulis dengan nomor yang berbeda. Contoh daftar pustaka dapat dilihat sebagai berikut:

[1] E. Barnad and D. Casasent, *Shift Invariance and the Neocognitron, in Neural Networks*, Band 3, S. 403-410, Pergamon Press, 1990.
[2] K. Fukushima, *Handwritten Aplhanumeric Character Recognition by the Neocognitron*, IEEE Trans. on Neural Networks, Vol. 2, No. 3, May 1991
[3] B. Gates, *Microsot Windows and The Universe*, http://www.microsoft.com, diakses tanggal 12 Maret 2002 pukul 12:03
[4] D. Rumelhart and J. McClelland (Ed.), *Parallel Distributed Processing, Vol. 1*, MIT Press, Cambridge, Massachusetts, 1986