Departemen Teknik Informatika
Fakultas Teknologi Industri
Institut Teknologi Bandung

UAS IF5054 Kriptografi (3 SKS)
Dosen: Ir. Rinaldi Munir, M.T.
Jumat, 23 Desember 2005
Waktu: 90 menit

---

1. Enkripsi kalimat berikut dengan metode *Playfair Cipher*:

   `AIR DIISI KE DALAM BOTOL`

   dengan kuncinya dibentuk dari sebuah kalimat berikut:

   `POHON JATI TUMBUH DI HUTAN` (20)

2. Pada algoritma *DES*, dekripsi menggunakan kunci K_{16}, K_{15}, …, K_2, K_1. Bagaimana cara memperoleh urutan K_{16} tanpa menghitung K_{15}, …, K_2, K_1 terlebih dahulu? (10)

3. Sebuah kotak-*S* di dalam algoritma *cipher* blok adalah 10×8 *S-box*.
   (a) Jika elemen-elemen kotak-*S* direpresentasikan sebagai matriks, berapa ukuran matriks yang dibutuhkan? (5)
   (b) Berapa nilai tertinggi dan terendah elemen di dalam matriks tersebut? (5)

5. Mengapa *MAC* (*Message Authentication Code*) yang dilekatkan (*embedded*) pada suatu pesan bukan merupakan tanda-tangan digital untuk pesan tersebut? (10)

6. Jelaskan dengan sebuah contoh kasus mengapa nilai *hash* dari pesan (dengan menggunakan *MD5*, *SHA*, dsb) kadang-kadang tidak dapat digunakan untuk otentikasi dokumen digital? (10)

8. Misalkan Alice dan Bob akan berkomunikasi dengan saling mengirim pesan. Sebelum bertukar pesan, Alice ingin mengotentikasi Bob terlebih dahulu, begitu pula Bob ingin mengotentikasi Alice agar mereka yakin tidak berkomunikasi dengan orang ketiga (*man in the middle*). Tuliskan sebuah protokol untuk mengotentikasi satu sama lain dengan menggunakan algoritma kriptografi kunci-publik. Parameter yang tersedia adalah pasangan kunci (kunci publik PK dan kunci privat SK) masing-masing Alice dan Bob. Gunakan simbol-simbol PK-A, PK-B, SK-A, SK-B, E, dan D. (A = Alice, B = Bob) di dalam protokol tersebut. (20)

8. Selain aplikasi kriptografi untuk *Pay TV*, ATM, komunikasi dengan *handphone*, *Smart Card*, PGP, dan kartu kredit, tuliskan 3 buah aplikasi kriptografi yang lain dalam kehidupan sehari-hari dan jelaskan penggunaan kriptografi dalam aplikasi tesrebut. (20)

9. Apa harapan/perkiraan anda untuk mata kuliah ini? (A/B/C/D/E) (2)

SELAMAT BERPIKIR DAN BEKERJA