



ITB | News

Promosi Doktor ITB: Yusuf Kurniawan

krisna

Rabu, 7 - Februari - 2007, 08:45:28

Bandung, itb.ac.id - Sekolah Pasca Sarjana ITB mempromosikan Yusuf Kurniawan memperoleh gelar Doktor di bidang teknik pada Sabtu (27/1) lalu. Yusuf mengajukan disertasi berjudul "Desain Algoritma Enkripsi 'block cipher' Baru yang Tahan Menghadapi Analisis Sandi Linear dan Diferensial." Dalam penelitian disertasinya, staf pengajar jurusan Teknik Informatika Universitas Pasundan Bandung ini mendesain algaoritma enkripsi yang memenuhi kriteria AES?NESSIE (Advanced Encryption Standard/New European Schemes for Signatures, Integrity and Encryption).

Penelitian Yusuf menghasilkan dua buah algoritma enkripsi, yaitu BC1 (block cipher 1) dan BC2 (block cipher 2). BC1 memiliki struktur SPN (Substitution Permutation Network). BC1 didesain agar algoritma enkripsi dan dekripsinya sama. Hasilnya, BC1 memiliki tingkat keamanan enkripsi dan dekripsi yang sama, difusi yang cepat, serta hemat sumber daya dalam implementasi. Kelebihan ini harus ditebus dengan lambatnya BC1 pada beberapa platform. BC2 menggunakan struktur Feistel dan memiliki enkripsi dan dekripsi yang sama juga. BC2 tahan terhadap analisis linear dan diferensial hingga tiga ronde. BC2 juga memiliki kecepatan yang baik pada komputer pribadi (PC) 32 bit.

Dalam disertasinya, Yusuf juga menyimpulkan bahwa penggunaan berbagai kotak substitusi yang berbeda pada sebuah algoritma tidak selalu meningkatkan kekuatan algoritma enkripsi, bila dibandingkan pemakaian satu jenis kotak substitusi. Kotak substitusi yang bergantung kunci juga tidak selalu memberikan kekuatan yang lebih baik bila dibandingkan dengan penggunaan kotak substitusi yang tetap. Melakukan sedikit modifikasi terhadap algoritma enkripsi dapat mengakibatkan perubahan keamanan yang sangat besar.
