

PROPOSAL PROYEK AKHIR

EC-5010 Keamanan Sistem Informasi

Evelyn 13201019

Judul: Identity-Based Encryption

Abstrak

Identity-Based Encryption merupakan teknik enkripsi dengan menggunakan kunci asimetris yang mempunyai keistimewaan, yaitu *public-key* yang digunakan dapat berupa sembarang string. Biasanya, enkripsi menggunakan *public-key* yang rumit dan sulit diingat. *Identity-based encryption* menggunakan kunci yang lebih "user-friendly". *Public-key* pada *Identity-Based Encryption* ini dapat berupa alamat email, nomor telepon, ataupun suatu kalimat. Kelebihan lain dari teknik enkripsi ini yaitu tidak diperlukannya penentuan pasangan kunci sebelum melakukan enkripsi. Dengan menggunakan *Identity-Based Encryption*, seseorang dapat mengirimkan email yang telah dienkripsi dengan *public-key* walaupun penerima belum mempunyai bahkan belum pernah mendengar *private-key* sekalipun. Pada saat penerima menerima email yang terenkripsi tersebut, penerima akan menghubungi *Private Key Generator*, yang akan melakukan autentikasi dan memberikan *private-key* untuk membaca email tersebut.

Referensi

Dan Boneh, Matthew Franklin . "Identity-Based Encryption from the Weil Pairing". <http://crypto.stanford.edu/~dabo/papers/ibe.pdf>

www.voltage.com/technology/ibe.htm