Penggunaan teknik idea untuk pengamanan file dengan teknik sha-i sebagai pembangkit key dan digital signature

Hotland Jeffri D.T., author

Abstrak

ABSTRAK
Pada skripsi ini dilakukan rancang bangun perangkat lunak enkripsi dengan menggunakan teknik International Data Encryption Algorithm (IDEA) untuk pengamanan file yang akan dikirimkan melalui jaringan komputer, dimana key untuk melakukan enkripsi dan mendapatkan digital signature dibangkitkan oleh SHA-1. Perangkat lunak di skripsi ini juga mempunyai fasilitas untuk mengirimkan e-mail dan file.

Perangkat lunak dibangun dengan menggunakan Borland Delphi 5,0 Enterprise Edition.

Dari uji coba dan analisa yang dilakukan didapat bahwa untuk mengetahui informasi terhadap file yang telah dienkripsi, dengan cara brute force attack dibutuhkan waktu 1,6 X 10 26 tahun. Dari sisi kecepatan, perangkat lunak ini mempunyai kemampuan untuk mengenkripsi file dan menambahkan digital signature hingga mencapai sekitar 400 byte/milidetik.
<hr>