ABSTRAKSI

Perkembangan internet yang semakin luas memungkinkan untuk penyebaran perangkat lunak semakin mudah, pengguna perangkat lunak dapat men-*download* langsung dari situs pembuat perangkat lunak di internet atau dapat memperolehnya lewat situs-situs pendistribusian perangkat lunak.

Dengan sistem pendistribusian yang semakin mudah tersebut akan menimbulkan permasalahan baru, yaitu bagaimana menjaga keaslian perangkat lunak dan bagaimana membatasi fungsionalitas perangkat lunak sehingga hanya bisa digunakan oleh pihak tertentu saja.

Tugas Akhir ini menganalisis dan mengimplementasikan penggunaan *digital signature* untuk mengatasi permasalahan diatas dengan menggunakan algoritma RSA untuk tanda tangan digital dan SHA-1 untuk fungsi hash satu arah. Perangkat lunak yang akan dilindungi (*.exe) dilengkapi dengan fungsi untuk memeriksa keaslian dan registrasi.

Sistem yang dibangun dalam Tugas Akhir ini terdiri dari tiga bagian utama yaitu perangkat lunak yang akan ditandatangani diimplementasikan dengan menggunakan Delphi 7, perangkat lunak penandatangan diimplementasikan dengan menggunakan Delphi 7 dan perangkat lunak untuk registrasi diimplementasikan dengan menggunakan PHP 5.0.4

Kata kunci : Perangkat Lunak, Tanda Tangan Digital, RSA, SHA-1, Delphi 7, PHP 5.0.4