

ABSTRAK

Distribusi perangkat lunak melalui *file installer (.exe)* memiliki potensi celah keamanan yang dapat dimanfaatkan untuk menyebarkan *malware* atau kode berbahaya. Untuk mengatasi risiko ini, dirancang sistem keamanan menggunakan algoritma kriptografi RC4 berbasis *Python*, yang berfungsi melakukan enkripsi dan dekripsi file installer secara cepat dan efisien. Pengembangan sistem mencakup analisis kebutuhan, perancangan antarmuka, implementasi RC4 dengan *Key-Scheduling Algorithm (KSA)* dan *Pseudo-Random Generation Algorithm (PRGA)*, serta pengujian menggunakan metode blackbox. Aplikasi dibangun dengan pustaka *tkinter*, *os*, *sys*, dan *time*, serta dilengkapi fitur pembuatan kunci otomatis, *progress bar*, *log proses*, dan deteksi kesalahan input. Proses enkripsi dan dekripsi dilakukan melalui operasi *XOR* antara data file dan keystream yang dihasilkan RC4. Hasil pengujian menunjukkan bahwa sistem mampu mengenkripsi dan mendekripsi *file installer (.exe)* pada berbagai ukuran dan jenis file tanpa mengalami kegagalan proses. Kinerja sistem tetap optimal meskipun digunakan panjang kunci hingga 32 karakter, dengan waktu pemrosesan yang relatif cepat dan selisih waktu yang tidak signifikan, serta mampu menolak file tidak valid atau kunci salah sekaligus menjaga integritas dan kerahasiaan *file installer (.exe)* tanpa mengorbankan performa, sehingga dapat menjadi referensi praktis bagi pengembang dalam menambahkan lapisan keamanan pada distribusi perangkat lunak berbasis *.exe*.

Kata kunci: Kriptografi, Algoritma RC4, Enkripsi, Dekripsi, *File Installer*, *Python*