Abstraksi

Yuhendrik.59413556
IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST-SHAMIR-ADLEMAN (RSA) PADA BERKAS DIGITAL MENGGUNAKAN PYTHON 2.7.
Skripsi, Fakultas Teknologi Industri, Jurusan Teknik Informatika, Universitas Gunadarma, 2017.
Kata Kunci : Kriptografi, Enkripsi, AES, RSA

(xiii + 56+ lampiran)

Pada tahun 2017, *malware* Wannacry menghebohkan masyarakat pengguna komputer. Malware ini menyerang semua berkas dokumen pada sistem operasi berbasis windows, mulai dari Windows XP sampai yang teranyar, yaitu Windows 10. Wannacry memadukan dua algoritma kripftografi, yaitu *Advanced Encryption Standard* (AES) dan *Rivest-Shamir-Adleman* (RSA). Algoritma AES digunakan untuk mengenkripsi berkas, sedangkan algoritma RSA digunakan untuk mengenkripsi kunci yang digunakan untuk mengenkripsi berkas yang membuat pengguna sulit mengembalikan berkasnya secara mandiri karena harus memecahkan kunci privat RSA untuk mengetahui kunci untuk dekripsi berkas. Hal tersebut yang menjadikan penulis mengimplementasikan algoritma AES dan RSA menjadi aplikasi yang bertujuan mengenkripsi berkas untuk tujuan keamanan. Aplikasi mengenkripsi berkas menggunakan algoritma AES dengan panjang kunci 256 bit lalu mengenkripsi kunci yang digunakan menggunakan algoritma RSA dengan panjang 2048 bit selanjutnya menyematkan kunci tersebut pada berkas yang telah dienkripsi. Waktu yang diperlukan program untuk mengenkripsi berbagai jenis berkas sekaligus dengan total ukuran berkas sebesar 1618269,91 KB (KiloBytes) adalah 45,33 detik, sedangkan waktu yang diperlukan untuk melakukan dekripsi adalah 58,38 detik.

Daftar Pustaka (1996-2017)