

ABSTRAK

Daffa AlRojak, 51417397

**APLIKASI ENKRIPSI DAN DEKRIPSI MENGGUNAKAN AES-128
(ADVANCED ENCRYPTION STANDARD) DAN GCM (GALOIS
COUNTER MODE)**

**Penulisan Ilmiah. Teknik Informatika, Fakultas Teknologi Industri,
Universitas Gunadarma, 2020**

**Kata kunci :*Desktop*, Java, Kriptografi, Advanced Encryption
Standard(AES), Galois Counter Mode (GCM)**

(xii + 69 + Lampiran)

Pada saat ini teknologi informasi dan komunikasi semakin berkembang dengan pesat, seiring berkembangnya teknologi kita jadi sering bertukar informasi sesama teman, keluarga maupun untuk urusan bisnis. Namun, tanpa disadari bahwa pertukaran data yang dilakukan belum tentu aman. Hal ini dapat mengakibatkan terjadinya interupsi, intersepsi, modifikasi, dan fabrikasi sehingga dibutuhkan suatu cara untuk mengamankan data, yaitu kriptografi. Aplikasi enkripsi dan dekripsi dibuat untuk mengamankan data pengguna dari orang yang tidak berhak. Aplikasi ini dibuat menggunakan Netbeans dengan bahasa pemrograman *Java* dan menggunakan Algoritma kriptografi *Advanced Encryption Standard* (AES) dan *Galois Counter Mode* (GCM). Berdasarkan hasil uji coba aplikasi untuk mengenkripsi atau mendekripsi berbagai jenis *file*, aplikasi ini dapat memproses enkripsi maupun dekripsi berbagai jenis format file serta dengan berbagai jenis ukuran file yang tidak melebihi dari batasan ukuran file input sebesar 2 *gigabyte*. File hasil enkripsi memiliki ukuran lebih besar dari ukuran sebelumnya Sedangkan ukuran file dekripsi lebih kecil dari ukuran sebelumnya.

Daftar pustaka (2003 – 2020)