Lana Fitrotun Nuha, 2020**, Pengamanan File MP3 Menggunakan Algoritma Advanced *Encryption Standard* (AES),** Skripsi ini dibawah bimbingan Drs. Edi Winarko, M.Cs. dan Auli Damayanti, M.Si., Departemen Matematika, Fakultas Sains dan Teknologi, Universitas Airlangga, Surabaya.

ABSTRAK

Perkembangan industri musik yang sangat pesat saat ini, telah membuat seniman musik gencar menghasilkan karya baru. Banyaknya karya yang tercipta, berupa lagu-lagu yang diproduksi dalam bentuk file MP3. Jika file berhasil digandakan dan didistribusikan oleh orang yang tidak bertanggung jawab maka tindakan itu termasuk kedalam pelanggaran hak cipta. Oleh karena itu perlu pengamanan pada file audio berformat MP3. Pada skripsi ini, dilakukan penelitian yang bertujuan untuk menerapkan Algoritma *Advanced Encryption Standard* (AES) untuk pengamanan file MP3. Pengamanan ini dilakukan dengan mengenkripsi file tersebut dengan suatu kunci khusus. *Bytes-bytes* dari file dienkripsi dengan 4 tahapan pokok yaitu, *AddRoundKey, SubBytes, ShiftRow, MixColoumns.* Sebelum proses enkripsi, akan dilakukan ekspansi kunci Algoritma *Advanced Encryption Standard* (AES). Sedangkan pada proses deskripsi ada 4 tahapan pokok yaitu, *AddRoundKey, InvSubBytes, InvShiftRow, InvMixColoumns.* Sebelum proses deskripsi juga akan dilakuan ekspansi kunci. Program yang digunakan untuk melakukan kriptografi menggunakan Algoritma *Advanced Encryption Standard* (AES) adalah Bahasa pemrograman Microsoft Visual Basic 6.0. Hasil implementasi pada file MP3 *filebesar.mp3* dengan kunci *'MATEMATIKA'*, didapatkan hasil enkripsi file dengan nilai bytes yang berbeda dengan aslinya atau tidak dapat diputar, sedangkan ada hasil deskripsi, file yang ter enkripsi dapat kembali menjadi file MP3 semula.

Kata Kunci : File MP3, Algoritma *Advanced Encryption Standard* (AES), Pengamanan File.

Lana Fitrotun Nuha, 2020**, Securing MP3 Files Using the Advanced Encryption Standard (AES) Algorithm,**This thesis is supervised by Drs. Edi Winarko, M.Cs. and Auli Damayanti, M.Si., Departement of Mathematics, Faculty of Science dan Tecnology, Airlangga University, Surabaya.

ABSTRACT

The very rapid development of the music industry at this time has made music artists intensively produce new works. There are many works that have been created, in the form of songs produced in MP3 files. If the file is successfully duplicated and distributed by irresponsible people, it is a copyright violation. Therefore it is necessary to secure the MP3 audio file format. In this thesis, a research is conducted which aims to apply the Advanced Encryption Standard (AES) Algorithm for securing MP3 files. This security is done by encrypting the file with a special key. The bytes of the file are encrypted with 4 main steps namely, AddRoundKey, SubBytes, ShiftRow, MixColoumns. Prior to the encryption process, the Advanced Encryption Standard (AES) algorithm key will be expanded. While in the description process there are 4 main stages, namely, AddRoundKey, InvSubBytes, InvShiftRow, InvMixColoumns. Prior to the description process, a key expansion will also be carried out. The program used to perform cryptography using the Advanced Encryption Standard (AES) algorithm is the Microsoft Visual Basic 6.0 programming language. The results of the implementation of the MP3 file filebesar.mp3 with the key "MATHEMATICS", obtained the results of the encryption of files with different bytes value from the original or cannot be played, In the description result, the encrypted file can return to the original MP3 file.

Keywords: MP3 files, Advanced Encryption Standard (AES) Algorithm, File Security.