

## **ABSTRAK**

Untuk menjamin keamanan dan keutuhan dari suatu data, dibutuhkan suatu proses penyandian. Dengan cara penyandian tersebut, data asli tidak akan terbaca oleh pihak yang tidak berkepentingan. Pertimbangan bahwa sebuah standard algoritma yang baru sangatlah diperlukan untuk tetap menjaga kerahasiaan suatu data. Dalam hal ini, kunci yang lebih panjang juga merupakan keharusan. *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi *encryption-decryption* yang dapat digunakan untuk mengamankan data. Kelebihan algoritma AES adalah pengamanan yang sangat kuat pada saat ini dibandingkan algoritma kriptografi sebelumnya. Algoritma AES dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit. Dengan panjang kunci 128 bit, Misal state =19, hasil SubBytes = d4, ShiftRows = d4, MixColumns = 04, AddRoundKey = a4 dan proses tersebut diulang sampai 10 kali hasil ciphertext = 39.

***Kata Kunci*** : *Kriptografi, Encryption-Decryption, Advanced Encryption Standard (AES) - 128, Rijndael*

### **ABSTRACT**

*To ensure the security and integrity of the data, we need a process of encoding. By way of encoding the original data will not be read by unauthorized parties. Considering that a new standard algorithm is required to maintain the confidentiality of the data. In this case, the longer keyword also a must. Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to secure the data. AES algorithm to encrypt and decrypt the data block along with a 128-bit key length of 128 bits, 192 bits or 256 bits. With a key length of 128 bits, Eg state = 19, the result SubBytes = d4, ShiftRows = d4, MixColumns = 04, AddRoundKey = a4 and the process is repeated up to 10 times the ciphertext = 39.*

**Keyword** : *Cryptographic, Encryption-Decryption, Advanced Encryption Standard(AES)-128.*