ABSTRAK

Pada saat ini banyak orang membutuhkan komputer untuk menyelesaikan berbagai pekerjaannya. Oleh Sebab itu Seiring dengan perkembangan zaman, kebutuhan manusia menningkat. Termasuk kebutuhan akan informasi. Oleh sebab itu, pengiriman dan penyimpanan data melalui media elektronik memerlukan suatu proses yang mampu menjamin keamanan dan keutuhan dari data tersebut. Untuk menjamin keamanan dan keutuhan dari suatu data, dibutuhkan suatu proses penyandian. Enkripsi dilakukan ketika data akan dikirim. Proses ini akan mengubah suatu data asal menjadi data rahasia yang tidak dapat dibaca. Sementara itu, proses dekripsi dilakukan oleh penerima data yang dikirim tersebut. Data rahasia yang diterima akan diubah kembali menjadi data asal. Dengan cara penyandian, data asli tidak akan terbaca oleh pihak yang tidak berkepentingan, melainkan hanya oleh penerima yang memiliki kunci dekripsi. Dengan menggunakan algoritma AES dalam kriptrografi kerahasiaan data tidak dapat di lihat atau dibaca oleh pihak yang tidak bekepentingan. Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut.

Kata kunci : AES, kriptrografi, enkripsi, dekripsi, kerahasiaan data.

ABSTRACT

At this time a lot of people need a computer to complete various jobs. By Therefore Along with the times, human needs menningkat. Including the need for information. Therefore, shipping and storage of data via electronic media requires a process that is able to ensure the security and integrity of the data. To ensure the security and integrity of the data, we need a process of encoding. Encryption is done when the data is sent. This process will transform the original data into a confidential data can not be read. Meanwhile, the decryption process performed by the receiver of the data sent. Confidential data received will be converted back to the original data. By way of encoding, the original data will not be read by unauthorized parties, but only to the recipient who has a decryption key. By using the AES algorithm in kriptrografi confidentiality of data can not be seen or read by parties who are not bekepentingan. Cryptography is the study of mathematics that have a relationship with information security aspects such as data integrity, authenticity, and authenticity of data entities. Cryptography uses a variety of techniques in an effort to secure the data. Data transmission and storage of data via electronic media requires a process that can guarantee the security and integrity of the data transmitted.

Key Words: AES, kriptrografi, encryption, decryption, data confidentiality