INTISARI

Keamanan informasi merupakan aspek penting di era pertumbuhan pengguna internet saat ini. Banyaknya kejahatan di dunia maya muncul sebagai akibat dari lemahnya keamanan informasi, hal ini mendorong penggunaan teknik enkripsi dan dekripsi dalam setiap komunikasi data. Oleh karena itu ilmu kriptografi memiliki peran yang sangat penting. Apalagi saat ini adalah era *Internet of Things*, yaitu era teknologi yang mengkoneksikan segala perangkat elektronik dengan internet. Maka diperlukan teknik enkripsi data yang ringan dan bisa diimplementasikan di semua perangkat.

Salah satu algoritme kriptografi simetris yang paling banyak digunakan adalah algoritme *Rijndael Cipher* yang dikenal sebagai AES (*Advanced Encryption Standard*). Algoritme ini diimplementasikan secara luas di berbagai perangkat elektronik, seperti di komputer maupun *embedded system*. Masalah implementasi di *embedded system* yang mempunyai frekuensi *clock* rendah adalah lamanya waktu eksekusi apabila data yang dienkripsi cukup besar. Maka diperlukan suatu *engine* AES yang ditanam di *embedded system* untuk mempercepat kecepatan eksekusi.

Pada penelitian ini dilakukan perancangan dan implementasi *engine* AES di FPGA Altera Cyclone IV EP4CE22F17C6N. Operasi enkripsi pada *engine* AES dikendalikan oleh prosesor Nios II sebagai *host-processor*. Hasil pengujian menunjukkan bahwa *engine* AES ini dapat melakukan komputasi 164,66 kali lebih cepat dibandingkan dengan hanya menggunakan prosesor Nios II saja sebagai *embedded system.*

Kata kunci : algoritme aes, fpga, kriptografi, prosesor nios, enkripsi

ABSTRACT

Information security is an important aspect in the era of the growth of Internet users today. The number of cybercrimes emerged as a result of weak information security, it encourages the use of encryption and decryption techniques in data communications. Therefore, cryptography has a very important role. Especially today is the era of the Internet of Things, the era of technology that connect all electronic devices with the Internet. It would require data encryption technique that is lightweight and can be implemented on all devices.

One of the symmetric cryptographic algorithm that most widely used is Rijndael cipher algorithm known as AES (Advanced Encryption Standard). This algorithm is implemented widely in various electronic devices, such as computers and embedded systems. Implementation problems in embedded systems that have a low clock frequency is the length of time of execution if the encrypted data is large enough. It would require an engine AES planted in embedded systems to accelerate the speed of execution.

In this research, design and implementation of AES engine in Altera Cyclone IV FPGA EP4CE22F17C6N. AES encryption operation on the engine are controlled by the Nios II processor as the host-processor. The test results showed that the AES engine can perform computational 164.66 times faster compared to just using the Nios II processor only as embedded systems.

Keywords : *aes algorithm, fpga, cryptography, nios processor, encrypt*