Perancangan dan implementasi algoritma enkripsi arcfour pada perangkat kriptografi berbasis FPGA = Design and implementation of arcfour encryption algorithm into FPGA based cryptographic device

Mohamad Syahral, author

Abstrak

Kriptografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi karena kriptografi mengkodekan suatu informasi sedemikian rupa sehingga informasi tersebut tidak dapat diketahui oleh pihakpihak yang tidak berhak mengetahuinya. Dalam tugas akhir ini dibahas tentang perancangan dan inplementasi suatu algoritma enkripsi dalam bentuk modul perangkat keras yang dapat dihubungkan langsung ke komputer dan mengenkripsi data-data yang akan dikirimkan ke komputer lainnya melalui sebuah modem yang terhubung ke PSTN. Algoritma yang digunakan adalah algoritma arcfour dan diimplementasikan ke FPGA Xilinx Spartan-IIE LC Development Board dengan menggunakan bahasa deskripsi perangkat keras VHDL. Pada tugas akhir ini algoritma enkripsi arcfour berhasil diimplementasikan ke FPGA Xilinx Spartan-IIE LC Development Board dan melakukan enkripsi datadata berupa teks yang dikirimkan serta mendekripsi data yang diterima. Sedangkan untuk data berupa file, proses enkripsi dan dekripsi masih belum berhasil dengan sempurna.

<hr>

Cryptography is one of the method that use to secure information for transmission, where cryptography encodes the information in certain way so that the information would not be known by anyone that have no access to the information. The focus of this study is designing and implementation one of encryption algorithm in a hardware device that can be connected directly to computer and decode the data that can be transmitted to another computer through a modem that connected to PSTN. Encryption algorithm that used is arcfour algorithm and implemented in Xilinx Spartan-IIE LC Development Board using VHDL Hardware Description Languange. In this study, the arcfour algorithm has been successfully implemented in FPGA Xilinx Spartan-IIE LC Development Board, encrypting text data that transmitted and decrypting received text data. But for data transfer of files, encryption and decryption process was not yet perfect successful.