ABSTRAK

Dewasa ini komputer telah mengalami perkembangan sangat pesat, baik dari segi perangkat keras maupun perangkat lunak. Pesatnya perkembangan dunia komputer akhir-akhir ini mempercepat berkembangnya teknologi baru yang memanfaatkan teknologi komputer tersebut sebagai media untuk mewujudkan otomasi pengoperasian peralatan listrik yang salah satunya adalah lampu rumah.

Pengoperasian lampu sangat membantu seseorang yang ingin selalu memonitor keadaan rumah , tempat, atau peralatan penelitian yang berada di ruang terpisah, sementara itu dia dapat melakukan kegiatan yang lain. Manajemen sistem penerangan adalah suatu usaha untuk mengelola dan mengatur suatu peralatan penerangan. Komputer adalah suatu sistem elektronik yang dapat memanipulasi dan mengolah masukan data yang cepat dan tepat. Dalam perancangan sistem sering kali digunakan komputer sebagai alat pengontrol terhadap sistem yang dibuat komunikasi antara komputer dengan alat yang dikontrol dijembatani oleh suatu rangkaian yang disebut antar muka atau *Interface*.

Kata kunci :lampu, *Interface*, komputer

ABSTRACT

In the Internet world there is no truly safe. There's always a gap in any applications that are made. To minimize attacks on the data transmission is usually applied cryptography. One fairly popular cryptographic algorithms is the RSA algorithm. RSA (Rivest-Shamir-Addleman) in the field of cryptography is a public key encryption algorithm.

In this final project will be discussed implementation of RSA cryptography algorithm on protocol SSL (Secure Socket Layer) in the Authentication Web site. SSL is a protocol used for secure web browsing. Many of the features provided in the SSL is a form of security in Internet browsing. This paper explains about the security provided by SSL to create secure web browsing at the time. Explanation that will include security features that are included in every component of an existing message when negotiating security services established between the client and server. Also described is also related to issues of possible attacks on the Internet that could be addressed by SSL, the attacker the opportunity to do an attack on a web through SSL, and the sub-existing protocol on SSL to maintain security when browsing the web.

Keywords: SSL, RSA, authentication, Cryptography