

ABSTRAK

Sistem keamanan pada data administrasi merupakan system yang dibangun untuk memberikan jaminan keamanan pada data administrasi di suatu perusahaan. Dengan adanya jaringan internet yang merupakan media komunikasi yang sangat efektif dan efisien, pengiriman data-data dapat dilakukan melalui jaringan ini. Namun hal ini memiliki resiko apabila data yang dikirimkan tersebut diakses oleh orang yang tidak berhak.

Untuk mencegah supaya informasi penting yang terdapat di client maupun yang dikirimkan melalui jaringan tidak diakses oleh orang yang tidak berhak (unauthorized persons), maka keamanan dan kerahasiaan data pada sistem ini merupakan aspek yang sangat penting terkait dengan pentingnya informasi tersebut dapat diterima oleh orang yang berhak.

Tugas akhir ini menggambarkan rancangan suatu sistem keamanan pada data administrasi perusahaan yang bertitik berat pada teknologi keamanan data lewat jaringan internet. Dalam hal ini teknik yang digunakan adalah kriptografi asimetrik menggunakan algoritma RSA yang terdiri dari algoritma pembangkitan kunci (key generation algoritm), algoritma enkripsi (encryption algoritm) dan algoritma dekripsi (decryption algoritm) serta algoritma Digital Signature.

Kata kunci : *Kriptografi asimetrik, algoritma RSA, algoritma pembangkit kunci, algoritma enkripsi, algoritma dekripsi, algoritma Digital Signature.*