ABSTRAKSI

Pembayaran elektronik sekarang sudah menjadi seperti gaya hidup dan kebutuhan bagi sebagian masyarakat, terutama masyarakat perkotaan yang menginginkan pola bertransaksi yang praktis dan cepat. Dengan berkembangnya teknologi di bidang jaringan internet, suatu proses pembelian dan pembayaran melalui internet sudah bukan hal yang asing lagi.

Masalah terpenting dalam jaringan komputer adalah masalah keamanan data yang dikirimkan. Pelaku kejahatan memanfaatkan celah keamanan yang ada untuk dimasuki dan melakukan manipulasi data. Pihak penjahat itu bisa saja berniat untuk sekedar mencari tahu saja, atau juga bisa mencuri berbagai macam hal seperti uang, data rahasia, dll.

Secure Socket Layer (SSL) merupakan suatu protokol yang telah dikembangkan dan dipergunakan untuk mengatasi permasalahan keamanan yang mengancam proses transaksi menggunakan jaringan internet. SSL didukung pula dengan penyediaan fasilitas enkripsi yang cukup memadai dan dilengkapi dengan sebuah proses *handshaking* dan pengiriman data yang cukup aman untuk mengatasi berbagai kejahatan jaringan internet yang ada.

Dengan adanya kejahatan *cyber* yang berkembang di jaringan internet, maka tugas akhir ini akan menganalisa sistem keamanan yang mampu disediakan oleh sistem tersebut, meliputi simulasi serangan dan juga analisa yang disusun berdasarkan referensi yang sudah ada.

Sistem keamanan yang diimplementasikan ternyata bisa memenuhi parameter-parameter keamanan internet yaitu *confidentiality*, *authority*, *authentication*, *integrity*, dan *non-repudiation.* Sistem dengan protokol SSL ini juga sanggup mengantisipasi simulasi serangan *man-in-the-middle* dan juga masih aman terhadap serangan *brute-force* dalam waktu beberapa tahun ke depan. Kelemahan yang bisa diketahui dari sistem ini adalah masih rentan terhadap serangan *denial of service*, yang bisa membuat performa jaringan *server* menjadi sangat sibuk, dan bisa membuat kegagalan dalam transaksi rata-rata sebesar 2,31 % dari 15000 simulasi transaksi.

Kata kunci : enkripsi, pembayaran elektronik, keamanan jaringan, SSL