ABSTRAKSI

Perkembangan internet yang sangat pesat di dunia menyebabkan banyak perusahaan barang dan jasa merubah gaya bisnisnya melalui internet. Salah satu yang marak dikembangkan adalah sistem perdagangan melalui internet.

Dengan semakin berkembangnya perdagangan di Internet, banyak pula protokol protokol yang dipergunakan untuk perdagangan di Internet. Protokol ini digunakan untuk menghindari adanya penyusupan atau penyalahgunaan fasilitas perdagangan di internet yang menyebabkan kerugian oleh salah satu pihak. Salah satu protokol yang dianggap paling aman adalah *Secure Electronic Transaction* (SET) yang dikeluarkan oleh Visa dan Mastercard. Di Indonesia belum ada yang mengimplementasikan SET untuk perdagangan di Internet. Dalam penelitian ini dicoba untuk membuat emulasi protokol SET dan kemudian menganalisanya.

SET (*Secure Electronic Transaction*) merupakan protokol yang dikeluarkan oleh Visa dan Mastercard yang ditujukan untuk melindungi proses perdagangan melalui internet terhadap kejahatan – kejahatan yang mungkin dilakukan melalui internet. Protokol ini didukung oleh penyediaan fasilitas enkripsi yang cukup memadai. Fasilitas utama yang dibanggakan oleh protokol ini adalah adanya *dual signature* yang membuat pemisahan antara data order pembelian dan informasi pembayaran. Pada protokol ini, *merchant* hanya dapat mengetahui informasi order barang yang diajukan oleh *client* tanpa dapat mengetahui informasi pembayaran yang akan digunakan oleh *client*. Oleh karena itu, dalam protokol ini dibutuhkan pihak ketiga yaitu *payment gateway* yang akan mengurus proses pembayaran kedua belah pihak.

Tujuan dari tugas akhir ini adalah untuk merancang emulasi objek-objek yang dipakai dalam protokol SET dan kemudian menganalisa protokol ini pada aplikasi *electronic payment*.

Sistem yang dirancang ternyata dapat memenuhi parameter – parameter keamanan jaringan komputer yaitu *confidentiality, integrity, authentication, authority,* dan *non-repudiation.* Sistem belum mampu mengatasi pemutusan pengiriman data yang dilakukan pada serangan *man-in-the-middle* namun data yang tertangkap masih terlindungi karena masih dalam bentuk *ciphertext*. Sistem masih aman terhadap serangan *brute-force* sampai beberapa tahun ke depan.

Kata kunci : *electronic payment*, SET, *dual signature*