ABSTRAK

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 cukup aman untuk transaksi adalah *i-Keyed Protocol* (iKP). Dalam penelitian ini dicoba untuk membuat emulasi protokol iKP dan kemudian menganalisanya.

iKP (*i-Keyed Protocol*) merupakan protokol yang dikeluarkan oleh IBM 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. Dengan digunakannya dua buah public key, maka pihak buyer hanya dapat melihat transaksi yang terjadi antara *buyer-seller*.

Tujuan dari tugas akhir ini adalah untuk merancang emulasi objek-objek yang dipakai dalam protokol iKP 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 : pembayaran elektronik, enkripsi, RSA, iKP