ABSTRAK

Keamanan data merupakan sesuatu yang penting di dalam perkembangan teknologi terutama di bidang teknologi informasi. Data yang tersimpan harus dapat terjamin keamanannya sehinga tidak menimbulkan penyalahgunaan data. Salah satunya dalam pembelian tiket, semakin berkembangnya zaman kita dapat membeli tiket secara online. Namum rentan akan pembobolan data terutama pada bagian data pembeli. Ada pun solusi untuk mengatasi pembobolan data tersebut sistem seharusnya memakai kriptografi. Dengan kriptografi pembeli dapat mengirimkan data secara aman, karena menggunakan proses enkripsi.

Dalam penelitian tugas akhir ini akan merancang suatu sistem yang dapat menjaga keamanan pada sistem pembelian tiket online dengan menggunakan Algoritma Kurva Eliptik dan MD5 dimana enkripsi dilakukan dengan public key dan verifikasi dengan fungsi MD5. Dari percobaan serangan dengan *Man in middle* tidak bisa terjadi karena tidak mempunyai publik key yang berbeda dengan server aslinya. Penggunaan algoritma ECC dan MD5 sangat di anjurkan untuk penggunaan suatu aplikasi terutama yang membutuhkan jaringan yang rentan akan serangan dan pencurian dari pihak lain.

Kata Kunci: *Elliptic curve cryptography, Security MD5, Security system, Database security.*