ABSTRAK

Seiringnya perkembangan zaman, bidang teknologi semakin maju terutama di bidang Komputer. Sudah banyak pengembangan teknologi baru yang bahkan hampir tidak pernah terpikirkan sama sekali. Salah satunya dalam pembelian tiket saat ini pun sudah bisa membelinya secara online. Tetapi siapa yang menduga jika ternyata pembelian tiket secara online rentan pembobolan data terutama di bagian data pemilik User. Adapun solusi untuk mengatasi pembobolan data tersebut sistem seharusnya memakai Kriptografi. Dengan kriptografi pembeli dapat mengirimkan data pembelian secara aman.

Pada penelitian tugas akhir ini akan dirancang suatu sistem yang dapat menjaga keamanan pada sistem pembelian tiket online dengan menggunakan Algoritma Kurva Eliptik dan dengan *Fungsi Security Hash Algorithm* 256 yang dimana dengan cara pengenkripsian dengan public key dan verifikasi dengan fungsi hash.

Pada pengujian dan analisis ini memiliki Respond Time dengan rata-rata 203.6 ms dengan ukuran kunci sebesar 512 bits dan Signature Key size dari SHA-256 sebesar 256 bytes. Jenis serangan yang sudah dianalisa ialah Spoofing, Sniffing, dan Man in Middle Attack. Spoofing dapat diatasi dengan penggunaan fungsi enkripsi dan dekripsi pada suatu proses.

Kata kunci: *Elliptic Curve Cryptosystem, Security Hash Algorithm 256, security system, encryption,decryption. Signature key.*

ABSTRACT

Nowadays, Technology is very common especially in Computer Science. there manny new program Developement whose unbelieveable. One of them is Buying the tickets with online system today. But, who knows if ticketing online transaction not very safe because there's more attacker for get our ticket without permission. And the solution is, we can use Crypthograph as Secure Key for any transaction, include for online transaction too.

On final task now, will design a system for keeping secure from online transaction with ECC Algorithm which become for encryption and decryption and Hash Function SHA-256 As Digital Signature for verification.

Experiment and Analysis of final task have a some conclusion, Respon Time have average about 203.6 ms with key size 512 bits and Signature Key from SHA-256 about 256 bits. We analysing there’s many attack will crush the application, they are Spoofing, Sniffing, and Man in Middle Attack. The Attacks will stop with using encryption, decryption and signature on the process.

Keyword: *Elliptic Curve Cryptosystem, Security Hash Algorithm 256, security system, encryption,decryption. Signature key.*