

ABSTRACT

Nowadays, Technology is very common especially in Computer Science. there many new program Developement whose unbelievable. 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 Cryptograph 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.*