ABSTRACT

Identity Based Encryption facilitate is an easy way to cryptography by using arbitrary string as a public key. In the common public key cryptography, the encryption using a complicated public key and hard to remember. In the Identity Based Encryption, the public key can be email address, phone number or an arbitrary word. Using this method, the encryption can be done before pairing the public key and the private key. When the recipient recieve an encrypted message, the recipient have to contact the Private Key Generator to obtain his/ her private key and decrypt the encryped message using his/ her private key.

The Identity Based Encryption in this project is based on Boneh and Franklin method. An overview of the Identity Based Encryption Boneh Franklin implementation is given in this project and the duration measurement of this implementation using operating system high precision timer.

Key Word: Identity-Based Encryption, Public Key, Private Key, Private Key Generator.