ABSTRACT

In modern communication systems, the cryptographic algorithms play a central role in ensuring information security. This thesis has employed certain widely used cryptographic algorithms.

A hybrid algorithm is designed, combining the best of both symmetric (AES) and asymmetric (ECC over GF(p)) methodologies. The MD5 hash algorithm is adopted to ensure integrity of the data. Since ECC were shown to be insecure, research into HECC helps to provide a feasible alternative. This thesis presents techniques allowing secured and faster implementations than the existing ones. Such techniques are necessary in order to use high security cryptographic algorithms in real world applications. The focus is on Advanced Encryption Standard (AES), the most commonly used secret key cryptographic algorithm, and Hyper Elliptic Curve Cryptography (HECC), public key cryptographic algorithms which have gained popularity in the recent years and are replacing traditional public key cryptosystems, such as RSA and ECC.

This thesis has employed a hyper elliptic curve cryptosystem for genus2 and genus 3. Their performances are compared in terms of divisor generation, key generation, and encryption and decryption process. The digital envelope is designed and implemented using hybrid algorithm which combines the best of both symmetric (AES) and
asymmetric (HECC over GF(p) Genus 2) methodologies. The result of this thesis can be almost directly applied in practice.

The Secured Electronic Medical Record (SEMR) system provides a secure way to access the EMR. This system provides an insight into developing a distributed system which is secure, robust and user friendly. This thesis suggests a design and implementation of a digital envelope that combines the hashing algorithm of MD5, the symmetric key algorithm of AES and the asymmetric key algorithm of Hyper Elliptic Curve Cryptography (HECC).