INTISARI

SKEMA TANDA TANGAN DIGITAL KURVA ELIPTIK

Oleh

CHRISTOPHER ALDORA TJITRABUDI

12/330958/PA/14416

Kurva eliptik adalah kurva yang didefinisikan oleh persamaan $E : y^2 = x^3 + ax + b$ dengan suatu konstanta real a dan b. Himpunan semua titik (x, y) dalam kurva tersebut membentuk grup abelian terhadap operasi penjumlahan titik yang didefinisikan dengan aturan *chord-and-tangent*. Grup tersebut dinamakan grup kurva eliptik. Lebih lanjut, dapat didefinisikan kurva eliptik atas lapangan berhingga. Grup kurva eliptik atas lapangan berhingga digunakan dalam kriptografi karena masalah logaritma diskrit pada grup tersebut dipercaya sangat sulit untuk dipecahkan. Masalah logaritma diskrit adalah contoh fungsi satu arah, yang merupakan dasar dari kriptografi kunci publik.

National Institute of Standards and Technology (NIST) mempublikasikan skema tanda tangan digital yang bernama *Elliptic Curve Digital Signature Algorithm* (ECDSA). ECDSA adalah skema tanda tangan digital yang memanfaatkan kurva eliptik dan kriptografi kunci publik. Skema tanda tangan digital adalah metode untuk menandatangani pesan digital, yaitu pesan yang disimpan secara elektronik. Berbeda dengan tanda tangan konvensional yang berupa goresan tinta, tanda tangan digital berupa bilangan bulat yang diperoleh dari suatu pesan dengan kunci milik penandatangan. Pada skripsi ini dibahas mengenai kurva eliptik dan aplikasinya dalam skema tanda tangan digital.

ABSTRACT

ELLIPTIC CURVE DIGITAL SIGNATURE SCHEME

By

CHRISTOPHER ALDORA TJITRABUDI

12/330958/PA/14416

Elliptic curve is a curve defined by the equation $E : y^2 = x^3 + ax + b$ with real constants a and b. The set of all points (x, y) in the curve forms an abelian group with respect to the addition operation defined by the chord-and-tangent rule. The group is called the group of the elliptic curve. Furthermore, elliptic curve over finite field is defined. The group of elliptic curve over finite field is used in cryptograpy because the discrete logarithm problem on those group is believed hard to solve. Discrete logarithm problem is an example of one way function, which is the foundation of public key cryptography.

National Institute of Standards and Technology (NIST) published a digital signature scheme named Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA is a digital signature scheme that uses elliptic curve and public key cryptography. Digital signature shceme is a method to sign a digital messages, i.e. messages that were stored electronically. Unlike conventional signature which is in the form of ink strokes, digital signature is an integer obtained from a message with a signer's key. In this thesis we examined the elliptic curves and it's application in digital signature schemes.