Kriptografi kurva eliptik dan aplikasinya pada smart card

Wiratna Sari Wiguna, author

Abstrak

Kriptografi kurva eliptik dapat digunakan untuk pertukaran kunci, enkripsi dan dekripsi, dan tanda tangan digital. Elliptic Curve Digital Signature Algorithm (ECDSA) adalah algoritma penandatanganan digital dan verifikasi yang menggunakan aritmetika kurva eliptik. Smart card adalah kartu yang dilengkapi dengan chip memori dan kemampuan komputasi. Smart card banyak digunakan di berbagai bidang untuk identifikasi dan penyimpanan data. Kriptografi kurva eliptik dianggap sesuai untuk diimplementasikan pada smart card yang memiliki memori dan kemampuan komputasi terbatas. Pemrograman smart card dapat dilakukan dengan teknologi Java Card.

Dalam tugas akhir ini penulis menjelaskan kriptografi kurva eliptik dan mengimplementasikan ECDSA atas Galois Field) 2 (163 GF pada smart card dengan menggunakan Java Card. Hasil pengujian menunjukkan bahwa ECDSA dapat digunakan pada smart card untuk penandatanganan digital dan verifikasi. Penggunaan memori untuk verifikasi dan penandatanganan digital hampir setara namun verifikasi memerlukan waktu komputasi dua kali lebih lama daripada penandatanganan digital karena verifikasi membutuhkan dua buah operasi perkalian skalar pada kurva eliptik sedangkan penandatanganan digital hanya memerlukan sebuah operasi perkalian skalar.