Cr3 - Crittografia 3

Prerequisiti

CR1, GE3

Programma

Teoria delle Curve Ellittiche. La struttura di gruppo sui punti razionali, L'invariante j, curve ellittiche in caratteristica 2, Endomorfismi, curve singolari, curve ellittiche modulo n. Punti di torsione, Polinomi di divisione. L'accoppiamento di Weil. Curve ellittiche su campi finiti, L'endomorfismo di Frobenius. Il problema di determinare l'ordine del gruppo. L'algoritmo Baby Step, Giant Step di Shanks. L'algoritmo di Schoof. Crittosistemi sulle Curve Ellittiche. Il problema del Logaritmo Discreto. Attacco MOV. Attacco sulle curve anomale. Crittosistemi sulle curve ellittiche basati sul problema della fattorizzazione. Un crittosistema basato sull'accoppiamento di Weil. Fattorizzzione di numeri interi utilizzando le curve ellittiche.

Materiale Didattico