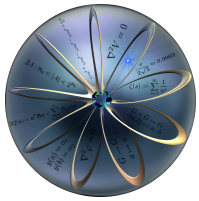

planetmath.org

Math for the people, by the people.

elliptic curve discrete logarithm problem

Canonical name	EllipticCurveDiscreteLogarithmProblem
Date of creation	2013-03-22 13:46:01
Last modified on	2013-03-22 13:46:01
Owner	mathcam (2727)
Last modified by	mathcam (2727)
Numerical id	7
Author	mathcam (2727)
Entry type	Definition
Classification	msc 94A60
Synonym	elliptic curve discrete log problem
Related topic	DiffieHellmanKeyExchange
Related topic	ArithmeticOfEllipticCurves

The elliptic curve discrete logarithm problem is the cornerstone of much of present-day elliptic curve cryptography. It relies on the natural group law on a non-singular elliptic curve which allows one to add points on the curve together. Given an elliptic curve E over a finite field F, a point on that curve, P, and another point you know to be an integer multiple of that point, Q, the "problem" is to find the integer n such that $nP = Q$.

The problem is computationally difficult unless the curve has a "bad" number of points over the given field, where the term "bad" encompasses various collections of numbers of points which make the elliptic curve discrete logarithm problem breakable. For example, if the number of points on E over F is the same as the number of elements of F, then the curve is vulnerable to attack. It is because of these issues that point-counting on elliptic curves is such a hot topic in elliptic curve cryptography.

For an introduction to point-counting, reference Schoof's algorithm.