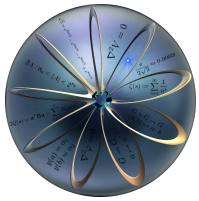

planetmath.org

Math for the people, by the people.

Diffie-Hellman key exchange

Canonical name	DiffieHellmanKeyExchange
Date of creation	2013-03-22 13:45:58
Last modified on	2013-03-22 13:45:58
Owner	mathcam (2727)
Last modified by	mathcam (2727)
Numerical id	6
Author	mathcam (2727)
Entry type	Algorithm
Classification	msc 94A60
Related topic	EllipticCurveDiscreteLogarithmProblem
Related topic	ArithmeticOfEllipticCurves

The Diffie-Hellman key exchange is a cryptographic protocol for symmetric key exchange. There are various implementations of this protocol. The following interchange between Alice and Bob demonstrates the Elliptic Curve Diffie-Hellman key exchange.

- 1) Alice and Bob publicly agree on an elliptic curve E over a large finite field F and a point P on that curve.
- 2) Alice and Bob each privately choose large random integers, denoted a and b.
- 3) Using elliptic curve point-addition, Alice computes aP on E and sends it to Bob. Bob computes bP on E and sends it to Alice.
- 4) Both Alice and Bob can now compute the point abP, Alice by multipliying the received value of bP by her secret number a, and Bob vice-versa.
- 5) Alice and Bob agree that the x coordinate of this point will be their shared secret value.

An evil interloper Eve observing the communications will be able to intercept only the objects E, P, aP, and bP. She can succeed in determining the final secret value by gaining knowledge of either of the values a or b. Thus, the security of the exchange depends on the hardness of that problem, known as the elliptic curve discrete logarithm problem. For large a and b, it is a computationally "difficult" problem.

As a side note, some care has to be taken to choose an appropriate curve E. Singular curves and ones with "bad" numbers of points on it (over the given field) have simplified solutions to the discrete log problem.