Schnorr group

From Wikipedia, the free encyclopedia

A **Schnorr group**, proposed by Claus P. Schnorr, is a large prime-order subgroup of $\mathbb{Z}_p^*$, the multiplicative group of integers modulo p for some prime p. To generate such a group, generate p,q,r such that

$$p = qr + 1$$

with p,q prime. Then choose random h in the range $1 < h < p$ until you find one such that

$$h^r \not\equiv 1 \pmod{p}.$$

This value

$$g = h^r \mod p$$

is a generator of a subgroup of $\mathbb{Z}_p^*$ of order q.

Schnorr groups are useful in discrete log based cryptosystems including Schnorr signatures and DSA. In such applications, typically p is chosen to be large enough to resist index-calculus and related methods of solving the discrete-log problem (perhaps 1024-2048 bits), while q is large enough to resist the birthday attack on discrete log problems, which works in any group (perhaps 160-512 bits). Because the Schnorr group is of prime order, it has no non-trivial subgroups, thwarting confinement attacks due to small subgroups. Implementations of protocols that use Schnorr groups must verify where appropriate that integers supplied by other parties are in fact members of the Schnorr group; x is a member of the group if $0 < x < p$ and $x^q \equiv 1 \pmod{p}$. Any member of the group except the element 1 is also a generator of the group.

See also: Topics in cryptography

Retrieved from "http://en.wikipedia.org/wiki/Schnorr_group"
Categories: Cryptography stubs | Asymmetric-key cryptosystems | Number theory | Group theory