The CLAUS BAT

Daniel J. Bernstein *

djb@cr.yp.to

CLAUS (Collaboratively Agreed User Secret) is a sample secret-sharing BAT (Benchmarkable Asymmetric Tool). CLAUS uses the popular OpenSSL library, `http://www.openssl.org`, to generate keys and to compute shared secrets. Other BAT implementors may find CLAUS useful as an illustration of the ease of writing BATs.

CLAUS uses a very simple form of the Diffie-Hellman secret-sharing system. Each secret key a is used to generate a public key $2^a \bmod p$ and, given another public key $2^b \bmod p$, the shared secret $2^{ab} \bmod p$. Here p is a fixed 1024-bit prime copied from OpenSSL's `crypto/dh/p1024.c`. CLAUS isn't parametrized; it supports only this 1024-bit prime.

Beware that the speed and security of CLAUS can be improved in many ways. CLAUS is *not* meant as a state-of-the-art implementation of public-key cryptography.

* Date of this document: 2006.06.04.