The DONALD BAT

Daniel J. Bernstein *

djb@cr.yp.to

DONALD is a sample signing BAT (Benchmarkable Asymmetric Tool) that implements the DSA public-key signature system. Other BAT implementors may find DONALD useful as an illustration of the ease of writing BATs.

DONALD uses the popular OpenSSL library, `http://www.openssl.org`, to sign and verify messages. DONALD's `signatureofshorthash` function feeds the input through SHA-1 and then uses OpenSSL's `DSA_do_sign` to sign the result. DONALD's `verification` function feeds the input through SHA-1 and then uses OpenSSL's `DSA_do_verify` to verify the result.

BATMAN automatically builds `signedmessage` and `messagesigned` from `signatureofshorthash` and `verification`, using DONALD to sign a SHA-256 hash of a long message. Notice the double hashing here, with messages being fed through SHA-256 and then SHA-1; a pure DSA implementation would instead feed messages of any length through SHA-1.

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

---

* Date of this document: 2007.02.13.