The Blowfish Encryption Algorithm

www.schneier.com/academic/blowfish/

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all uses.

The original Blowfish paper was presented at the First Fast Software Encryption workshop in Cambridge, UK (proceedings published by Springer-Verlag, *Lecture Notes in Computer Science #809*, 1994) and the April 1994 issue of *Dr. Dobb's Journal*. "Blowfish--One Year Later" appeared in the September 1995 issue of *Dr. Dobb's Journal*.

Many cryptographers have examined Blowfish, although there are few published results. Serge Vaudenay examined weak keys in Blowfish; there is a class of keys that can be detected--although not broken--in Blowfish variants of 14 rounds or less. Vincent Rijmen's Ph.D. thesis includes a second-order differential attack on 4-round Blowfish that cannot be extended to more rounds.

Everyone is welcome to download Blowfish and use it in their application. There are no rules about use, although I would appreciate being notified of any commercial applications using the product so that I can list them on this website.

David Honig has written a paper about implementing Blowfish in hardware.

For Blowfish implementors, here are the hexadecimal digits of pi, arranged as four s_boxes and one p_array, as per the Blowfish default. Those who want to experiment with longer-round variants of Blowfish can find 65535 hex digits of pi here.

Here are new test vectors so that you can test your own implementation of Blowfish. Here are the test vectors rewritten in a format more friendly to C programmers.

NOTE: There is a bug in some source code implementations of Blowfish. Here are the details. The reference implementation does not have this bug.

up to Academic

Photo of Bruce Schneier by Per Ervland.