WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Deutsch
Español
Français
Português
Русский
Svenska
Українська
Edit links

Yarrow algorithm

From Wikipedia, the free encyclopedia

This article has multiple issues. Please help **improve it** or discuss these issues on the **talk page**. [hide]

- This article includes a list of references, but **its sources remain unclear** because it has **insufficient inline citations**. *(September 2013)*
- This article **relies too much on references to primary sources**. *(September 2013)*

The **Yarrow algorithm** is a cryptographically secure pseudorandom number generator. The name is taken from the yarrow plant, the stalks of which are dried and used as a randomising agent in I Ching divination.

It was designed by Bruce Schneier, John Kelsey, and Niels Ferguson of Counterpane Labs (Kelsey et al., 1999). The Yarrow algorithm is explicitly unpatented, royalty-free and open source; no license is required to use it. An improved design from Ferguson and Schneier, Fortuna, is described in their book, *Practical Cryptography*.

Yarrow is incorporated in iOS[1] and Mac OS X for their /dev/random devices. FreeBSD also used Yarrow for /dev/random, but phased it out in favor of Fortuna.[2]

External links [edit]

- Yarrow algorithm page
- *Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator*, J. Kelsey, B. Schneier, and N. Ferguson

References [edit]

1. ^ http://www.apple.com/ipad/business/docs/iOS_Security_Oct12.pdf
2. ^ https://svnweb.freebsd.org/base?view=revision&revision=284959

This cryptography-related article is a stub. You can help Wikipedia by expanding it.

Categories: Pseudorandom number generators | Cryptographically secure pseudorandom number generators | Cryptography stubs

This page was last modified on 21 August 2015, at 23:12.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.