Quelle: www.cryptool.de

E-Learningprogramm Cryptool

Menü: Einzelverfahren – Tools – Zufallsdaten erzeugen

- **Linearer Kongruenzgenerator → Generatorspezifische Parameter wählen**
- **F1 (für Hilfe)**

Cryptool ist auch auf den Pool-Rechnern im 11. Stock installiert!

Die folgende Tabelle liefert einen Überblick über die Parameter einiger ausgewählter LCG.

a	b	N	Referenz
19496	0	2^15-19	Chiang, Hwang, Kao
214013	13523655	2^24	BASIC
16598013	12820163	2^24	Qbasic
62605	113218009	2^29	Berkeley UNIX Pascal
452807053	0	2^31	URN12
16807	0	2^31-1	_Minimal Standard_ von Lewis, et al.
41358	0	2^31-1	L'Ecuyer
48271	0	2^31-1	Park & Miller
51081	0	2^31-1	Härtel
69621	0	2^31-1	Park & Miller
950706376	0	2^31-1	FISH von Fishman & Moore
63060016	0	2^31-1	SIMSCRIPT II
397204094	0	2^31-1	SAS & IMSL-Library von Hoaglin
65539	0	2^31	IBM's RANDU
1103515245	12345	2^31	UNIX rand [Rip90], ANSI C
129	907633385	2^32	Turbo Pascal
69069	1	2^32	VAX VMS-Generator von Marsaglia
663608941	0	2^32	C-RAND von Ahrens
1099087573	0	2^32	Fishman
3141592653	1	2^32	DERIVE
2147001325	715136305	2^32	BCPL von Richards, Whitby-Strevens
5^15	7261067085	2^35	Boeing Computer Services BCSLIB
71971110957370	0	2^47-115	L'Ecuyer
25214903917	11	2^48	SUN-UNIX drand48
44485709377909	0	2^48	Cray X-MP Library
68909602460261	0	2^48	Fishman
13^13	0	2^59	NAG Fortran Library
2307085864	0	2^63-25	L'Ecuyer
427419669081	0	10^12-11	MAPLE