Cheatography

Symmetric Encryption Algorithms Cheat Sheet

by rubberdragonfarts (rubberdragonfarts) via cheatography.com/19400/cs/2423/

Symmetric Block Style Algorithms

Name	Rounds	Keysize	Blocksize
Lucifer	16	128	128
DES	16	64 (56)	64
3DES	48	128 (112) 192 (168)	64
Blowfish	16	32-448 128-default	64
Twofish	16	128,192,256	128
IDEA	8	128	64
CAST-128	16	40-128	64
CAST-256	48	128,160,192,-224,256	128
RC2	18	0-1024	64
RC5	0-255	0-2048	32,64,128
RC6	20	128,192,256	128
AES	10,12,14	128,192,256	128
SAFER SK64	8-10	64,128	64,128
SAFER SK128	8,12,16	128,192,256	128
Mars	32	128-448	128
Skipjack	32	80	64
Serpent	32	128,192,256	128
Seed	16	128	128
Misty1	any multiple of 4	128	64
Gost	32	256	64
Clefia	18,22,26	128,192,256	128
Camellia	18,24	128,192,256	128
ARIA	12,14,16	128,192,256	128
TEA	16,32	128	64
ICE	16	64	64
SHACAL-1	80	128-512	160
SHACAL-2	80	128-512	256

(*) identifies effective strength if different from length

Symmetric Streaming Algorithms

Name	Keysize
RC4	40-2048
W7	128
Sober	128
Rabbit	128
SEAL	160

DES Block Modes

ECB – Electronic Code Book
CBC – Cipher Block Chaining
CFB – Cipher Feedback
OFB – Output Feedback
CTR – Counter Mode

AES Methods

SubBytes
ShiftRows
MixColumns
AddRoundKey

Remembering the common symmetric algorithms

C - CAST
3 - 3DES
2 - Two Fish
B - Blowfish
R - RC4,RC5, RC6
A - AES
I - IDEA
D - DES
S - SAFER

European NESSIE Project

Misty1
Camellia
SHACAL-2
AES

By **rubberdragonfarts** (rubberdragonfarts)

cheatography.com/rubberdragonfarts/

Published 6th August, 2014.
Last updated 7th May, 2016.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com