

# Rijndael by *J. Daemen and V. Rijmen*

Block size	128 bits
Key Size	128, 192, 256 bits
Speed	~18-20 cycles / byte
Mathematical Foundation	Galois Fields
Implementation	<ul style="list-style-type: none"><li>• Basic operations : <math>\oplus</math>, <math>+</math>, shift</li><li>• Small code : 98k</li></ul>

Adopted by the NIST in December 2001

# (pure) Encryption Modes

a.k.a. how to encrypt long messages

**ECB - Electronic Code Book**

**CBC - Cipher Block Chaining**

CFB - Cipher Feedback

OFB - Output Feedback

**CTR - Counter**