## AES - Advanced Encryption Standard

## Timeline

- 1996 NIST issues public call for proposal
- 1998 | 5 algorithms selected
- 2001 winners were announced

## 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> <li>Basic operations : ⊕, + , shift</li> <li>Small code : 98k</li> </ul>

Adopted by the NIST in December 2001