

AES - Advanced Encryption Standard

Timeline

- **1996** NIST issues public call for proposal
- **1998** 15 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 style="list-style-type: none">• Substitution-permutation network• Basic operations : \oplus, $+$, shift• Small code : 98k |

Adopted by the NIST in December 2001