A Performance Comparison of the Five AES Finalists

Bruce Schneier, Counterpane

Doug Whiting, Hi/ fn

Encryption Speeds for 128-bit Keys in Assembly
Encryption Speeds for 192-bit Keys in Assembly

Encryption Speeds for 256-bit Keys in Assembly
Encryption Speeds for 128-bit Keys in C

![Graph showing encryption speeds for 128-bit keys on various processors.]

Encryption Speeds for 192-bit Keys in C

![Graph showing encryption speeds for 192-bit keys on various processors.]

Clock cycles

Cyrix 6x86MX, Pentium, Pentium II, TurboSparc, SuperSparc, UltraSparc, Alpha EV45, Alpha EV56, Alpha EV6, HP PA7000

MARS, RC6, Rijndael, Serpent, Twofish
Encryption Speeds for 256-bit Keys in C

Key Setup and Encryption Rate, Per Byte, for 128-bit Keys on a Pentium II in Assembly
Key Setup and Encryption Rate, Per Byte, for 192-bit Keys on a Pentium II in Assembly

Key Setup and Encryption Rate, Per Byte, for 256-bit Keys on a Pentium II in Assembly
Minimum Secure Rounds

MARS  11
RC6   15
Rijndael  8
Serpent  9
Twofish  6

Encryption Speeds for the Minimal Secure Variant in C
Key Setup and Encryption Rate, Per Byte, for the Minimal Secure Variant on a Pentium II in Assembly

Hardware Key Agility

Sample Application:
- High-speed IPSEC gateways.
- OC-3 full-duplex or greater.
- 10K-100K+ security associations.
- Small-packet (e.g. 64 bytes) performance is the critical benchmark.
**Typical Data Flow Today**

64-byte packet → Context (from RAM) → 70 - 100 bytes: 3DES = 24, HMAC = 40 → Crypto Module → 110-byte packet → Save Context (to RAM) → 4 - 32 bytes

**Data Flow with AES Precomputed Subkeys**

64-byte packet → Context (from RAM) → 200+ bytes: AES = 160+, HMAC = 40 → Crypto Module → 110-byte packet → Save Context (to RAM) → 4 - 32 bytes
### On-The-Fly Key Schedule Penalty

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>MARS</td>
<td>10+ blocks (!)</td>
</tr>
<tr>
<td>RC6</td>
<td>9 blocks (!)</td>
</tr>
<tr>
<td>Rijndael</td>
<td>minimal</td>
</tr>
<tr>
<td>Serpent</td>
<td>minimal</td>
</tr>
<tr>
<td>Twofish</td>
<td>minimal</td>
</tr>
</tbody>
</table>