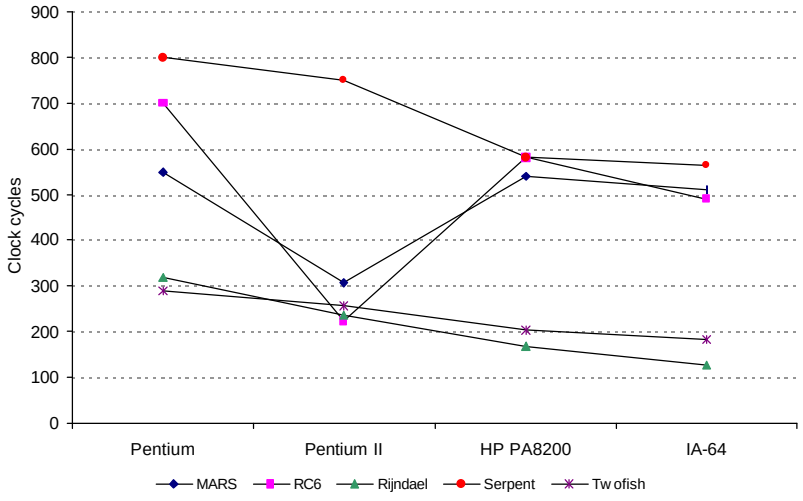
A Performance Comparison of the Five AES Finalists

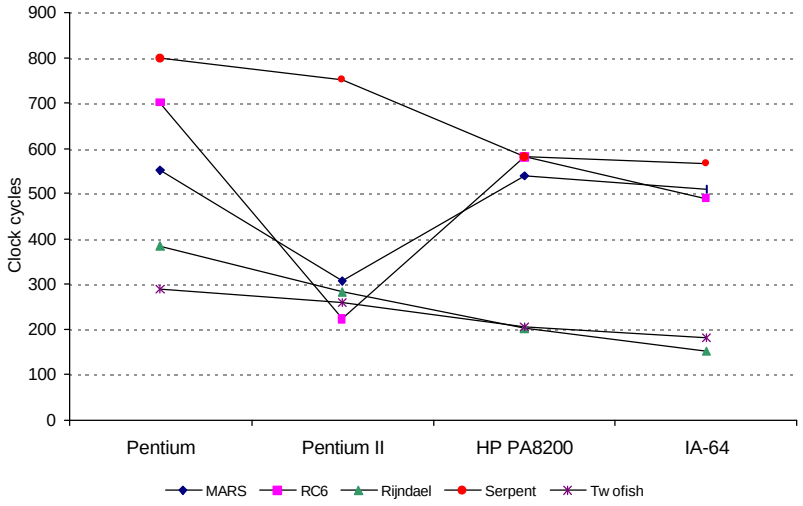
Bruce Schneier, Counterpane

Doug Whiting, Hi/fn

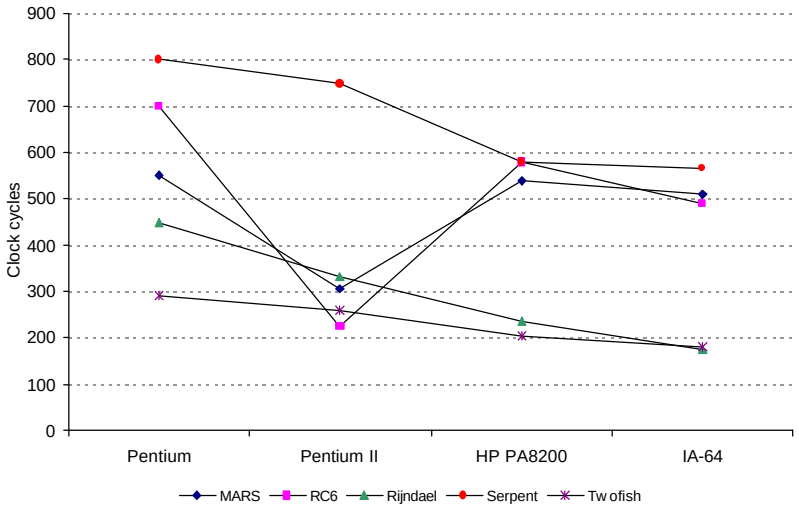
Encryption Speeds for 128-bit Keys in Assembly



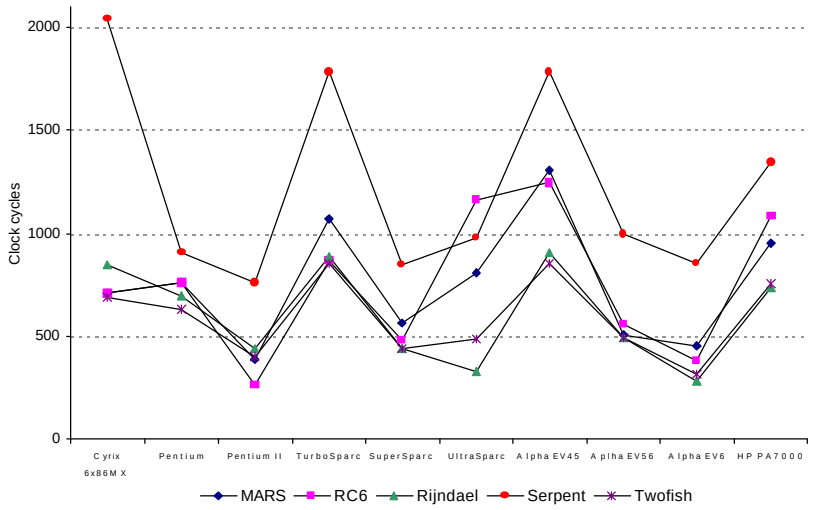
Encryption Speeds for 192-bit Keys in Assembly



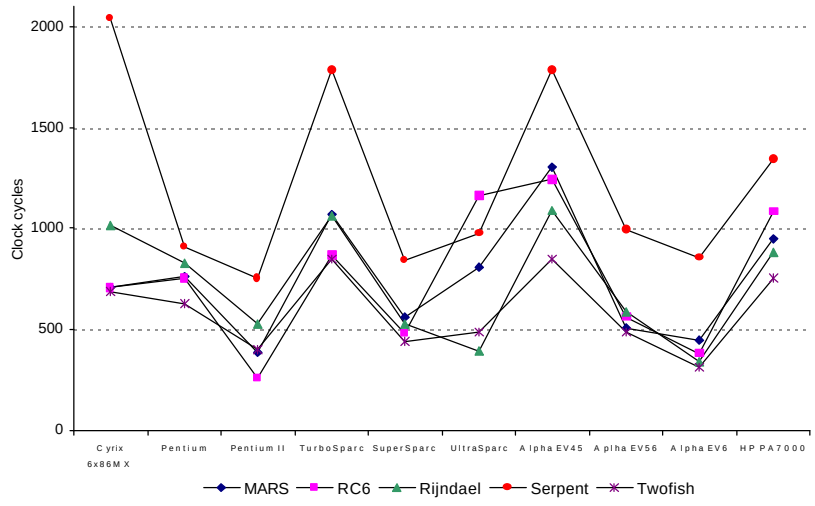
Encryption Speeds for 256-bit Keys in Assembly



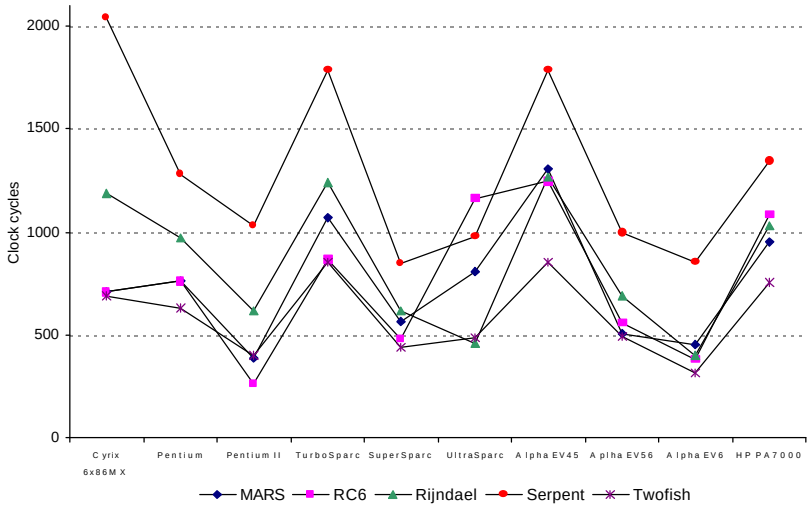
Encryption Speeds for 128-bit Keys in C



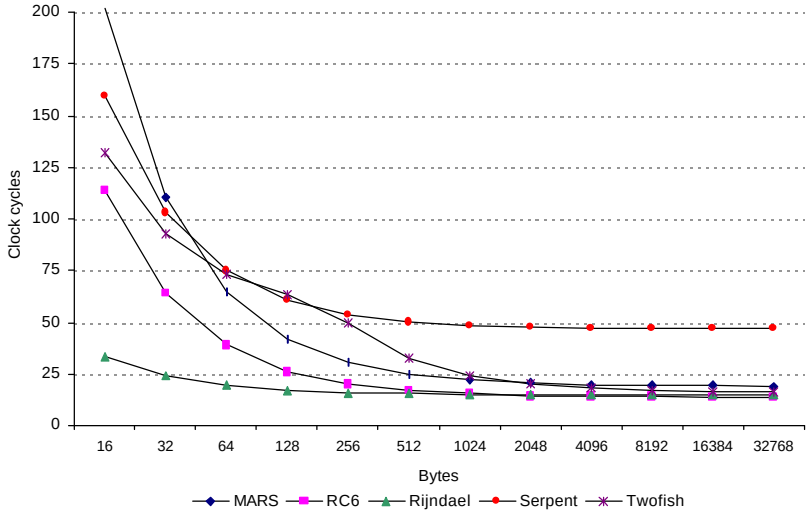
Encryption Speeds for 192-bit Keys in C



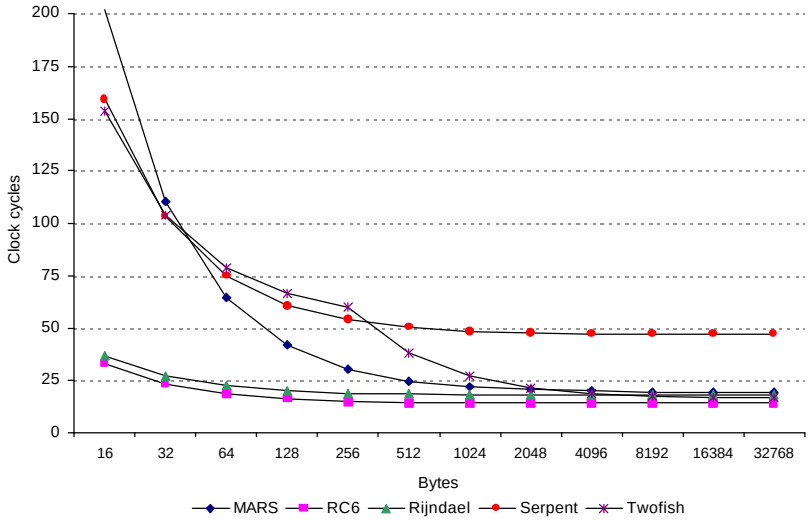
Encryption Speeds for 256-bit Keys in C



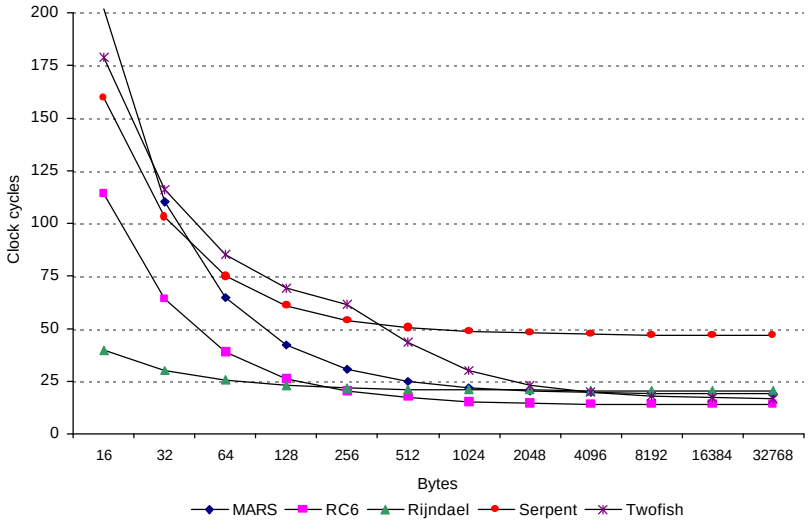
Key Setup and Encryption Rate, Per Byte, for 128-bit Keys on a Pentium II in Assembly



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



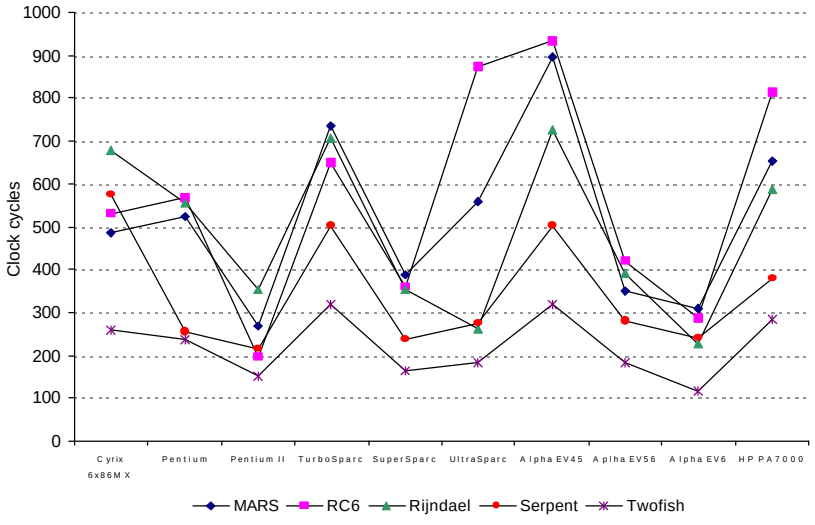
Key Setup and Encryption Rate, Per Byte, for 256-bit Keys on a Pentium II in Assembly



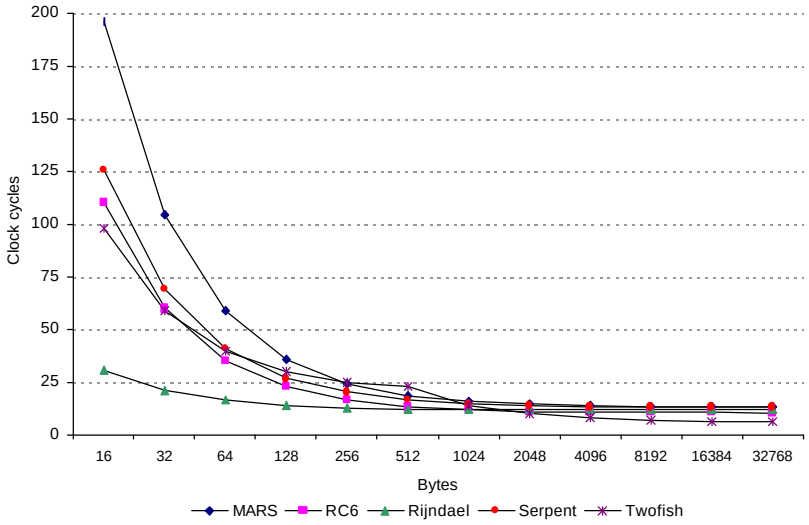
Minimum Secure Rounds

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

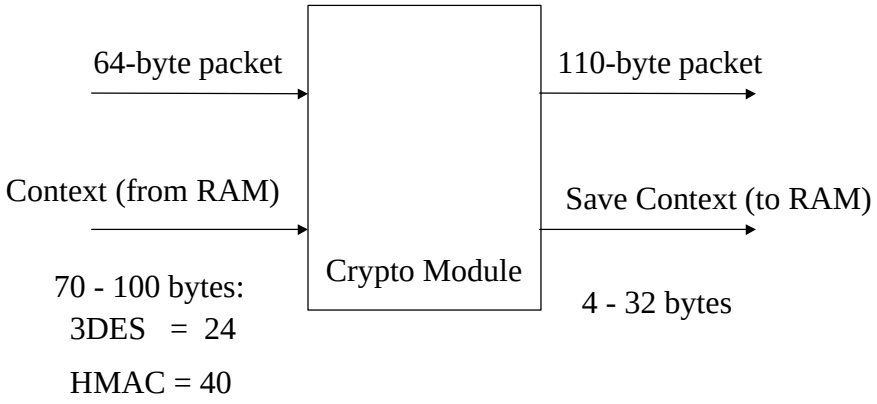


Hardware Key Agility

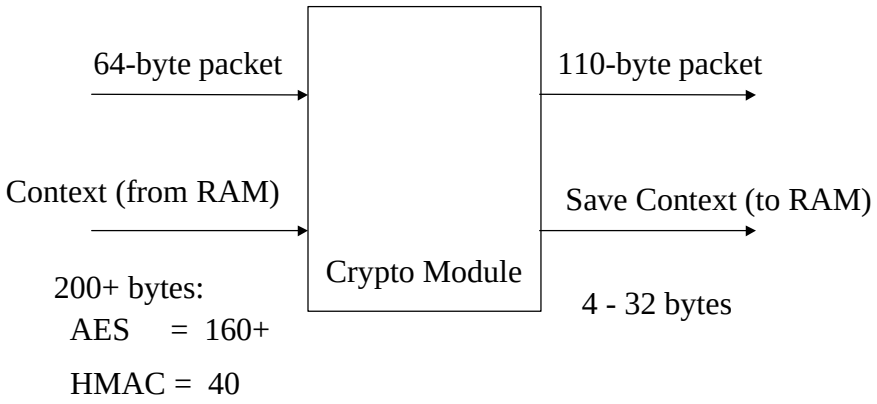
Sample Application:

- High-speed IPSEC gateways.
- OC-3 full-duplex or greater.
- 10K-100K+ security associations.
- Small-packet (e.g. 64 bytes) performance is the the critical benchmark.

Typical Data Flow Today



Data Flow with AES Precomputed Subkeys



On-The-Fly Key Schedule Penalty

MARS	10+ blocks (!)
RC6	9 blocks (!)
Rijndael	minimal
Serpent	minimal
Twofish	minimal