AES = Advanced Encryption Standard

USA offiziell standardisiert und wird dort seitdem für die Verschlüsselung staatlicher Dokumente verwendet

Entwickler: Vincent Rijmen und Joan Daemen

Die Blocklänge des AES beträgt 128 Bit. Das Verfahren Rijndael unterstützt zwar auch 192 und 256 Bit

Die AES-Schlüssellänge kann – wie bei allen AES-Kandidaten – wahlweise auf 128, 192 oder 256 Bit festgelegt werden. Die Rundenzahl ist, wie in der folgenden Tabelle dargestellt, von der Schlüssellänge abhängig: Schlüssellänge Rundenzahl