

Twofish ist ein symmetrischer Blockverschlüsselungsalgorithmus mit einer Blockgröße von 128 Bit.

Twofish ist ein symmetrisches Verschlüsselungsverfahren, das zum Schutz digitaler Daten vor unbefugtem Zugriff eingesetzt wird. Es wurde 1998 von einem Entwicklerteam um den US-amerikanischen Kryptografen Bruce Schneier vorgestellt und gehörte zu den fünf Finalisten im Wettbewerb um den neuen Verschlüsselungsstandard AES (Advanced Encryption Standard).

Bei Twofish handelt es sich um eine sogenannte Blockchiffre, die Daten in Blöcken von jeweils 128 Bit verschlüsselt. Das Verfahren unterstützt Schlüssellängen von 128, 192 und 256 Bit. Bei der symmetrischen Verschlüsselung wird derselbe geheime Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln der Daten verwendet.

Twofish arbeitet mit einer Feistel-ähnlichen Struktur und führt insgesamt 16 Verschlüsselungsrunden durch. Dabei werden verschiedene mathematische Operationen kombiniert, um die ursprünglichen Daten so zu verändern, dass sie ohne den passenden Schlüssel nicht mehr lesbar sind. Das Verfahren wurde auf hohe Sicherheit und eine effiziente Umsetzung in Software und Hardware ausgelegt.

Im Jahr 2000 entschied sich das US-amerikanische National Institute of Standards and Technology (NIST) für das Verschlüsselungsverfahren Rijndael als Grundlage des neuen AES-Standards. Twofish wurde damit nicht zum offiziellen AES-Standard, gilt aber weiterhin als gut untersuchtes und nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren.

Twofish kann beispielsweise zur Verschlüsselung von Dateien, Datenträgern und anderen gespeicherten Informationen verwendet werden. Bekannt ist das Verfahren unter anderem durch die Verschlüsselungssoftware VeraCrypt, die Twofish auch in Kombination mit anderen Verschlüsselungsalgorithmen unterstützt.

Die Sicherheit verschlüsselter Daten hängt allerdings nicht nur vom verwendeten Algorithmus ab, sondern auch von der Qualität des Schlüssels, dem eingesetzten Betriebsmodus und der korrekten technischen Umsetzung.