

ChaCha20 ist ein symmetrischer Verschlüsselungsalgorithmus, der zur Familie der Stromchiffren gehört. Er wurde 2008 vom US-amerikanischen Kryptografen Daniel J. Bernstein vorgestellt und basiert auf dem älteren Verschlüsselungsverfahren Salsa20. ChaCha20 wurde entwickelt, um digitale Daten schnell und sicher zu verschlüsseln, und wird heute unter anderem bei verschlüsselten Internetverbindungen und Netzwerkprotokollen eingesetzt.

Im Gegensatz zu Blockchiffren wie AES verarbeitet ChaCha20 die Daten nicht in Blöcken fester Klartextgröße, sondern erzeugt einen kryptografischen Schlüsselstrom. Dieser wird mithilfe einer XOR-Verknüpfung mit den zu verschlüsselnden Daten kombiniert. Bei der Entschlüsselung wird derselbe Schlüsselstrom erneut verwendet, wodurch sich der ursprüngliche Klartext wiederherstellen lässt.

ChaCha20 verwendet einen 256 Bit langen geheimen Schlüssel und führt insgesamt 20 Verarbeitungsrunden aus. Der interne Zustand des Algorithmus besteht aus 512 Bit und wird durch Additionen, XOR-Verknüpfungen und Bitrotationen verändert. Diese Operationen sind auf modernen Prozessoren besonders effizient ausführbar. Die Zahl 20 im Namen bezeichnet die Anzahl der Runden und nicht die Schlüssellänge.

Neben dem geheimen Schlüssel benötigt ChaCha20 einen sogenannten Nonce (Number Used Once) sowie einen Blockzähler. Die Nonce sorgt dafür, dass bei mehreren Verschlüsselungsvorgängen mit demselben Schlüssel unterschiedliche Schlüsselströme entstehen. Besonders wichtig ist, dass dieselbe Kombination aus Schlüssel und Nonce nicht mehrfach verwendet wird, da andernfalls die Vertraulichkeit der verschlüsselten Daten gefährdet werden kann.

Häufig wird ChaCha20 mit dem Authentifizierungsverfahren Poly1305 kombiniert. Diese Verbindung wird als ChaCha20-Poly1305 bezeichnet und gehört zu den Verfahren der authentifizierten Verschlüsselung (Authenticated Encryption with Associated Data, AEAD). Dabei werden die Daten nicht nur verschlüsselt, sondern zusätzlich gegen unbemerkte Veränderungen geschützt. ChaCha20 allein bietet dagegen keine solche Integritätsprüfung.

ChaCha20-Poly1305 wird unter anderem bei TLS 1.3, dem Verschlüsselungsprotokoll moderner HTTPS-Verbindungen, eingesetzt. Auch das VPN-Protokoll WireGuard verwendet eine darauf basierende authentifizierte Verschlüsselung. ChaCha20 ist insbesondere auf Geräten ohne spezielle AES-Hardwarebeschleunigung eine leistungsfähige Alternative zu AES-basierten Verfahren.

ChaCha20 gehört zu den etablierten modernen Verschlüsselungsalgorithmen. Durch seine vergleichsweise einfache Struktur, hohe Verarbeitungsgeschwindigkeit und gute Eignung für

unterschiedliche Hardwareplattformen wird er in zahlreichen Sicherheitsanwendungen eingesetzt. Für den praktischen Datenschutz ist jedoch nicht nur der Algorithmus selbst entscheidend, sondern auch seine korrekte Implementierung und die sichere Verwaltung der verwendeten Schlüssel und Nonces.

Weiterführende Informationen

Symmetrische Verschlüsselung, Stromchiffre, Salsa20, ChaCha20-Poly1305, Poly1305, AES, TLS 1.3, WireGuard