LU05.L04 - Vergleich moderner symmetrischer Verschlüsselungsverfahren

	Sicherheit	Schlüssellänge	Schwächen	Anwendungsbereiche
IDEA	Hoch, aber durch Brute-Force-Angriffe bedroht	128 Bit	Empfindlich gegenüber bestimmten kryptoanalytischen Angriffen	E-Mail-Verschlüsselung, VPNs, Dateiverschlüsselung
AES	Sehr hoch, gilt als Standard	128, 192, 256 Bit	Theoretische Seitkanalangriffe, praktisch weiterhin sicher	Regierungsdaten, Finanzsektor, allgemeine Datenverschlüsselung
ChaCha20	Hoch, verbessert gegenüber älteren Stromchiffren	256 Bit	Weniger erforscht als AES, aber bisher keine bedeutenden Schwächen bekannt	TLS ab Version 1.3, sichere Messaging-Dienste, mobile Verschlüsselung