

Betriebsarten für Blockchiffren

Verfahren	Vorteile	Nachteile
Electronic Codebook (ECB)	<ul style="list-style-type: none"> ✓ Schnell: Blöcke können unabhängig voneinander verschlüsselt werden, gut parallelisierbar ✓ Bei fehlerhafter Übertragung eines Blocks wird nur ein Block falsch entschlüsselt ✓ Einfache Implementierung ✓ Unabhängig von einem IV 	<ul style="list-style-type: none"> ✓ Unsicher gegenüber Replay-Attacken, Blöcke können unbemerkt mehrfach gesendet, neu eingespeist oder in ihrer Reihenfolge getauscht werden ✓ Angriffe gegen monoalphabetische Chiffren möglich (Häufigkeitsanalysen) ✓ Verschlüsselung kann erst begonnen werden, wenn ein Block vollständig ist (schlecht z.B. bei Tastatureingaben)
Cipher Block Chaining (CBC)	<ul style="list-style-type: none"> ✓ Attacken gegenüber monoalphabetischen Chiffren werden bei CBC unwirksam ✓ Gleiche Klartextblöcke werden zu verschiedenen Chiffretext-blöcken verschlüsselt 	<ul style="list-style-type: none"> ✓ Austauschproblem: IV ✓ Bei fehlerhafter Übertragung eines Blocks werden genau 2 Blöcke falsch entschlüsselt ✓ Langsamer als ECB wegen Berechnungsabhängigkeiten
Output Feedback (OFB)	<ul style="list-style-type: none"> ✓ Berechnung des Schlüsselstroms unabhängig vom Klartext, kann also vorausberechnet werden (<i>synchrone Stromchiffre</i>) ✓ Hohe Verschlüsselungsraten ✓ Fehlerhafte Übertragung eines Blocks --> 1 falsch entschlüsselter Block 	<ul style="list-style-type: none"> ✓ Austauschproblem: IV ✓ Klartextbits haben keinen Einfluss auf den folgenden Schlüsselstrom
Cipher Feedback (CFB)	<ul style="list-style-type: none"> ✓ Gute Diffusion: Chiffretextblöcke hängen von ihren jeweiligen Vorgängern und den Klartexten ab (<i>asynchrone Stromchiffre</i>) 	<ul style="list-style-type: none"> ✓ Austauschproblem: IV ✓ Keine Vorausberechnung des Schlüsselstroms möglich --> geringere Geschwindigkeit als z.B. bei OFB ✓ Fehlerhafte Übertragung eines Chiffreblocks führt zur falschen Entschlüsselung von genau 2 Blöcken