Kryptologie LAB 03 - Betriebsmodi

Luc Spachmann

FSU Jena

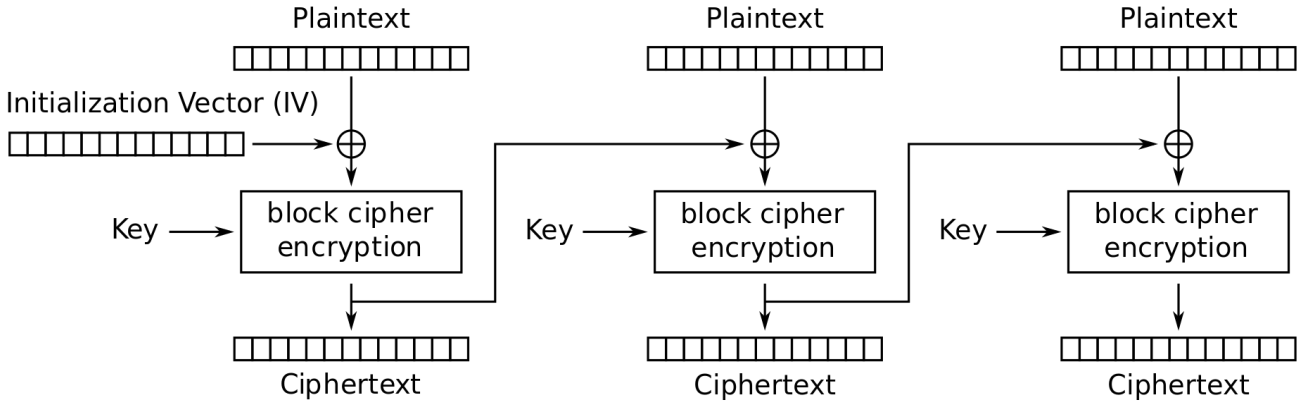
9. November 2023

Betrachtete Betriebsmodi

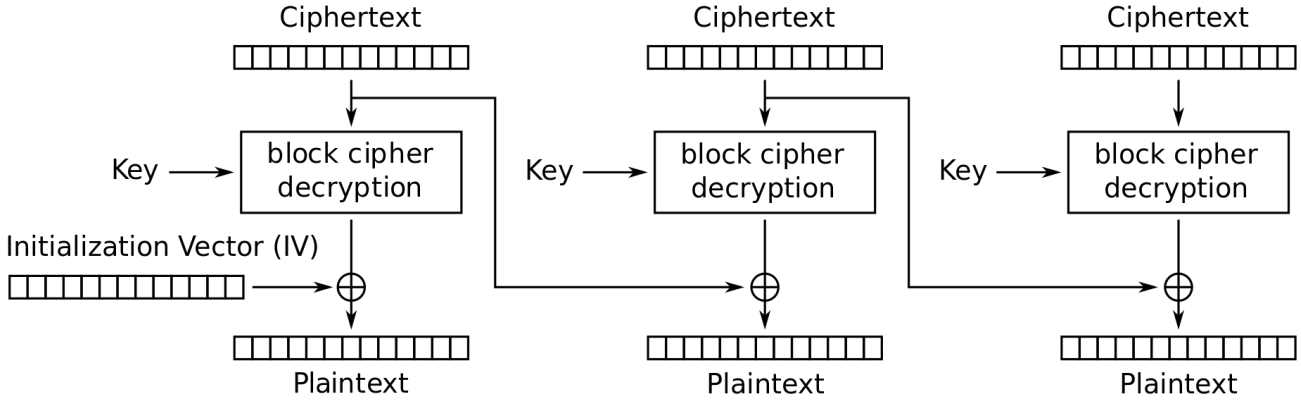
Neu: Ab jetzt Bitstrings, nicht mehr Buchstaben als Alphabet

- electronic code book (ECB)
  - Zerschneiden der Nachricht in Blöcke
  - Diese jeweils verschlüsseln
- cipher block chaining (CBC)
- output feedback (OFB)
- counter (CTR)

CBC Details



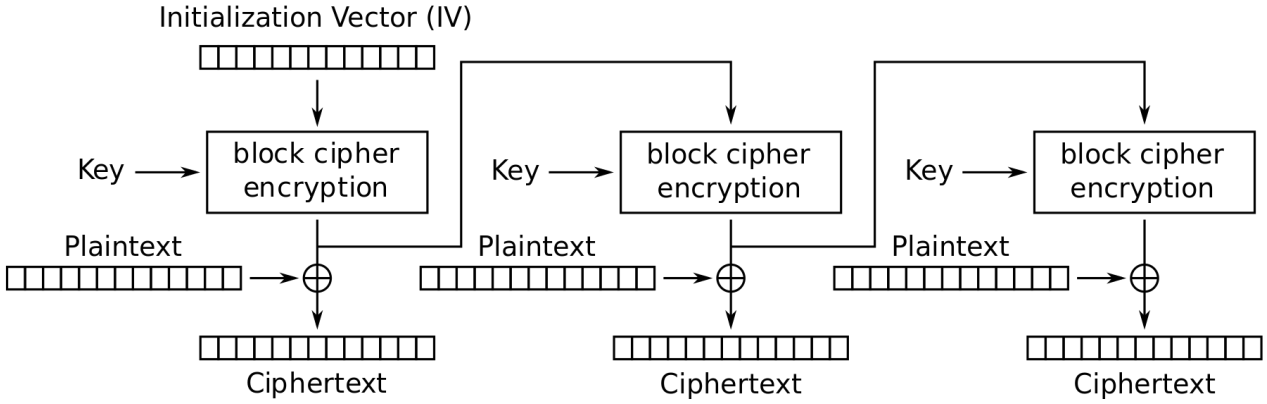
Cipher Block Chaining (CBC) mode encryption



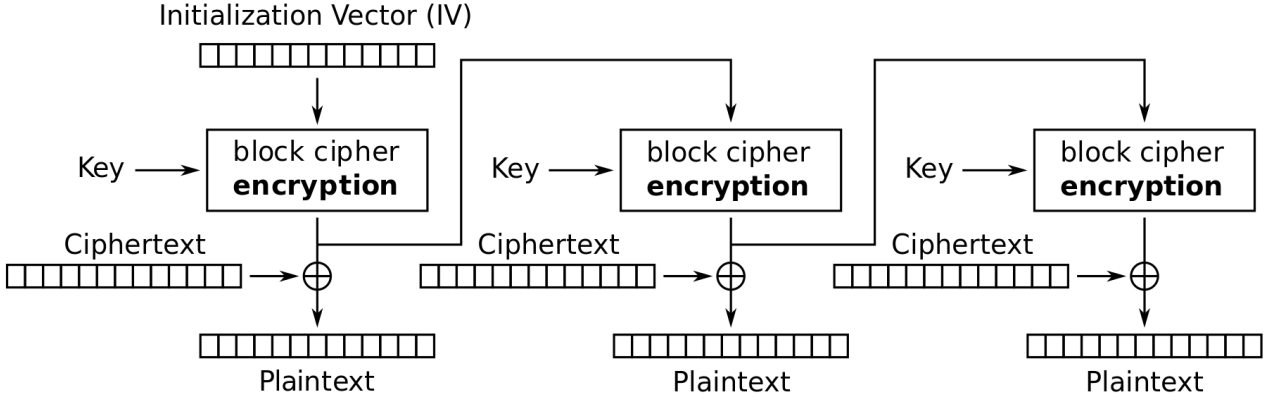
Cipher Block Chaining (CBC) mode decryption

Initialisierungsvektor Nullvektor

OFB Details



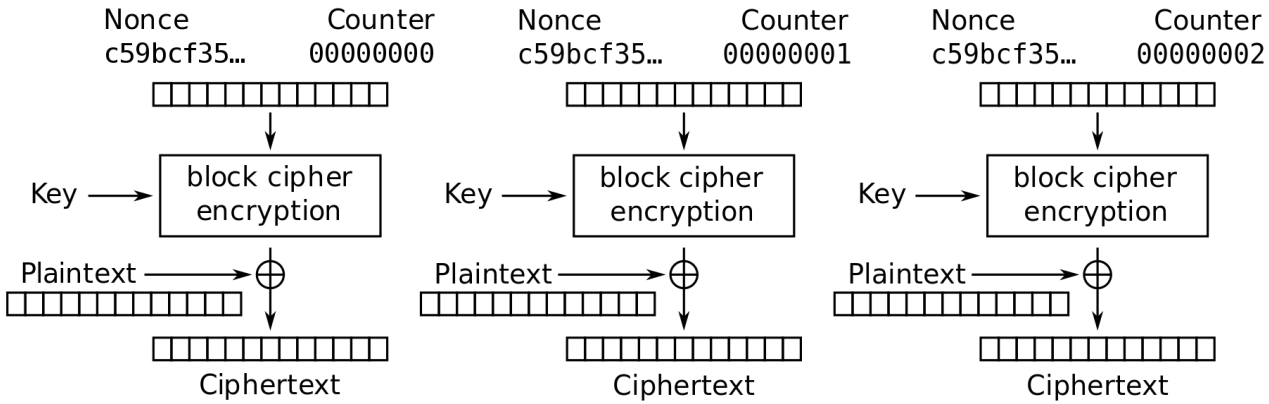
Output Feedback (OFB) mode encryption



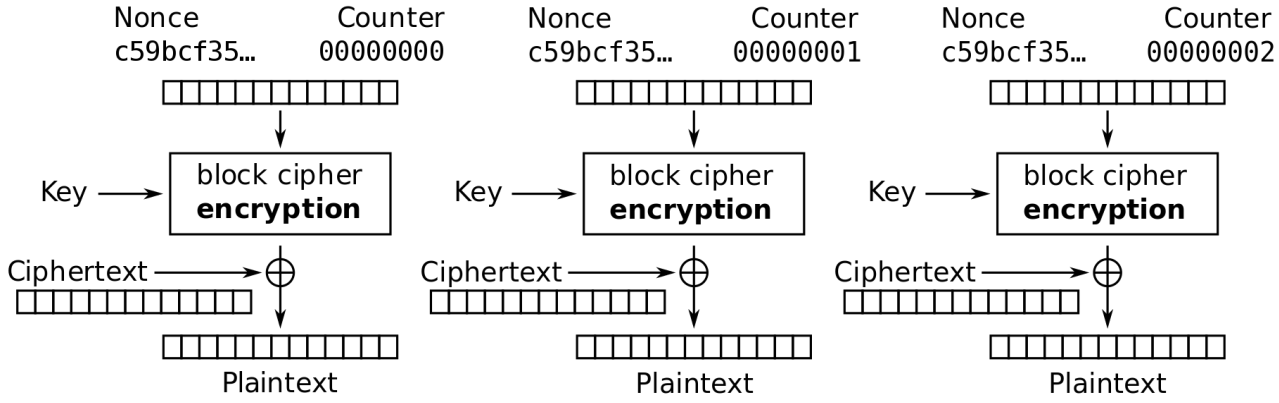
Output Feedback (OFB) mode decryption

Initialisierungsvektor Parameter

CTR Details



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Initialisierungsvektor (Nonce) hier Nullvektor, also nur Counter verschlüsseln

Aufgaben

- Funktionen für diese Betriebsmodi implementieren
- Gesuchte Blocklänge t als Parameter
- Für ECB/CBC: Nachricht mit Nullen auffüllen auf vielfaches von t
- Verwendete Ver-/ Entschlüsselungen als Blackbox
- Idee nächste Woche: mit AES verbinden