

# Betriebsmodi von Blockchiffren - Kontrollfragen

Dozent: Prof. Dr. Michael Eichberg  
Kontakt: [michael.eichberg@dhbw.de](mailto:michael.eichberg@dhbw.de), Raum 149B  
Version: 1.0.1

---

# 1. Betriebsmodi - Grundlagen

---

# Übung

## 1.1. Grundlagen

1. Warum sind Betriebsmodi von Nöten? Begründen Sie mit einem Beispiel.
2. Eignet sich CBC für die Verwendung einer Blockchiffre als Stromchiffre?
3. Nennen Sie zwei *allg.* Verfahren für das Padding von Nachrichten und erklären Sie diese kurz.
4. Welche Kriterien können zur Bewertung eines Operationsmodis herangezogen werden?
5. Verhalten sich alle Betriebsmodi bei Bitfehlern im Chiffretext - zum Beispiel aufgrund von Übertragungsfehlern - gleich?

(D.h. wenn einzelne Bits des Chiffretexts gekippt sind.)

## 2. Spezielle Betriebsmodi

---

# Tweakable Blockchiffre

## 2.1. AES-XTS

1. Erklären Sie den Aufbau von AES-XTS.
2. Warum muss der Tweak nicht geheim gehalten werden?