# Kontrollfragen: Blockchiffren



Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhbw.de, Raum 149B

Version: 1.0.1

# 1. Blockchiffren - Allgemein

### Kontrollfragen

1.1. Wie unterscheidet sich eine Blockchiffre von einer Stromchiffere?



1.3. Sind Blockchiffren Stromchiffren technisch überlegen?

1.4. Welche grundlegenden Techniken sollten Blockchiffren immer umsetzen, um welche Ziele zu erreichen?

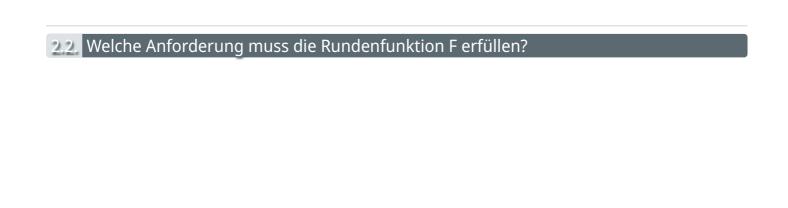
1.5. Welchem Zweck soll die Diffusion bzw. Konfusion dienen?

### 2. Blockchiffren - Feistel

Δ

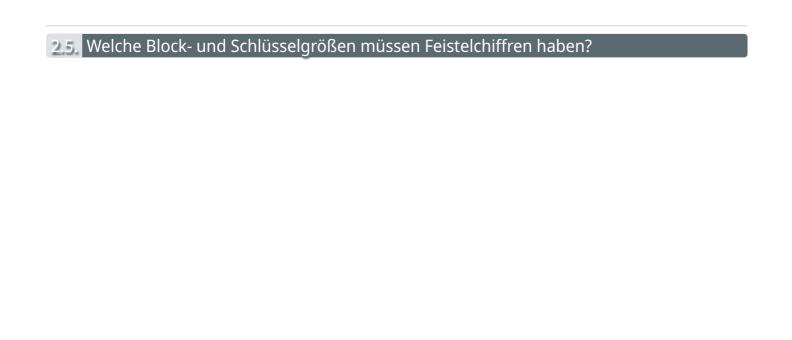
#### Kontrollfragen

2.1. Warum wird am Ende einer Verschlüsselung (und Entschlüsselung) noch eine SWAP-Operation durchgeführt?





2.4. Wenn wir nur eine Runde eine Feistelchiffre anwenden, sind dann bereits alle Daten zumindest rudimentär verschlüsselt?



2.6. Was ist bei der Generierung des Unterschlüssel bei Ver- und Entschlüsseln zu beachten?

#### 3. Blockchiffren - DES

## Kontrollfragen

3.1. Welche Schlüsselgröße hat DES?

#### 3.2. Welche Aussage über DES ist korrekt?

- DES basiert auf einem Feistel-Netzwerk mit 16 Runden.
- Beim Design von DES wurde das Kerckhoff Prinzip eingehalten.
- DES ist gegen Brute-Force-Angriffe immun.

3.3. Was versteht man unter Triple-DES (3DES)?