DHBW
Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

IT-Security Cryptography and Secure Communications

Excercise: **Block Cipher Operation**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2023-10-11

1. Why is it important in CBC to protect the IV?
2. In which operation modes is padding necessary?
3. What happens in case of a transmission error (single bit flip in the ciphertext) in ECB, CBC, CFB, OFB, CTR?
4. Why does the IV in OFB has to be a nonce (i.e., unique to each execution of the encryption algorithm)?