RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie
Eike Kiltz
Emiel Wiedijk

Präsenzübungen zur Vorlesung

Introduction to Cryptography

Winter 2025/2026

Blatt 1

Exercise 1:
What does Kerckhoff's principle state?

A. Security should rely on keeping the algorithm secret
B. The key should be as long as the message
C. A cryptosystem should be secure even if everything except the key is public

Exercise 2:
What operation does the One-Time Pad use for encryption?

A. AND operation
B. XOR operation ($\oplus$)
C. Modular addition

Exercise 3:
What is the key property that makes XOR suitable for OTP?

A. It is self-inverse: $(M \oplus K) \oplus K = M$
B. It always produces output of 1
C. It compresses the data

Exercise 4:
What makes OTP provably secure?

A. The ciphertext is uniformly distributed regardless of the plaintext
B. The XOR operation is fast
C. The key is very long

Exercise 5:
What probability does each possible ciphertext have in OTP for a given plaintext?

A. 0
B. 1
C. $\frac{1}{2^n}$, where n is the message length in bits
D. $\frac{1}{2^{n/2}}$, where n is the message length in bits

Exercise 6:
What does "real or random" mean in cryptographic security?

A. The key is either real or randomly generated
B. The message is either meaningful or random
C. The adversary cannot distinguish actual ciphertexts from random data

Exercise 7:
What happens if you reuse a key in OTP?

A. Security is broken; patterns can be revealed
B. The encryption becomes faster
C. Nothing, it remains secure

Exercise 8:
What alternative operation to XOR would still provide OTP security?

A. OR operation
B. Modular addition
C. AND operation

Exercise 9:
What is the correct relationship in OTP correctness?

A. $\mathsf{Dec}(K, \mathsf{Enc}(K, M)) = M$
B. $\mathsf{Enc}(K, \mathsf{Dec}(K, C)) = C$
C. $\mathsf{Enc}(M, K) = \mathsf{Dec}(M, K)$

Exercise 10:
What assumption about the adversary is necessary for OTP security proofs?

A. The adversary is computationally bounded
B. The adversary cannot see ciphertexts
C. The adversary cannot influence key sampling

Exercise 11:
Show that the OTP where $\oplus$ is replaced with $\pmod n$ is correct and secure.

Exercise 12:
Consider the following variant of the OTP.

A. Let $K = (K_1, K_2) \in \{0,1\}^{2n}$ be a uniformly distributed key. Encryption is defined as

$$\mathsf{Enc}((K_1, K_2), M) := M \oplus K_1 \oplus K_2.$$

Provide a correct decryption procedure and show its security.
B. Show that the cipher from part A is still secure if K_1 is known.
C. Let $K \in \{0,1\}^n$ be a uniformly distributed key. Encryption and decryption are defined as

$$\mathsf{Enc}(K, M) := K; \quad \mathsf{Dec}(K, C) := C$$

Show that encryption is secure. Would you recommend using the cipher?