RUHR UNIVERSITÄT BOCHUM
RUB

Lehrstuhl für Kryptologie
Eike Kiltz

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
Solution: [C]. According to Kerckhoff's principle says we should assume that the cryptosystem is public, to avoid security through obscurity.

Exercise 2:
What operation does the One-Time Pad use for encryption?
A. AND operation
B. XOR operation ($\oplus$)
C. Modular addition
Solution: [B]. As defined in the lecture the OTP uses XOR, implementing the OTP with AND gives neither correctness nor security. You could define a variant of the one-time pad using 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
Solution: [A]. Because XOR is invertible we can recover the message as long as we know the key.

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
Solution: [A]. As the ciphertext has the same (uniform) distribution for every plaintext, the adversary cannot deduce any information about the plaintext.

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

Solution: [C]. The ciphertext looks uniform, and there are 2^n possible bitstrings of length n, therefore any individual ciphertext occurs with probability $\frac{1}{2^n}$.

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

Solution: [C]. The "real or random" paradigm is useful because if the adversary cannot distinguish valid ciphertexts from random data, then he also cannot distinguish between ciphertexts of different plaintexts.

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

Solution: [A]. Suppose we use the key K for messages M_1 and M_2. Based on the ciphertexts $C_1 = M_1 \oplus K$ and $C_2 = M_2 \oplus K$ the adversary can deduce

$$M_1 \oplus M_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = C_1 \oplus C_2.$$

Exercise 8:
What alternative operation to XOR would still provide OTP security?
A. OR operation
B. Modular addition
C. AND operation

Solution: [B]. If K is uniformly distributed over $\{0, \ldots, n-1\}$ then $M + K \mod n$ is also uniform, regardless of M.

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

Solution: [A]. We should recover the original message by decrypting using the same key.

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

Solution: [C]. The ciphertext looks uniform to the adversary because he has no information about the key. If the adversary could influence key sampling, then the ciphertext would not be uniform anymore and information about the message will leak.

Exercise 11:
Show that the OTP where $\oplus$ is replaced with $\pmod n$ is correct and secure.
Solution: We define the following encryption scheme on messages $M \in \{0, \ldots, n-1\}$, and key K uniform in $\{0, \ldots, n-1\}$.

$$\begin{aligned} \mathsf{Enc}(K, M) &= M + K \mod n \\ \mathsf{Dec}(K, C) &= C - K \mod n. \end{aligned}$$

For **correctness** we need to show that $\mathsf{Dec}(K, \mathsf{Enc}(K, M)) = M$ for all K and M. This follows because

$$\begin{aligned} \mathsf{Dec}(K, \mathsf{Enc}(K, M)) &= (M + K \mod n) - K \mod n \\ &= (M + K - K) \mod N \\ &= M \mod N \\ &= M, \end{aligned}$$

because $0 \leq M < N$.
For **security** we use the "real or random" paradigm. The adversary should not be able to distinguish between a random ciphertext and a valid encryption of a message. A valid encryption of a message M is modelled by the following $\mathsf{Attack}(M)$ game

$\underline{\mathsf{Attack}(M)}$:
$K \leftarrow \{0, \ldots, n-1\}$
$C := M + K \mod n$
return C

As encryptions should look uniform, we want that $\Pr[\mathsf{Attack}(M) = C] = \frac{1}{n}$ for all M and C. This fact follows because

$$\begin{aligned} \Pr[\mathsf{Attack}(M) = C] &= \Pr[M + K \mod n = C] \\ &= \Pr[K = (C + M) \mod n] \\ &= \frac{1}{n} \end{aligned}$$

as K is chosen uniformly at random, so the value of $C + M$ is as likely as any other. As $\mathsf{Attack}(M)$ is indistinguishable from a randomly chosen ciphertext our variation of the one-time pad is 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.
Solution: This cipher is essentially equivalent to encrypting a message with one-time pad twice with independent keys. The decryption procedure should be defined as

$$\mathsf{Dec}((K_1, K_2), C) = C \oplus K_1 \oplus K_2.$$

To prove **correctness** we need to show that $\mathsf{Dec}((K_1, K_2), \mathsf{Enc}((K_1, K_2), M)) = M$. This follows because

$$\begin{aligned}
\mathsf{Dec}((K_1, K_2), \mathsf{Enc}((K_1, K_2), M)) &= \mathsf{Dec}((K_1, K_2), M \oplus K_1 \oplus K_2) \\
&= M \oplus K_1 \oplus K_2 \oplus K_1 \oplus K_2 \\
&= M \oplus (K_1 \oplus K_1) \oplus (K_2 \oplus K_2) \\
&= M \oplus 0 \oplus 0 \\
&= M.
\end{aligned}$$

To prove **security** we need to show that outputs from the following $\mathsf{Attack}(M)$ game look uniform for any message $M \in \{0,1\}^n$.

$\underline{\mathsf{Attack}(M)}$:
$K_1 \leftarrow \{0,1\}^n$
$K_2 \leftarrow \{0,1\}^n$
$C := M \oplus K_1 \oplus K_2$
return C

So

$$\begin{aligned}
\Pr[\mathsf{Attack}(M) = C] &= \Pr[M \oplus K_1 \oplus K_2 = C] \\
&= \Pr[K_2 = M \oplus K_1 \oplus C] \\
&= 1/2^n.
\end{aligned}$$

B. Show that the cipher from part A is still secure if K_1 is known.
Solution: Recall that the cipher essentially encrypts a message using two independent keys. Intuitively, if one key is known, then the second key should still provide security. We model leakage of K_1, by giving the adversary access to K_1 as part of our $\mathsf{Attack}(M)$ game

$\underline{\mathsf{Attack}(M)}$:
$K_1 \leftarrow \{0,1\}^n$
$K_2 \leftarrow \{0,1\}^n$
$C := M \oplus K_1 \oplus K_2$
return (C, K_1)

Let $M \in \{0,1\}^n$ be any message. For every ciphertext C and leaked key $\tilde{K}$ we have

that

$$\begin{aligned}\Pr[\mathsf{Attack}(M) = (C, \tilde{K})] &= \Pr[(M \oplus K_1 \oplus K_2, K_1) = (C, \tilde{K})] \\ &= \Pr[M \oplus K_1 \oplus K_2 = C \wedge K_1 = \tilde{K}] \\ &= \Pr[K_2 = M \oplus \tilde{K} \oplus C] \cdot 2^{-n} \\ &= 2^{-n} \cdot 2^{-n} \\ &= 2^{-2n}.\end{aligned}$$

So even if the K_1 part of the key leaks, the joint distribution of (C, K_1) still looks uniform for every possible message, so security of preserved.

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?

Solution: To show security we need that encryptions of the message do not leak any information about the message. We redefine our $\mathsf{Attack}(M)$ game as

$\mathsf{Attack}(M)$:
$K \leftarrow \{0,1\}^n$
$C := K$
return C

Now $\Pr[\mathsf{Attack}(M) = C] = 2^{-n}$ easily follows for all messages M and ciphertexts C as $\Pr[\mathsf{Attack}(M) = C] = \Pr[K = C] = 2^{-n}$ because K is uniform.

While the encryption is secure, it is also useless as decryption is not possible. When we decrypt, we recover $\mathsf{Dec}(K, \mathsf{Enc}(K, M)) = \mathsf{Dec}(K, K) = K$ the key rather than the message.