Binäres One-Time-Pad (Bin-OTP)

Beim **Bin-OTP** arbeiten wir nicht mit dem lateinischen Alphabet $\{A, \ldots, Z\}$, sondern mit dem binären Alphabet $\{0, 1\}$.

Klartextbit \ Schlüsselbit	0	1
0	0	1
1	1	0

Abbildung: Binäre Vigenère-Tabelle ($\oplus$ / XOR-Operation)

Verschlüsselung mit der $\oplus$-Operation (XOR)

Die Verschlüsselung erfolgt Bit für Bit mittels der Operation $\oplus$ (auch *XOR* oder exklusives ODER genannt):

$$0 \oplus 0 = 0 \qquad \text{und} \qquad 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1 \qquad \text{und} \qquad 1 \oplus 1 = 0$$

Verschlüsselung mit der $\oplus$-Operation (XOR)

Die Verschlüsselung erfolgt Bit für Bit mittels der Operation $\oplus$ (auch *XOR* oder exklusives ODER genannt):

$$0 \oplus 0 = 0 \quad \text{und} \quad 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1 \quad \text{und} \quad 1 \oplus 1 = 0$$

Beispiel (Verschlüsselungsbeispiel)

Klartext 101, Schlüssel 111:

$$\begin{array}{cccc} & 1 & 0 & 1 \\ \oplus & 1 & 1 & 1 \\ \hline & 0 & 1 & 0 \end{array}$$

Somit ist der Kryptotext 010.

Mathematische Eigenschaften der $\oplus$-Operation

Für beliebige binäre Folgen a, b, c gleicher Länge gelten folgende Gesetze:

- **Kommutativität**:

$$a \oplus b = b \oplus a$$

Mathematische Eigenschaften der $\oplus$-Operation

Für beliebige binäre Folgen a, b, c gleicher Länge gelten folgende Gesetze:

- **Kommutativität**:

$$a \oplus b = b \oplus a$$

- **Selbstinversität** (Verschlüsselung mit sich selbst ergibt 0):

$$a \oplus a = 0$$

Mathematische Eigenschaften der $\oplus$-Operation

Für beliebige binäre Folgen a, b, c gleicher Länge gelten folgende Gesetze:

- **Kommutativität**:

$$a \oplus b = b \oplus a$$

- **Selbstinversität** (Verschlüsselung mit sich selbst ergibt 0):

$$a \oplus a = 0$$

- **Neutrales Element** (Verschlüsselung mit Nullen verändert nichts):

$$a \oplus 0 = a$$

Mathematische Eigenschaften der $\oplus$-Operation

Für beliebige binäre Folgen a, b, c gleicher Länge gelten folgende Gesetze:

- **Kommutativität**:
$$a \oplus b = b \oplus a$$
- **Selbstinversität** (Verschlüsselung mit sich selbst ergibt 0):
$$a \oplus a = 0$$
- **Neutrales Element** (Verschlüsselung mit Nullen verändert nichts):
$$a \oplus 0 = a$$
- **Assoziativität**:
$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

Warum funktioniert die Entschlüsselung?

Sei t der Klartext und s ein zufälliger geheimer Schlüssel.

- **Verschlüsselung**: $c = t \oplus s$

Warum funktioniert die Entschlüsselung?

Sei t der Klartext und s ein zufälliger geheimer Schlüssel.

- **Verschlüsselung**: $c = t \oplus s$
- **Entschlüsselung** (erneute Anwendung desselben Schlüssels s):

$$\begin{aligned} c \oplus s &= (t \oplus s) \oplus s \\ &= t \oplus (s \oplus s) && \text{(Assoziativität)} \\ &= t \oplus 0 && \text{(Selbstinversität: } s \oplus s = 0\text{)} \\ &= t && \text{(Neutrales Element: } t \oplus 0 = t\text{)} \end{aligned}$$

Warum funktioniert die Entschlüsselung?

Sei t der Klartext und s ein zufälliger geheimer Schlüssel.

- **Verschlüsselung**: $c = t \oplus s$
- **Entschlüsselung** (erneute Anwendung desselben Schlüssels s):

$$\begin{aligned} c \oplus s &= (t \oplus s) \oplus s \\ &= t \oplus (s \oplus s) && \text{(Assoziativität)} \\ &= t \oplus 0 && \text{(Selbstinversität: } s \oplus s = 0\text{)} \\ &= t && \text{(Neutrales Element: } t \oplus 0 = t\text{)} \end{aligned}$$

Warum funktioniert die Entschlüsselung?

Sei t der Klartext und s ein zufälliger geheimer Schlüssel.

- **Verschlüsselung**: $c = t \oplus s$
- **Entschlüsselung** (erneute Anwendung desselben Schlüssels s):

$$\begin{aligned} c \oplus s &= (t \oplus s) \oplus s \\ &= t \oplus (s \oplus s) && \text{(Assoziativität)} \\ &= t \oplus 0 && \text{(Selbstinversität: } s \oplus s = 0\text{)} \\ &= t && \text{(Neutrales Element: } t \oplus 0 = t\text{)} \end{aligned}$$

Die erneute Anwendung des Schlüssels hebt die Verschlüsselung vollständig auf!

Auftrag: Bin-OTP

- Aufgaben 2.18-2.21
- Zeit: 15 Minuten
- Danach: Gemeinsame Besprechung der Lösungen