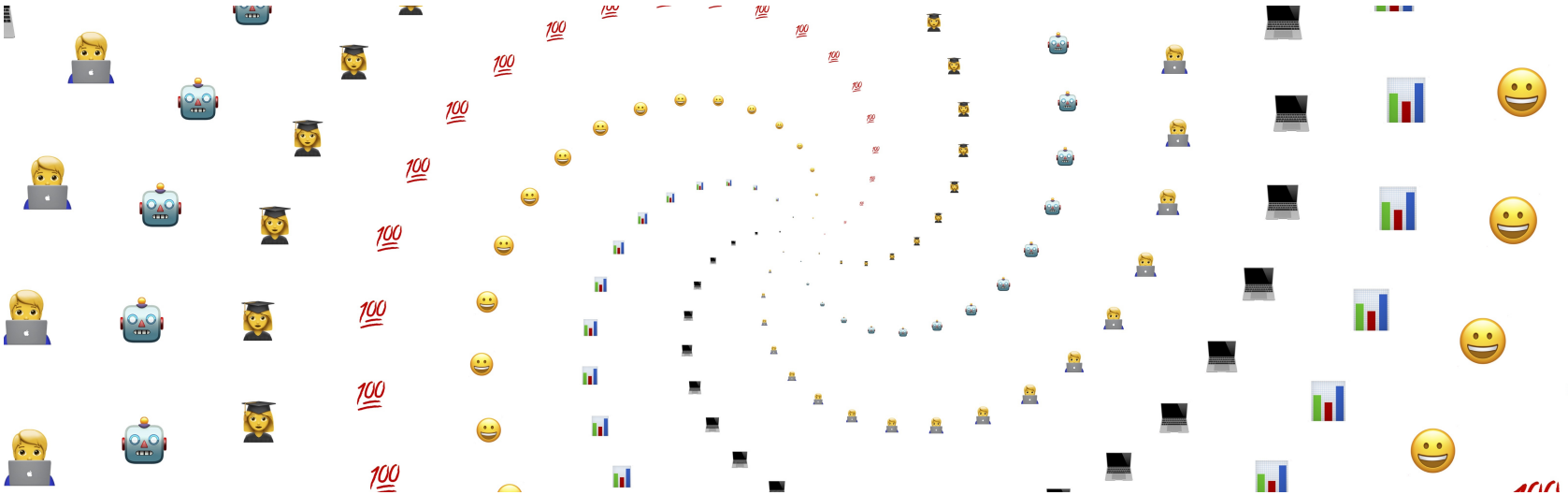
Kryptologie

Fachschaft Informatik
Kantonsschule Im Lee




MiningCave

Zodiac-Killer (Z340 Chiffre)

Die Z340-Chiffre (cypher) wurde 1969 vom Zodiac-Killer verschickt und blieb über 50 Jahre lang ungelöst. Erst 2020 gelang es einem internationalen Team, die komplexe **Transpositions-Substitution-Verschlüsselung** mit Hilfe von Supercomputern zu entschlüsseln.

Enigma

Die Enigma war eine elektromechanische Rotormaschine, die im Zweiten Weltkrieg zur Verschlüsselung des deutschen Nachrichtenverkehrs eingesetzt wurde. Das entschlüsseln der Enigma in Bletchley Park gilt als entscheidender Wendepunkt der modernen **Kryptoanalyse**.

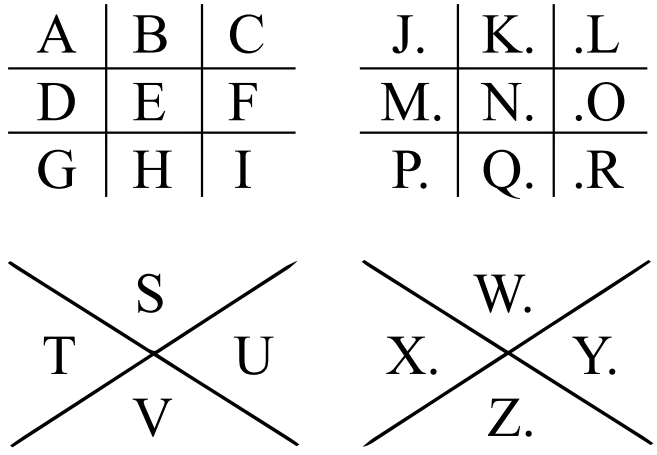
Signal-Protokoll

Moderne Messenger wie *Signal* nutzen eine **Ende-zu-Ende-Verschlüsselung**. Dabei werden Nachrichten direkt auf dem Gerät des Senders verschlüsselt und können nur vom Empfänger gelesen werden — selbst der Dienstanbieter hat keinen Zugriff auf den Klartext.
Der Quellcode ist offengelegt und kann von jedem überprüft werden, was das Vertrauen in die Sicherheit des Protokolls stärkt:
`https://github.com/signalapp`

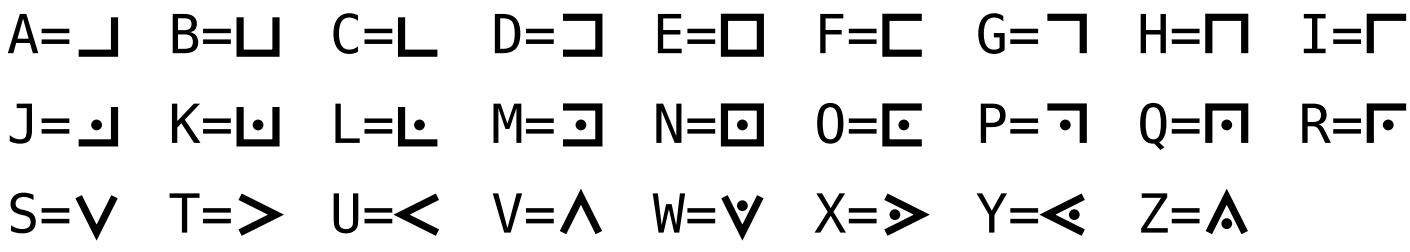
Kryptowährungen & Mining

Die Kryptologie ist das Fundament von Kryptowährungen wie Bitcoin. Hier werden kryptographische **Hash-Funktionen** und digitale Signaturen genutzt, um Transaktionen abzusichern und neue Blöcke in der Blockchain durch „Mining“ zu verifizieren. Ein Mining-Rig wertet kryptographische Hash-Funktionen aus.

Freimaurer-Geheimschrift



(a) Freimaurer-Alphabet



(b) Zuordnung der Symbole zu den lateinischen Grossbuchstaben

Abbildung: Freimaurer-Geheimschrift: Beispiel für ein Verfahren, dessen Sicherheit von der Geheimhaltung des Systems abhängt.

Nennen Sie weitere Beispiele von Geheimschriften.

Schema: Kommunikation mittels Geheimschriften

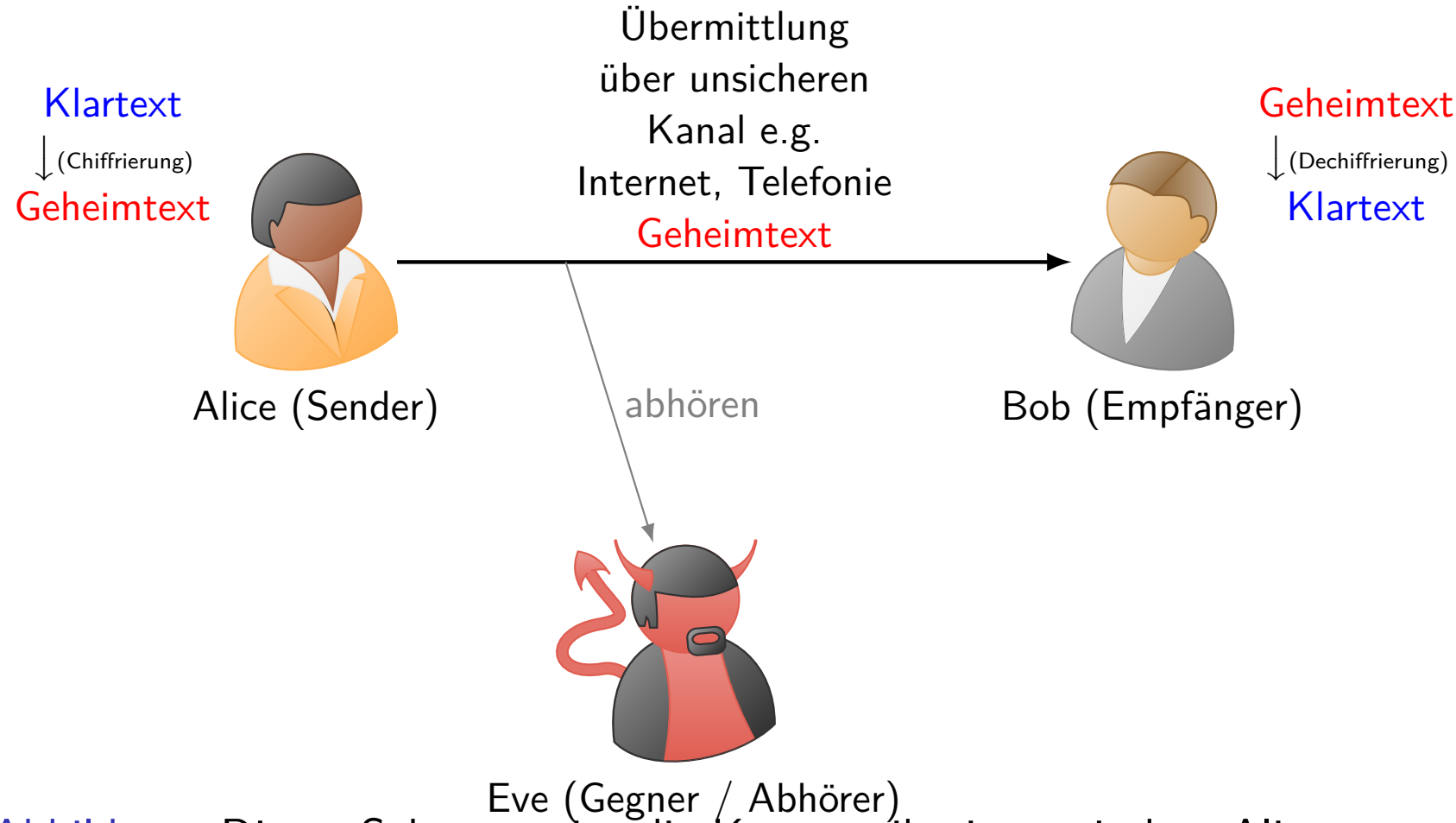


Abbildung: Dieses Schema zeigt die Kommunikation zwischen Alice (Sender) und Bob (Empfänger) unter Verwendung einer Geheimschrift. Der Name *Eve* ist eine clevere Abkürzung für *eavesdropper*, was auf Deutsch so viel wie *Abhörer* bedeutet.

Geheimschriften

Definition (Geheimschrift)

Eine **Geheimschrift** realisiert eine Transformation (*Chiffrierung*) von einem Klartext in einen Geheimtext. Die Umkehrung dieser Transformation (*Dechiffrierung*) ermöglicht es, den Klartext aus dem Geheimtext (typischerweise eindeutig) zu rekonstruieren:

$$\text{Chiffrierung}(\text{Klartext}) = \text{Geheimtext}$$
$$\text{Dechiffrierung}(\text{Geheimtext}) = \text{Klartext}.$$

Beispielsweise:

$$\text{Freimaurer\_Chiffrierung}(\texttt{HALLO}) = \sqcap\!\lrcorner\,\llcorner\cdot\,\llcorner\cdot\,\sqsubset\cdot$$
$$\text{Freimaurer\_Dechiffrierung}(\sqcap\!\lrcorner\,\llcorner\cdot\,\llcorner\cdot\,\sqsubset\cdot) = \texttt{HALLO}.$$

Limitierung von Geheimschriften

Bemerkung (*Security through Obscurity*)

Security through Obscurity (Sicherheit durch Verschleierung) bezeichnet die Praxis, die Sicherheit eines Systems dadurch zu gewährleisten, dass die Funktionsweise des Systems geheim gehalten wird.

Die Praxis der *Security through Obscurity* wird als unsicher angesehen, da sie auf der Annahme beruht, dass Angreifer nicht in der Lage sein werden, die Funktionsweise des Systems zu verstehen oder zu entdecken.

Kennen Sie Sicherheitsvorkehrungen, von denen wir alle genau wissen, wie sie funktionieren, die aber dennoch als sicher gelten?

Kennen Sie Sicherheitsvorkehrungen, von denen wir alle genau wissen, wie sie funktionieren, die aber dennoch als sicher gelten?

Tipp: Was tun Sie normalerweise, wenn Sie die Wohnung als letzte Person verlassen?

Von Geheimschriften zu Kryptosystemen

Idee (Kryptosystem)

Wir wollen von Geheimschriften zu sogenannten **Kryptosystemen** übergehen, die so konstruiert sind, dass sie auch dann sicher sind, wenn die grundlegende Funktionsweise des Systems öffentlich bekannt ist.

Ein solches System kennen Sie bereits aus dem Alltag: Wir wissen alle, wie ein Türschloss grundsätzlich mit einem Schlüssel zu öffnen ist, aber dennoch können wir unsere Türen sicher verschliessen, da die Sicherheit nicht von der Geheimhaltung des Mechanismus abhängt, sondern von der Geheimhaltung (sicheren Aufbewahrung) des Schlüssels.

Kryptosystem *Skytale*

Das Kryptosystem *Skytale* funktioniert wie folgt:

- Schreibe den Klartext zeilenweise in eine Tabelle (Matrix) von links nach rechts.

Abbildung: Praktische Umsetzung der Skytale-Verschlüsselung.

Kryptosystem *Skytale*

Das Kryptosystem *Skytale* funktioniert wie folgt:

- Schreibe den Klartext zeilenweise in eine Tabelle (Matrix) von links nach rechts.
- Allfällige leere Felder in der letzten Zeile der Tabelle werden mit beliebigen (am besten zufällig gewählten) Buchstaben gefüllt.

Abbildung: Praktische Umsetzung der Skytale-Verschlüsselung.

Kryptosystem *Skytale*

Das Kryptosystem *Skytale* funktioniert wie folgt:

- Schreibe den Klartext zeilenweise in eine Tabelle (Matrix) von links nach rechts.
- Allfällige leere Felder in der letzten Zeile der Tabelle werden mit beliebigen (am besten zufällig gewählten) Buchstaben gefüllt.
- Den Kryptotext erhalten wir, indem wir die Buchstaben Spalte für Spalte von links nach rechts und von oben nach unten lesen.

Abbildung: Praktische Umsetzung der Skytale-Verschlüsselung.

Auftrag

- Lösen Sie die Aufgaben 1.1 und 1.2 im Skript
- Zeit: 10 Minuten
- Danach: Besprechung der Aufgaben

Auftrag

- Lösen Sie die Aufgaben 1.3 und 1.4 im Skript
- Zeit: 10 Minuten
- Danach: Besprechung der Aufgaben

Kryptosystem *Caesar*

Eines der bekanntesten Kryptosysteme der Antike ist die Caesar-Verschlüsselung, die von Julius Caesar verwendet wurde.

- Dabei wird jeder Buchstabe des Klartexts um eine feste Anzahl von Positionen im Alphabet verschoben.

Kryptosystem *Caesar*

Eines der bekanntesten Kryptosysteme der Antike ist die Caesar-Verschlüsselung, die von Julius Caesar verwendet wurde.

- Dabei wird jeder Buchstabe des Klartexts um eine feste Anzahl von Positionen im Alphabet verschoben.
- Die Anzahl der Positionen, um die verschoben wird, bildet den Schlüssel des Kryptosystems.

Bemerkung (Buchstaben als Zahlen)

Häufig wird die Verschiebung nicht direkt als Zahl angegeben, sondern als Buchstabe, der die Anzahl der Positionen angibt. So steht beispielsweise der Schlüssel `A` für eine Verschiebung um 0 Positionen (keine Verschiebung), `B` für eine Verschiebung um 1 Position und so weiter:

$$\texttt{A} \leftrightarrow 0 \text{ Positionen}, \texttt{B} \leftrightarrow 1 \text{ Position}, \texttt{C} \leftrightarrow 2 \text{ Positionen}, \ldots,$$
$$\texttt{Z} \leftrightarrow 25 \text{ Positionen}.$$

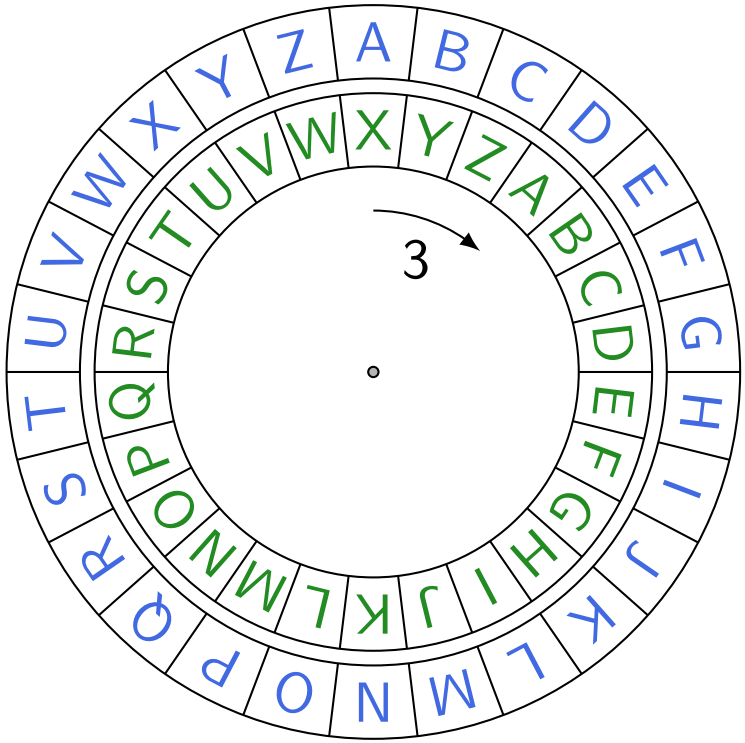
Definition (Ordnung eines Buchstabens)

Die **Ordnung** eines Buchstabens ist die Anzahl der Positionen, die dieser Buchstabe im Alphabet von `A` entfernt ist. Wir definieren

$$\mathrm{Ord}(\texttt{A}) = 0,\ \mathrm{Ord}(\texttt{B}) = 1,\ \mathrm{Ord}(\texttt{C}) = 2,\ \ldots,\ \mathrm{Ord}(\texttt{Z}) = 25.$$

Caesar mit Schlüssel `D`

Mit dem Schlüssel `D` (3 Positionen, da Ord(`D`) = 3) wird aus dem Klartext `HALLO` der Kryptotext `KDOOR`.
Dabei haben wir die innere Scheibe um 3 Positionen im Uhrzeigersinn gedreht, um die Verschlüsselung („lesen von innen nach aussen“) durchzuführen.
Zur Entschlüsselung lesen wir von „aussen nach innen“.



Hier finden Sie ein interaktives Werkzeug, um die Caesar-Verschlüsselung und -Entschlüsselung durchzuführen.

Die Entschlüsselung (bei Schlüssel 3) kann auch erfolgen, indem man die innere in die Ausgangsposition zurückdreht und dann nochmals um 3 Positionen gegen den Uhrzeigersinn dreht (dies können wir um eine Verschiebung um -3 Positionen anschauen). Mit diesem Vorgehen können wir die Drehscheiben wieder von „innen nach aussen“ lesen, um den Klartext zu erhalten.

Auftrag

- Lösen Sie die Aufgabe 1.5 im Skript
- Zeit: 5 Minuten

Schema: Kommunikation mittels Kryptosystemen

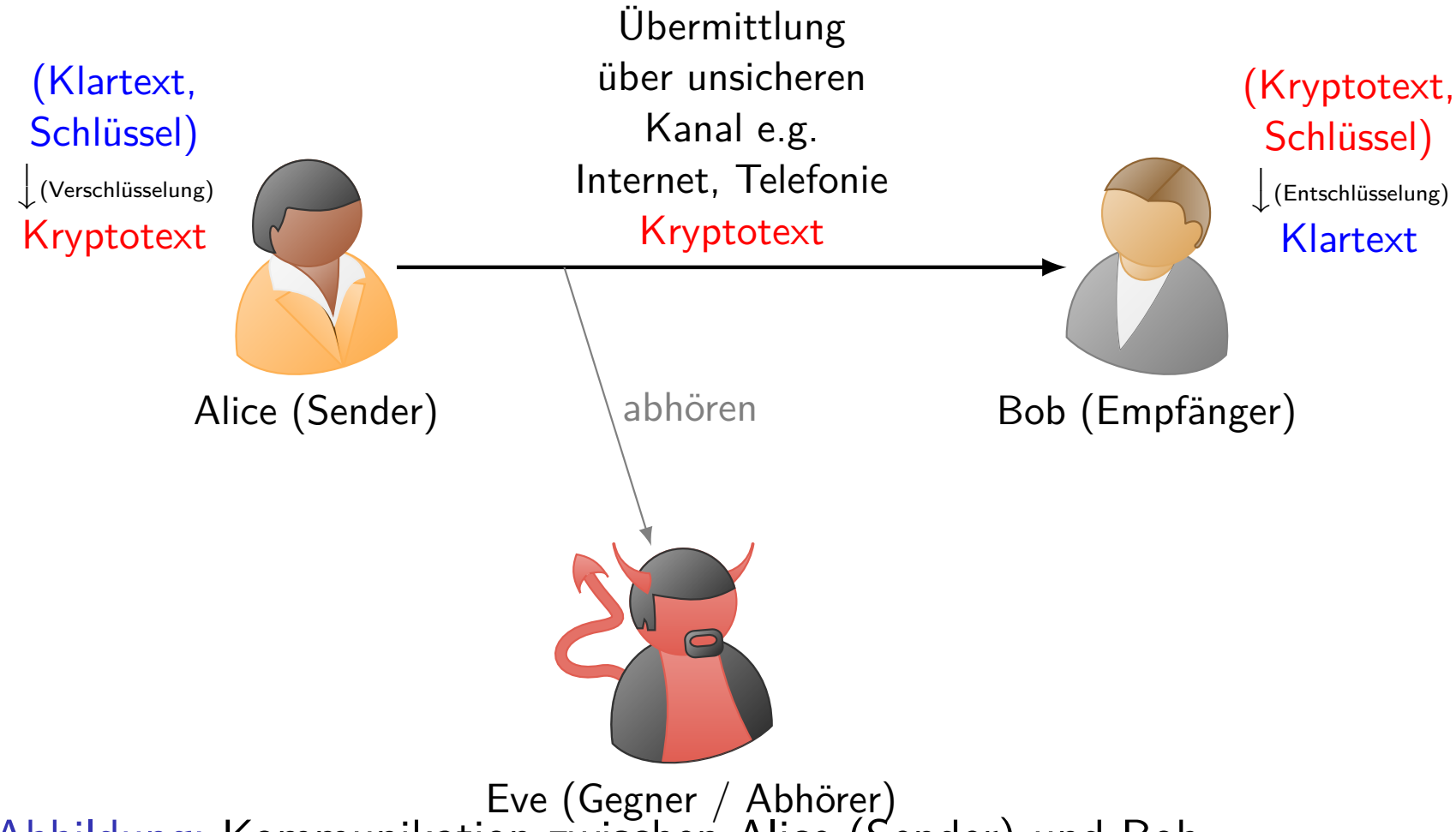


Abbildung: Kommunikation zwischen Alice (Sender) und Bob (Empfänger) unter Verwendung eines Kryptosystems. Bob benötigt den Schlüssel, um den Kryptotext zu entschlüsseln.

Definition (Kryptosystem)

Ein **Kryptosystem** realisiert eine Transformation (*Verschlüsselung*) von einem Klartext in einen Kryptotext, die von einem Schlüssel abhängt. Die Menge aller möglichen Schlüssel wird *Schlüsselmenge* des Kryptosystems genannt. Die Umkehrung dieser Transformation (*Entschlüsselung*) ermöglicht es, den Klartext aus dem Kryptotext zu rekonstruieren, wenn man den Schlüssel kennt:

$$\text{Verschlüsselung}(\text{Klartext}, \text{Schlüssel}) = \text{Kryptotext}$$
$$\text{Entschlüsselung}(\text{Kryptotext}, \text{Schlüssel}) = \text{Klartext}.$$

Beispielsweise (mit Caesar):

$$\text{Caesar\_Verschlüsselung}(\texttt{HALLO}, 3) = \texttt{KDOOR}$$
$$\text{Caesar\_Entschlüsselung}(\texttt{KDOOR}, 3) = \texttt{HALLO}.$$

Schlüsselmenge bei Caesar: $\{0, 1, \ldots, 25\}$.

Bemerkung (Geheimschrift als Spezialfall eines Kryptosystems)

Eine Geheimschrift ist ein Spezialfall eines Kryptosystems, bei dem die Schlüsselmenge nur ein einziges Element enthält, nämlich die Anweisung, wie die Buchstaben vertauscht werden. Umgekehrt, kann ein Kryptosystem als eine Sammlung von Geheimschriften betrachtet werden, wobei für jede mögliche Schlüssel eine Geheimschrift definiert ist, die die Buchstaben entsprechend der Verschlüsselungsregel vertauscht.

Kerckhoffs'sches Prinzip

Der niederländische Kryptologe und Linguist *Auguste Kerckhoffs* stellte im Jahr 1883 die folgende Anforderung an die Sicherheit von Kryptosystemen auf, die heute als **Kerckhoffs'sches Prinzip** bekannt ist:

Zitat

„Ein Kryptosystem sollte auch dann sicher sein, wenn alles über das System bekannt ist, ausser dem Schlüssel." – Auguste Kerckhoffs, *La cryptographie militaire* (1883)[a]

[a] Originalzitat: „Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi."

Auftrag

- Studieren Sie den Abschnitt 1.6 im Skript.
- Lösen Sie die Aufgaben 1.6, 1.7 und 1.8 im Skript
- Zeit: 15 Minuten

alle monoalphabetischen Substitutionen (Permutationen)

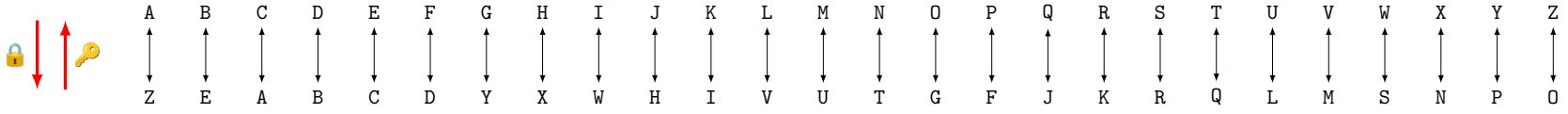


Abbildung: Monoalphabetische Substitution

Auftrag

- Studieren Sie den Abschnitt 1.6 im Skript.
- Lösen Sie die Aufgabe 1.9 im Skript
- Studieren Sie das Beispiel 1.4 im Skript.
- Zeit: 10 Minuten