Kryptographie – eine erste Übersicht

KGV bedeutet: Details erfahren Sie in der **K**rypto**g**raphie-**V**orlesung.

Abgrenzung

Steganographie:
Das **Kommunikationsmedium** wird **verborgen**.

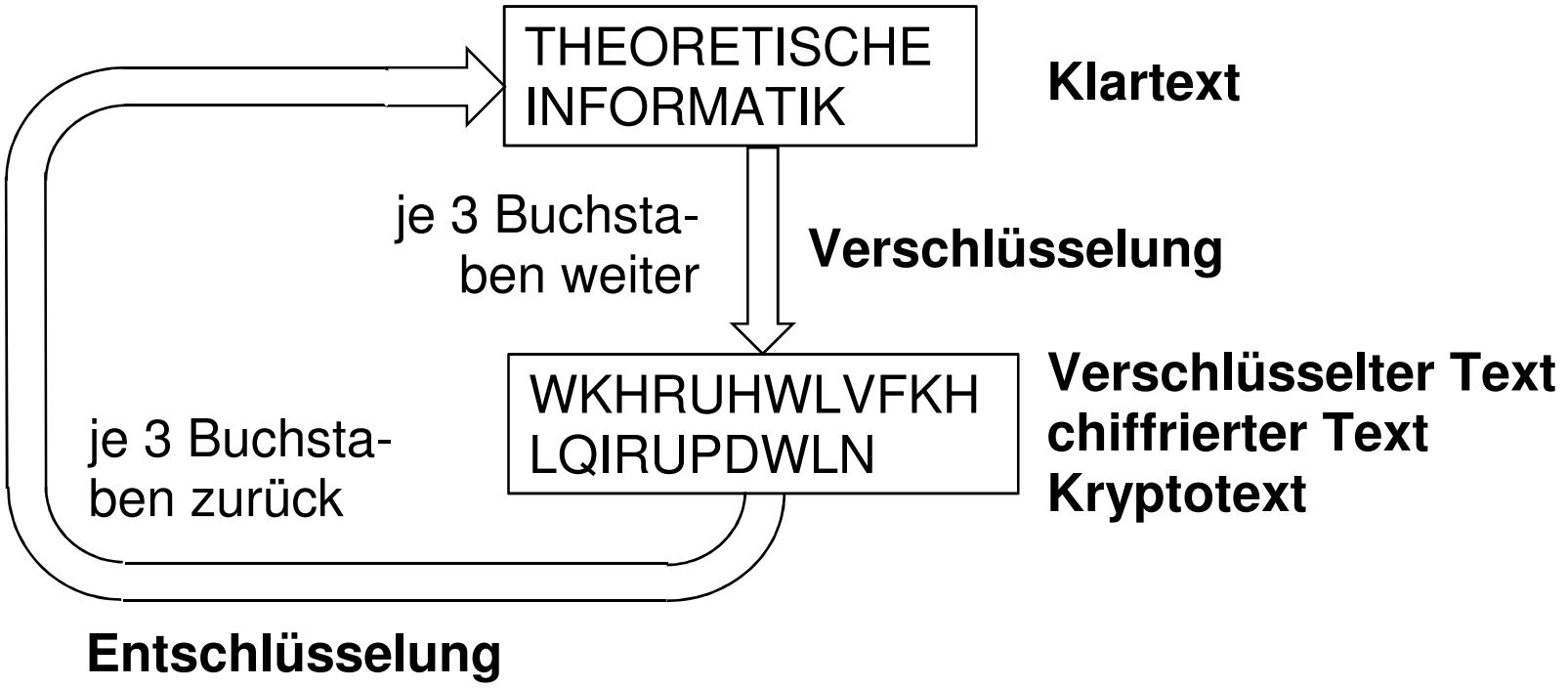
Klassische Beispiele:

- Ein Bote wird kahl geschoren, seine Kopfhaut haltbar beschriftet. Er wird nach dem Nachwachsen der Haare als harmloser Reisender losgeschickt.
- Eine Kapsel mit einem beschrifteten Zettel darin wird verschluckt.
- Ein Mikrofilm wird in einem harmlosen Brief als Satzpunkt getarnt oder unter die Briefmarke geklebt.

Kryptographie:
Die Nachricht wird für den Transport bis zur Unkenntlichkeit verändert und vom Empfänger wieder rekonstruiert. Die Übermittlung ist nicht unbedingt geheim.

Grundbegriffe am Beispiel

Beispiel: Caesars Methode



Verschlüsselungsmethode: Um *n* Buchstaben verschieben
Schlüssel: *n* = 3

Gefahren am Caesar-Beispiel

Verschlüsselungsmethoden (Chiffren) sprechen sich herum und lassen sich evtl. der Reihe nach durchprobieren.

Dann bietet nur eine Vielzahl von wählbaren Schlüsseln mehr Sicherheit – hier mit 26 zu wenige.

Prinzip von Auguste Kerckhoffs.

Blaise **de Vigenère** verbesserte die Caesar-Methode, indem er nicht immer die gleiche Verschiebung *n* anwendete, sondern anstelle von *n*, *n*, *n*, … ein Muster, z.B. 7, 5, 8, 5, 14, das – so oft wiederholt wie notwendig – zeichenweise addiert wird: erster Buchstabe +7, zweiter + 5 usw. Gerne verwendete man Muster, die einem Wort entsprachen (oben: GEHEIM)

Auch diese Methode ist angreifbar: KGV

Was aber, wenn man das Muster mindestens so lang macht wie alle Botschaften zusammen und das Muster gerade NICHT etwas Sinnvollem entspricht?

Sichere Kryptografie

… gibt es, auch im Caesar-Stil: **One-Time-Pads**

Nicht um **feste** Zahl von Buchstaben verschieben, sondern:

- Sender und Empfänger vereinbaren eine danach geheim gehaltene lange **Zufallsfolge** von Zahlen aus 1-26.
- Zum Verschlüsseln **addiert** der Sender die **erste** Zahl zum **ersten** Buchstaben, die zweite zum zweiten usw.
- Entsprechend **subtrahiert** der Empfänger zum Entschlüsseln.

Dann kann WKHRUHWLVFKHLQIRUPDWLN für Unbefugte mit gleicher Wahrscheinlichkeit

- THEORETISCHEINFORMATIK,
- ZEICHNUNGSBERECHTIGTER oder
- HACKERHABENNULLCHANCEN

usw. bedeuten. Der Kryptotext liefert praktisch **keine Hinweise** auf den Klartext.

Leider sind Erzeugung und sichere Weitergabe der OTP's **aufwändig**.

Begriffe

Kryptologie: Kryptographie + Kryptoanalyse

Kryptographie: möglichst so gut verschlüsseln,
dass Unbefugte dem Klartext nicht erfahren

Kryptoanalyse: möglichst trotzdem entschlüsseln

Stärke der Verschlüsselung:
Zeit und Aufwand, die man zur Entschlüsselung benötigt.

Schlüssel

... erzeugen Instanzen von Ver- und Entschlüsselungsmethoden

Symmetrische oder **Geheim-Schlüssel** werden identisch für Ver- und Entschlüsselung benutzt, so wie die 3 beim Caesar-Beispiel.

Problem bei der konventionellen symmetrischen Verschlüsselung:
Schlüsselverteilung:

- Wie gelangt der Schlüssel sicher zum Empfänger?

Bei **Schlüsselpaaren** aus einem **privaten** und einem **öffentlichen** Schlüssel K(Ben.,priv), K(Ben.,öff), hat der Benutzer einen privaten Schlüssel, und seinen öffentlichen Schlüssel **gibt** er einfach **bekannt** → (fast) kein Verteilungsproblem. (außer ... KGV)

Asymmetrische Kryptographie
Englisch: **Public Key Cryptography**

Public Key Cryptography, Details (1)

- Was mit dem einen Schlüssel verschlüsselt wird, kann mit dem anderen (und praktisch nur damit) entschlüsselt werden.
- Es muss praktisch **unmöglich** sein, aus dem öffentlichen Schlüssel den privaten **herzuleiten** oder umgekehrt.

Anwendungen

Bob und Charlie können mit Alices öffentlichem Schlüssel K(Alice,öff) ihre Nachrichten an Alice verschlüsseln. Dann kann nur Alice diese verschlüsselten Texte entschlüsseln und lesen. (**Vertraulichkeit**, **Geheimhaltung**)

Alice kann Texte aber auch mit ihrem privaten Schlüssel K(Alice,priv) verschlüsseln. Dann können Bob wie Charlie diese verschlüsselten Texte entschlüsseln und haben die Garantie, dass sie von Alice kommen.
(**Authentifizierung, Signaturverfahren**)

Public Key Cryptography, Details (2)

Vorteil: Das Übertragen von geheimen Schlüsseln zwischen Absender und Empfänger über einen sicheren Kanal entfällt.

Trotzdem: Problem(beispiel): Stammt der bei mir angekommene öffentliche Schlüssel tatsächlich von seinem angeblichen Urheber?

Beispiele für **Verschlüsselungssysteme mit öffentlichen Schlüsseln**

- Elgamal (nach dem Erfinder Taher Elgamal),
- RSA (nach den Erfindern Ron Rivest, Adi Shamir und Leonard Adleman),
- Diffie-Hellman (Martin Hellman, Whitfield Diffie und Ralph Merkle) und
- DAS, der Digital Signature Algorithm (von David Kravitz).

KGV

Mathematische Beiträge

Die Sicherheit der meisten asymmetrischen Kryptosysteme beruht auf der Schwierigkeit von Problemen, die in der algorithmischen Zahlentheorie untersucht werden.

Die bekanntesten dieser Probleme sind die Primfaktorzerlegung und das Finden diskreter Logarithmen.

KGV

Tipp: **Eigenstudium des RSA-Verfahrens**, z.B. anhand

1. B. Baumgarten: Kompendium der diskreten Mathematik
   Kap. ***Zahlentheorie***
2. https://de.wikipedia.org/wiki/***RSA-Kryptosystem***

Anwendungsfelder

- Wirtschaft
- Handel
- Verwaltung
- Recht
- Militär
- privater Datenschutz