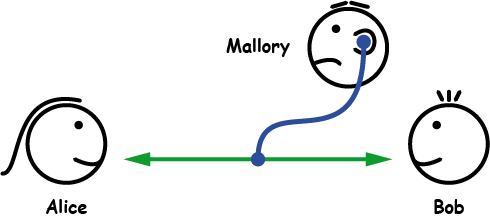
Verschlüsselung

Alice möchte eine Nachricht an Bob senden bzw. die beiden wollen miteinander Daten austauschen. Leider haben sie dafür ein nicht abhörsicheres (von Mallory abhörbares) Netz zur Verfügung.

Alice, Bob, Mallory sind die Hauptprotagonisten im der gängigen Kryptographie Literatur.

Ziel einer Verschlüsselung ist es also, die zu übertragenden Nachrichten zu „verändern“, sodass Mallory nicht mehr in der Lage ist die ursprüngliche Nachricht zu rekonstruieren (oder nur mit sehr viel Aufwand).



Terminologie

**Kryptographie:** Die Lehre der Absicherung von Nachrichten durch Verschlüsselung

**Kryptoanalyse:** Die Kunst, Chiffretext aufzubrechen, d.h. den Klartext zu reproduzieren, ohne Kenntnis des Schlüssels

**Kryptologie:** Vereinigt Kryptographie und Kryptoanalyse

**Steganographie:** Geheime Nachrichten werden NICHT verschlüsselt sondern versteckt. Z.B.: in Musik- oder Bilddateien

**Alphabet:** A ist eine endliche Menge von Zeichen. N = |A| ist die Mächtigkeit des Alphabets

**Klartext:** (plaintext): M … lesbarer Teil einer Nachricht. Bezeichnet eine Zeichenkette über dem Alphabet (A)

An = {a,b,c}

M = aabcc, abcabca

**Geheimtext** (Chiffretext): C … verschlüsselte Nachricht. Bezeichnet Zeichenkette ebenfalls über Alphabet (A) oder über einem anderen Alphabet.

**Schlüssel:** K … Zeichenkette zum Verschlüsseln

**Verschlüsselung** (Chiffrierung): Verfahren um eine Nachricht (M) unverständlich zu machen

**Chiffre** (encryption): E … ist eine invertierbare Funktion, d.h. eine umkehrbare Abbildung, welche aus Klartext *M* und einen Schlüssel *K* den Geheimtext *C* macht.

**Entschlüsselung** (decryption): D … Umkehrung von E zur Wiederherstellung des Klartextes M

E(M) = C D(C) = M

Praktisch alle Verschlüsselungsverfahren haben die Aufgabe eine/mehrere der folgenden 4 Eigenschaften einer Nachricht zu gewährleisten.

**Geheimhaltung:** Ziel der Geheimhaltung ist es, das Lesen einer Nachricht für Unbefugte unmöglich ist.

**Authentifizierung/Authentikation:** Identitätsbeweis des Senders einer Nachricht gegenüber dem Empfänger, d.h. der Empfänger kann sicher sein, dass die Nachricht nicht von einem anderen (unbefugten) Absender stammt.

**Integrität:** … die Nachricht darf während der Übertragung nicht (von Unbefugten) verändert werden. Sie bewahrt ihre Integrität, das heißt Unverletzbarkeit.

**Verbindlichkeit:** … der Sender kann später nicht leugnen, eine Nachricht abgeschickt zu haben.

## Verschlüsselung

Verschlüsselung erfolgt mit Hilfe von kryptographischen Algorithmen, welche auf die Nachricht angewendet werden. Ein kryptographischer Algorithmus ist eine Berechnungsvorschrift (mathematische Funktion) zur Ver- und Entschlüsselung.

### Injektive Ableitung

A

B

C

D

W

X

Z

A

B

C

D

W

X

Z

Y

Früher wurden eingeschränkte Algorithmen verwendet. Hier bestand die Sicherheit darin, dass die Arbeitsweise des Algorithmus geheim gehalten wurde.

Dies hat folgende gravierende Nachteile:

* Verlässt eine Person, die den Algorithmus kennt die Firma, dann muss der Algorithmus geändert werden.
* Auch wenn der Quellcode des Algorithmus nicht öffentlich ist, kann mithilfe des Maschinencodes der Algorithmus rekonstruiert werden.
* Weitergabe des Algorithmus an Dritte daher nicht möglich 🡪 Algorithmus sinnlos.
* Keine Qualitätskontrolle des Algorithmus. Software muss nicht der Kritik und den Angriffen der Öffentlichkeit standhalten.

Heute werden ausschließlich Algorithmus mit Schlüssel verwendet. Schlüssel ist meist eine natürliche Zahl, dargestellt im Binärsystem d.h. als Folge von Bits.

Algorithmus ist bekannt und veröffentlicht.

Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssels abhängen, nicht jedoch von der Geheimhaltung des Algorithmus.

**Symmetrische Algorithmen:** Zum Chiffrieren und Dechiffrieren wird immer der gleiche Schlüssel ***K*** verwendet.

**Problem:** Bevor Bob den Schlüssel K zum dechiffrieren verwenden kann muss der Schlüssel übertragen werden! Übertragung des Schlüssels ist unsicher. Kann von Mallory abgehört werden.

Früher Aufwand für Schlüsselübertragung oftmals nicht gerechtfertigt. Wurde vor allem im militärischen Bereich verwendet. Z.B.: U-Boot im 2. Weltkrieg

Heutzutage erfolgt Schlüsselaustausch durch:

* Diffie-Hellman-Schlüsseltausch
* Asymmetrische Verschlüsselung der zu verwendeten Schlüssel

### Asymmetrische Algorithmen

Schlüssel K1 wird zum Chiffrieren und Schlüssel K2 zum Dechiffrieren verwendet.

### Public Key Algorithmen

Möchte Alice an Bob eine Nachricht versenden, erstellt sie 2 Schlüssel:

KP … Public Key (öffentlicher Schlüssel): diesen lässt sie allen Kommunikationspartnern zukommen

KS … Secret Key (geheimer Schlüssel): diesen bewahrt Alice gut auf und gibt ihn an niemanden weiter

Bob verschlüsselt seine Nachricht mit KP und sendet diese Nachricht an Alice.

Prinzip entspricht Schloss vieler Wohnungstüren. Jeder kann die Türen schließen. Aber nur der Besitzer kann sie wieder öffnen.

Beispiel: PGP (Pretty Good Privacy)

### Stromchiffren

Bei Stromchiffren wird Byte für Byte die Nachricht verschlüsselt.

### Blockchiffren

Blockchiffren fassen immer eine Bestimmte Anzahl an Bytes zu einem Block zusammen und verschlüsseln anschließend diesen.

### Sicherheit von Schlüsseln …

… hängt immer von der Schlüssellänge ab.

#### Beispiel:

Brute Force Methode kann pro Sekunde 10 Schlüssel ausprobieren.

**Frage**: Wie lange dauert es um einen Schlüssel mit 8 Bit Länge zu knacken?

Wie lange bei einem Schlüssel von 32 Bit?

## Klassische Chiffren

* Bezeichnen klassische Chiffren welche bis etwa 1950 entwickelt und verwendet worden wurden.
* Verwenden mathematische Methoden auf einem endlichen Alphabet.

**Transpositionschiffre:** Geheimtext wird durch Permutation der Klartextzeichen erzeugt. Zeichen bleiben gleich, tauschen aber ihre Plätze.

**Substitutionschiffre:** Jedes Zeichen des Klartextes wird durch ein anderes Zeichen ersetzt. Position bleibt jedoch gleich.

* Heißen **monoalphabethisch**, wenn jedes Klartextzeichen immer auf das gleiche Geheimtextzeichen abgebildet wird.
* Heißen **polyalphabethisch** wenn sie nicht monoalphabethisch sind

**Frage:** Wie viele verschiedene Schlüssel für monoalphabethische Chiffren gibt es über unserem Alphabet [A-Z].

**Antwort:** 26! ≈ 4 \* 1026 ≈ 88 Bit

Selbst mit heutigen Computern und deren Rechenleistung ist es praktisch unmöglich alle Schlüssel durchzuprobieren. Trotzdem sind monoalphabetische Chiffren sehr unsicher und können mit Hilfe statistischer Methoden leicht geknackt werden.

### Verschiebechiffre

Hierbei wird jedes Klartextzeichen *z* durch ein um *k* Zeichen im Alphabet verschobenes Zeichen ersetzt. Hat ein Alphabet *n* Zeichen, so werden diese von *0* bis *n-1* durchnummeriert.

Folgende Regel gilt für die Verschlüsselung: **z 🡪 (z+k) mod n**

*„Julius Caesar hat seine Nachrichten mit der nach ihm benannten Chiffre verschlüsselt und dabei meist den Schlüssel* ***C*** *verwendet. D.h. die Zeichen um 3 Positionen verschoben“*

**Frage:** Wie viele Schlüssel besitzt der Verschiebechiffre über dem Alphabet [A-Z]?