Einführung in die Kryptographie

- Aufbau
  - Begriffsklärung
  - Geschichte
  - Kerckhoffs Prinzip
  - Digitale Kryptographie
    - Symmetrische und asymmetrische Verfahren, Hash-Funktionen,
  - Beispiele der praktischen Anwendung

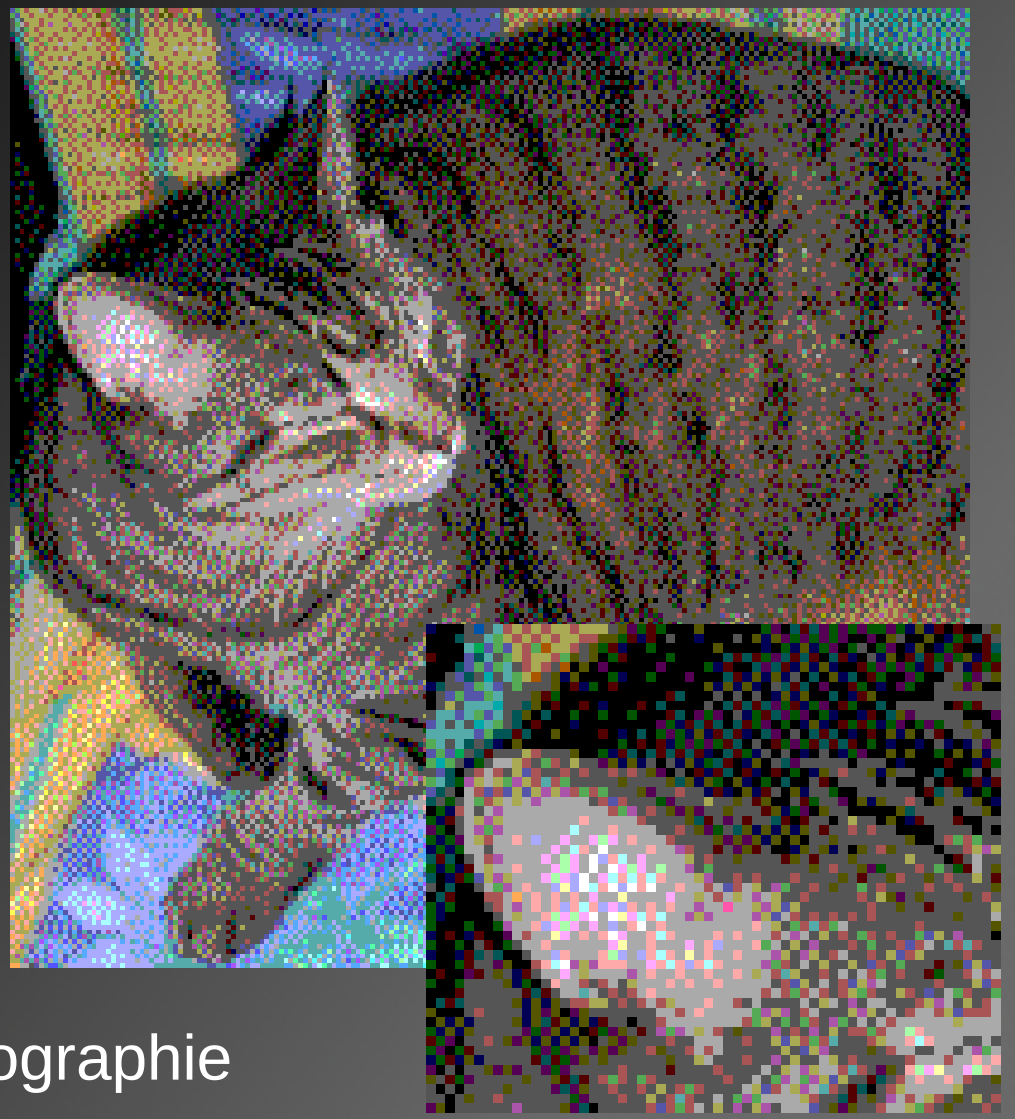
Begriffsklärung

- Aus dem altgriechischen:
  - geheim, verborgen
- Verhindert, dass eine dritte Person die Bedeutung der Information erfassen kann
- Zusammen mit der Kryptoanalyse bildet sie die Kryptologie
- Kryptoanalyse: Bedeutung eines Chiffres herausfinden ohne den Schlüssel zu kennen

Begriffsklärung

- Steganographie
  - Verbergen des Kanals über den kommuniziert wird.
  - Verstecken von geheimen Nachrichten in scheinbar unwichtigen Informationen.
  - Spezialfall: Digitale Wasserzeichen

Steganographie



Quelle: Wikipedia; Artikel: Steganographie

Geschichte

- Atbasch
- Ceasar-Chiffre

```
Alphabet: a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheim:   D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

  - Von Ceasar verwendet worden um mit seinen Streitkräften kommunizieren zu können.

Kerckhoffs Prinzip

- Erstmals definiert im Jahr 1883 in einem Militärhandbuch
- Sicherheit basiert auf dem Schlüssel, nicht auf die Geheimhaltung des Verfahrens
- Offenheit des Verfahrens
- Weitere Eigenschaften
  - Transportabel
  - Nicht mehr als eine Person zur Anwendung erforderlich
  - Mit telegraphischer Kommunikation kompatibel
- Gegenteil von „Security by Obscurity“

Hash-Algorithmen

- Kompressionsfunktion mit fixer Ausgabelänge
- Prüfsumme mit weiteren kryptographischen Eigenschaften
- Einwegfunktion, Diffusion
- Anwendungen:
  - Speichern von Passwörtern
  - Integrität von Informationen sicherstellen

```
echo "Klarmachen zum ändern." |md5sum
096449a978f8adf3307fb3d003857bb4

echo "Klarmachen zum ändern?" |md5sum
42caca1dc829a670eb9c67ed7b7ca763
```

Symmetrische Kryptographie

- Meistens Blockchiffren
  - Aufteilen der Nachricht in Blöcke gleicher Größe, Verknüpfung der Blöcke mit dem Schlüssel
- Lucifer (IBM) erste zivil nutzbare Blockchiffre (1971)
- Verwendung:
  - Festplatten und Dateien verschlüsseln
  - Internetprotokolle (SSL)

Asymmetrische Kryptographie

- Public-Key-Verschlüsselung
  - Verschlüsseln von Informationen mit einem öffentlichen Schlüssel, entschlüsseln nur mit einem privaten Schlüssel möglich.
- Auch für Signaturen geeignet
- Verwendung von Falltürfunktionen
- Bekannte Verfahren: RSA, Diffie-Hellman

Beispiele der praktischen Anwendung

- Verschlüsseln von Daten/Datenträgern
  - Festplatten: Truecrypt/Luks
  - Dateien: in vielen Komprimierungstools als Schutzfunktion integriert (7-Zip, WinRAR, etc...)
- Verschlüsseln von Kommunikation über Netzwerke/Internet
  - Email: PGP/OpenGPG als Plugin für viele Mail-Programme verfügbar (Enigmail für Thunderbird)
  - https

Fragen?