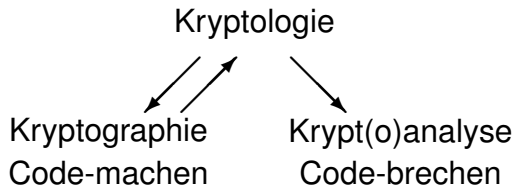


Kapitel 1: Einleitung

Beispiel für den Einsatz von Kryptosystemen:

Schutz der “Luftschnittstelle bei GSM-Handys” (→ Tafel)

Was ist „Kryptographie“?



krýptein = verbergen (aus dem Griechischen)

Für uns: Kryptographie = Kryptologie

Verwandte Gebiete: Steganographie
Computersicherheit

Geschichte

Seit der Antike: Verbreiteter, aber unsystematischer Einsatz kryptographischer Methoden (z.B. durch Caesar).

Ende 19. Jhdt.: Systematisierung und Formalisierung.

2. Weltkrieg: Polen, Briten und Amerikaner „knacken“ sehr starke deutsche Chiffren (u.a. „Enigma“). Erstmals Einsatz von Rechenmaschinen zum „Code-Knacken“.

70er Jahre: Data Encryption Standard (DES).
Public-Key Kryptographie.

80er Jahre: Zero-Knowledge Protokolle.

Seitdem: Massenhafte Verbreitung der Kryptographie (Geldautomaten, Internet, Mobilfunk, Pay-TV, Signaturgesetz ...).

Geschichte (2)

- ▶ Die klassische Kryptographie diente der Geheimhaltung von Nachrichten und wurde hauptsächlich von Militärs, Geheimdienstlern und Diplomaten genutzt.
- ▶ Die moderne Kryptographie (etwa seit 1975) beschäftigt sich mit erheblich weitergehenden Kommunikations- und Sicherheitsproblemen:
 - ▶ *“Cryptography is about communication in the presence of adversaries.”* (Ron Rivest)
 - ▶ *„Die Kryptographie beschäftigt sich mit Kommunikationsproblemen in der Anwesenheit von Gegnern.“*

Ziele beim Einsatz von Kryptographie:

- ▶ Die **Geheimhaltung** von Daten ("**Vertraulichkeit**")
(→ klassische Kryptographie)
(„*Nur wir können diesen Text lesen.*“)
- ▶ Die **Authentizität und Integrität** von Daten
(„*Du hast diesen Brief geschrieben, und niemand hat am Text etwas geändert.*“)
- ▶ Die **Authentizität** von Kommunikationspartnern
(„*Ach, Du bist es!*“)
- ▶ **Anonyme** Kommunikation
(elektronisches Geld, ...).

Kryptosysteme und ihre Anwendung

