Kryptographie

Vorlesung im Wintersemester 2018/19

gehalten von Claus Diem

Organisatorisches

Die Veranstaltung sollte über “Aktuelle Trends der Informatik” abgerechnet werden.

Die Prüfung ist schriftlich.

§0 Einführende Worte

Einige Begriffe

Kryptographie. Klassische Bedeutung (bis ca. 1970):

Methoden der Geheimschrift

Der Sender verschlüsselt Nachrichten, der Empfänger entschlüsselt sie mittels eines zuvor vereinbarten Geheimnisses (= Schlüssel).

$$\text{Klartext} \overset{\text{Verschlüsselung}}{\longrightarrow} \text{Chiffriertext} \overset{\text{Entschlüsselug}}{\longrightarrow} \text{Klartext}$$

Kryptoanalyse (seit ca. 1918). "Ohne Schlüssel entschlüsseln"

chiffrieren: verschlüsseln

dechiffrieren: entschlüsseln (normalerweise mit Schlüssel)

Wort für "ohne Schlüssel entschlüsseln"?

Englisch: to cryptanalyse

vielleicht: "kryptoanalysieren"?

Einige Begriffe

Kryptographie + Kryptoanalyse = Kryptologie

"Moderner" Gesichtspunkt: Angriffe werden gleich mitgedacht.

Dann: Kryptographie = Kryptologie

Definitionsversuch von "Kryptographie" nach heutiger Verwendung:

> *Kryptographie ist die Benutzung und das Studium von Techniken für alle sicherheitsrelevanten Aspekte des Verarbeitens, Übertragens und Benutzens von Informationen in Anwesenheit eines Gegners.*

(vergleiche englischsprachige Wikipedia)

Was bedeutet “Kryptographie”?

Ziele heute

- Vertraulichkeit (Verschlüsseln)
- Authentisierung (Ausweisen)
- Verbindlichkeit (Signieren)
- Integrität (Signieren)

Klassische Ideen

Zwei Personen wollen verschlüsselt Nachrichten austauschen.

1. Ansatz

Veränderung auf Buchstabenebene

- Substitution (ersetze einen Buchstaben durch einen anderen)
- Transposition (verändere die Reihenfolge)

2. Ansatz

Benutzung eines Codebuch

Angriffe mittels statistischer Analyse.

In beiden Fällen:

Es gibt ein Verfahren und einen Schlüssel.

Klassische Ideen

Auf Buchstabenniveau ...

Substitution

CLAUS $\rightarrow \circ\Delta * \backslash\bigcirc$

Transposition

CLAUS $\rightarrow$ ALSUC

Zur Substitution

- "Magische Symbole" sind unsinnig
- Benutze Substitutionstabelle(n)
- Spezialfall: rechts- /links-Shift ("Caesar")
- Substitutionstabelle = Alphabet

Zur Transposition

Beispiel:

Schreibe Text in einem Quadrat von oben nach unten, lies von links nach rechts aus.

Idealtypische Entwicklung

1. V. Verwendung eines einfaches Substitutionsverfahren
2. A. Häufigkeitsanalyse
3. V. Verwendung von mehr Zeichen, Aufteilung nach Wahrscheinlichkeit
4. A. Verwendung von Bigrammen
5. V. Verwendung von Transpositionen
6. A. Vielleicht: Verwendung von bekannten Textteilen / selbst gewählten Texten (der Angreifer jubelt sie dem Verteidiger unter, dieser verschlüsselt sie)

Literatur

C.D. Kryptologie - Methoden, Anwendungen und Herausforderungen