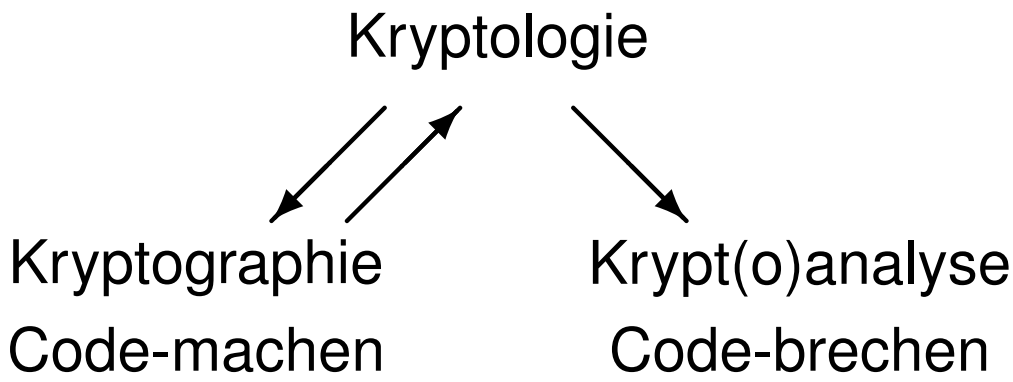
Kapitel 2: Grundlagen der Kryptographie

2: Grundlagen der Kryptographie



krýptein = verbergen (aus dem Griechischen)

Für uns: Kryptographie = Kryptologie

Geschichte (1/2)

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"). Erstmalig Einsatz von Rechenmaschinen zum "Code-Knacken".

Geschichte (2/2)

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

80er Jahre
Zero-Knowledge Protokolle.

Seitdem
Massenhafte Verbreitung der Kryptographie

Moderne Kryptographie

- Klassisch: Militär, Geheimdienste, Diplomaten, ...
- Modern (etwa seit 1975): Jedermann!
  "Cryptography is about communication in the presence of adversaries." (Ron Rivest)

Entitäten

In der Kryptographie gibt es die folgenden Entitäten.

Alice	Sender
Bob	Empfänger
Eve	passiver Angreifer; *eavesdropping*
Mallory	aktiver Angreifer; *malicious adversary*

Chiffren

- Eine **Chiffre** wird def. durch drei Mengen
  1. $\mathcal{M}$: Klartextemenge (Nachrichten)
  2. $\mathcal{C}$: Chiffretextmenge (Kryptogramme)
  3. $\mathcal{K}$: Schlüsselmenge
- und zwei (bzw. drei) effiziente Algorithmen
  1. $\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ (Verschlüsseln)
  2. $\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ (Entschlüsseln)
  (3. $\mathcal{G} : \emptyset \to \mathcal{K}$ (Schlüssel erzeugen))
- Für jeden Klartext $M \in \mathcal{M}$ und jeden Schlüssel $\mathbf{K} \in \mathcal{K}$

$$\mathcal{D}(\mathbf{K}, \mathcal{E}(\mathbf{K}, M)) = M$$

- Schreibweise statt $\mathcal{E}(\mathbf{K}, \cdot)$ bzw. $\mathcal{D}(\mathbf{K}, \cdot)$ auch $\mathcal{E}_{\mathbf{K}}(\cdot)$ bzw. $\mathcal{D}_{\mathbf{K}}(\cdot)$

Kerkhoffs Prinzip

Security-through-obscurity Prinzip

Die Sicherheit eines Systems oder eines Verfahrens hängt von der Geheimhaltung dessen Funktionsweise ab.

Gegenkonzept wurde 1883 von Auguste Kerckhoffs formuliert.

Kerkhoffs Prinzip (1883)

Die Sicherheit eines Verschlüsselungsverfahrens beruht auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus.

Sichtweise der modernen Kryptographie

Shannon (1949)

"Der Feind kennt das benutzte System"

- Unterscheidung zwischen Kryptosystem und Schlüssel.
- Forderung: Ein System soll auch dann sicher sein, wenn der Gegner das System kennt, bis auf den verwendeten Schlüssel.

Angriffskategorien für Verschlüsselungsverfahren

Bei allen Angriffen kennt die Angreifer:in $\mathcal{A}$ das verwendete Verschlüsselungsverfahren (bis ins letzte Detail).

- Known Ciphertext Angriff (KCA)
  - Gegeben: Abgefangene Chiffretext.
  - Ziel: M (partielle) rekonstruieren.
- Known Plaintext Angriff (KPA)
  - Gegeben: Abgefangene Klartext-Chiffretext-Paare (M_i, C_i) mit $C_i = \mathcal{E}_K(M_i)$.
  - Ziel: K (partielle) rekonstruieren.
- Chosen Plaintext Angriff (CPA)
  - Geg: API-Zugriff (Orakel-Zugriff) auf $\mathcal{E}_K$.
  - Ziel ist es die Ausgabe von $\mathcal{E}_K$ von Zufallswerten unterscheiden zu können und zwar mit einer Erfolgswahrscheinlichkeit die signifikant von 0.5 abweicht.

2.1: Klassische Kryptographie
Die Caesar-Chiffre (1/4)

Julius Caesar verschlüsselte seine Nachrichten, indem er Klartext-Buchstaben "a", . . . , "z" auf die folgende Weise auf Chiffretext-Buchstaben "A", . . . , "Z" abbildete.

a	$\longrightarrow$	D		v	$\longrightarrow$	Y
b	$\longrightarrow$	E		w	$\longrightarrow$	Z
c	$\longrightarrow$	F	. . .	x	$\longrightarrow$	A
d	$\longrightarrow$	G		y	$\longrightarrow$	B
e	$\longrightarrow$	H		z	$\longrightarrow$	C

Beispiel: "`caesar`" $\longrightarrow$ "FDHVDU"

Die Caesar-Chiffre (2/4)

Ist das nun eine Chiffre?

- Klartextmenge $\mathcal{M} = \{\text{"a"}, \ldots, \text{"z"}\}$
- Chiffretextmenge $\mathcal{C} = \{\text{"A"}, \ldots, \text{"Z"}\}$
  (Großbuchstaben wg. übersicht)
- Ver- und Entschlüsselungsalgorithmus $\mathcal{E}$ und $\mathcal{D}$: Klar!
- Schlüsselmenge???

Die Caesar-Chiffre (3/4)

Man ordne den Buchstaben eine Zahl aus der Menge $\mathbb{Z}_{26} = \{0, \ldots, 25\}$ zu

a	bzw.	A	$\leftrightarrow$	0
b	bzw.	B	$\leftrightarrow$	1
c	bzw.	C	$\leftrightarrow$	2
y	bzw.	Y	$\leftrightarrow$	24
z	bzw	Z	$\leftrightarrow$	25

Mengen $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$.

Die Caesar-Chiffre (4/4)

- Verschlüsseln: $\mathcal{E}(\mathbf{K}, M) = (M + \mathbf{K}) \bmod 26$
- Entschlüsseln: $\mathcal{D}(\mathbf{K}, C) = (C - \mathbf{K}) \bmod 26$
- Schlüsselerzeugung $\mathcal{G}$: Trivial!

Die Algorithmen sind offenbar effizient.

Es gilt

$$\mathcal{D}_{\mathbf{K}}(\mathcal{E}_{\mathbf{K}}(M)) = M + \mathbf{K} - \mathbf{K} = M.$$

Wir haben eine Chiffre!!!

Die Caesar-Chiffre (5)

Beispiel:
Wir haben den Chiffretext

“IGJG KOGU RCUU YQTV”

aufgefangen. Wer kann diese Nachricht dechiffrieren?

Die Substitutionschiffre

Bei einer Substitutionschiffre ordnet man jedem Klartext-Buchstaben eindeutig einen Chiffretext-Buchstaben zu, zum Beispiel

a	$\longrightarrow$	D		v	$\longrightarrow$	I
b	$\longrightarrow$	R		w	$\longrightarrow$	K
c	$\longrightarrow$	L	$\cdots$	x	$\longrightarrow$	F
d	$\longrightarrow$	M		y	$\longrightarrow$	X
e	$\longrightarrow$	H		z	$\longrightarrow$	Z

Die Substitutionschiffre (2)

Die Caesar-Chiffre ist eine Spezialfall der Substitutionschiffre. Während die Caesar-Chiffre bei einem Alphabet der Größe 26 nur 26 verschiedene Schlüssel erlaubt, sind es bei der Substitutionschiffre

$$26! = 26 * 25 * 24 * \cdots * 2 * 1 \approx 4 * 10^{26} \approx 2^{88.4}$$

"Blindes" Ausprobieren ("brute-force") führt bei der Caesar-Chiffre schnell zum Erfolg, ist bei der Substitutionschiffre aber aussichtslos.

Die Substitutionschiffre (3)

Doch: Auch die Substitutionschiffre ändert die Sprachstatistik nicht. Im Deutschen gilt ungefähr die folgende Verteilung

- "e": Ein Sechstel aller Buchstaben
- "e", "n", "i": zusammen ein Drittel aller Buchstaben
- "e", "n", "i", "s" "r", "a", "t", "d": zwei Drittel aller Buchstaben

Die Häufigkeit von Buchstabenpaaren, -tripeln, . . . , ist auch hilfreich.

Die Substitutionschiffre (4)

Hat man genug (z.B., die häufigsten acht) Buchstaben richtig zugeordnet, dann kann man sich die restlichen Buchstaben ergänzen.

Chiffretext:

```
dingnbrnsryebdnkirnivnbgewgrirerimvgthiaabn
onbgthzenggnzrfwnbynvvkfvdinhfneaiugrnvfthr
wethgrfwnvpnvvrpfvvkfvdnvivhfzrgthmvnbbfrnv
```

Acht Buchstaben ("e", "n", "i", "s" "r", "a", "t", "d") richtig:

```
dieserte*t**rde*iteiners**stit*ti*ns**i**re
*ers****esse*ta*er*enn*andie*ae**i*stena**t
****sta*en*ennt*ann*andenin*a*ts***nerraten
```

2.2: Perfekte Kryptographie
Informationstheoretische Sicherheit

*Eine Chiffre $(\mathcal{E}, \mathcal{D}, \mathcal{G})$ ist **informationstheoretisch sicher** wenn nicht einmal ein Angreifer mit **unbeschränkter Rechenzeit** diese knacken kann.*

(In diesem Abschnitt.)

Informationstheoretische Sicherheit

Auftretende Variablen:

- M: ein (unbekannter) Klartext
- C: ein (irgendwann bekannter) Chiffretext
- $\mathbf{X}$: Zufallsvariable für den Klartext
- $\mathbf{Y}$: Zufallsvariable für den Chiffretext
- $\mathbf{Z}$: Zufallsvariable für den Schlüssel

Situation beim Abhören einer verschlüsselten Nachricht:

Vorwissen: $\Pr[\mathbf{X} = M]$ (“a priori Wahrscheinlichkeit”)

Nachwissen: $\Pr[\mathbf{X} = M | \mathbf{Y} = C]$ (“a posteriori W.”)

Informationstheoretische Sicherheit (Def.)

Ein Chiffretext C ist *möglich*, wenn $\Pr[\mathbf{Y} = C] > 0$ gilt.

Definition 3.1

Eine Chiffre heißt *perfekt*, wenn für alle Klartexte M und alle möglichen Chiffretexte C gilt:

$$\Pr[\mathbf{X} = M | \mathbf{Y} = C] = \Pr[\mathbf{X} = M].$$

Die Substitutionsschiffre ist nicht perfekt.

- Angenommen es gilt: $\Pr[\mathbf{M} = otto] = 0.01$
- Dann gilt: $\Pr[\mathbf{M} = otto \mid \mathbf{C} = ABCD] = 0$
- $\Longrightarrow \Pr[\mathbf{M} = otto] \neq \Pr[\mathbf{M} = otto \mid \mathbf{C} = ABCD]$

Exkurs: Exklusives Oder (XOR)

Bitweise Addition modulo 2

Rechenregeln

- $a \oplus a = 0$
- $a \oplus 0 = a$
- $a \oplus b = b \oplus a$
- $a \oplus \overline{a} = 1 \ldots 1$
- $a \oplus b = c \iff a \oplus c = b \iff c \oplus b = a$

Wahrheitstabelle

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Beispiele:

- $7 \oplus 5 = 111 \oplus 101 = 010 = 2$
- $42 \oplus 23 = 101010 \oplus 010111 = 111101 = 61$
- $12 \oplus 12 = 1100 \oplus 1100 = 0000 = 0$
- $8 \oplus 0 = 1000 \oplus 0000 = 1000 = 8$

Eine einfache Beispiel-Chiffre

- Klartext- Chiffretext und Schlüsselmenge jeweils $\{0,1\}$
- Schlüssel **K** zufällig und gleichverteilt aus $\{0,1\}$ ($\mathbf{K} \xleftarrow{\$} \{0,1\}$)
- Chiffretext $C = M \oplus \mathbf{K}$:

Eine einfache Beispiel-Chiffre

Satz 4.1

Die Beispielchiffre ist perfekt.
Sie ist sogar für jede mögliche Verteilung der Klartexte perfekt.

(→ Tafel)

Beobachtung

Man beachte: Wenn wir den Schlüssel anders wählen (ungleichverteilt), ist die Beispielchiffre nicht perfekt.

(→ Tafel)

Das One-Time-Pad (Vernam, 1917)

- Ganze Zahl n ("Anzahl der Bits")
  Klartext- = Chiffretext- = Schlüsselmenge = $\{0,1\}^n$
- Verschlüsseln des Klartextes $M = (M_1, \ldots, M_n)$ unter dem Schlüssel $\mathbf{K} = (\mathbf{K}_1, \ldots \mathbf{K}_n)$:

$$\mathcal{E}_{\mathbf{K}}(M) = (M_1 \oplus \mathbf{K}_1, \ldots, M_n \oplus \mathbf{K}_n)$$

- Entschlüsseln des Chiffretextes $C = (C_1, \ldots, C_n)$:

$$\mathcal{D}_{\mathbf{K}}(C) = (C_1 \oplus \mathbf{K}_1, \ldots, C_n \oplus \mathbf{K}_n)$$

- Schlüssel $\mathbf{K} = (\mathbf{K}_1, \ldots \mathbf{K}_n) \in \{0,1\}^n$: zufällig und gleichverteilt

(Oft auch als Vernam-Chiffre bezeichnet.)
(Ggf. Klartext- = Chiffretext- = Schlüsselmenge = $\{\text{“a”}, \ldots, \text{“z”}\}^n$.)

Das One-Time-Pad (2)

Satz 4.2 (Shannon, 1949)

Das One-Time-Pad (OTP) ist perfekt.

Praktische Probleme des OTP

1. Gleichverteilte zufällige Wahl der Schlüssel

2. Lange Schlüssel, die man insbesondere nicht wiederverwenden darf $\rightarrow$ *nächste Folie*

3. Wenn aktive Angreifer einzelne Bits des Chiffretextes ändern, dann ändern sie *genau* die entsprechenden Bits im entschlüsselten Klartext

Wiederverwenden eines OTP-Schlüssels

Sind C und C' Chiffretexte unter dem gleichen OTP-Schlüssel **K**, dann gilt für die zugehörigen Klartexte M und M':

$$M = C \oplus \mathbf{K}, \quad M' = C' \oplus \mathbf{K},$$

also

$$M \oplus M' = C \oplus C'!$$

Angriffe:

1. Chosen und Known Plaintext: trivial
2. Known Ciphertext: liefert reichlich Information (siehe Bild)

Grundsätzliches Problem perfekter Chiffren

Satz 4.3

Für jede perfekte Chiffre $(\mathcal{E}, \mathcal{D}, \mathcal{G})$ gilt: Die Schlüsselmenge ist mindestens so groß wie die Menge der möglichen Klartexte.

2.3: Unterteilung der Modernen Kryptographie

Die moderne Kryptographie ist in zwei Gebiete unterteilt.

- Symmetrische Kryptographie
  - Zum Ver- und Entschlüsseln wird der gleiche Schlüssel verwendet
  - Wenig mathematische Strukturen
  - Sicherheit von Verfahren beruht auf sehr effizienten Bausteinen wie Blockchiffren und Hashfunktionen

- Asymmetrische Kryptographie
  - Zum Ver- und Entschlüsseln werden verschiedene Schlüssel verwendet
  - Viel mathemtische Strukturen
  - Sicherheit von Verfahren basiert auf Problemen der Zahlentheorie

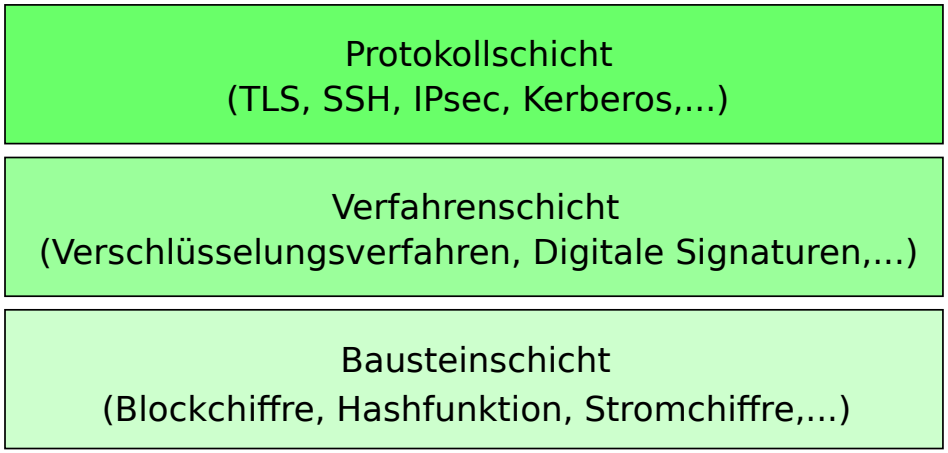
Die drei Schichten der modernen Kryptographie

Protokollschicht
(TLS, SSH, IPsec, Kerberos,...)

Verfahrenschicht
(Verschlüsselungsverfahren, Digitale Signaturen,...)

Bausteinschicht
(Blockchiffre, Hashfunktion, Stromchiffre,...)

Anmerkungen zu den Schichten (1)



- Es gibt Bausteine der symmetrischen und asymmetrischen Kryptographie.
  - AES (Symmetrischer Baustein)
  - RSA (Asymmetrische Baustein)
- Asymmetrische Verfahren können auch symmetrischer Bausteine (Hashfunktionen) verwenden

  Beispiel: RSA-Signaturen basiert auf RSA und einer Hashfunktion

Anmerkungen zu den Schichten (2)

Kryptographische Protokolle sind meist hybrid, d.h. Sie verwenden Verfahren der symmetrischen und asymmetrischen Kryptographie

Beispiel: Transport Layer Security (TLS)

- Asymmtrische Verfahren zur Authentifizierung und Schlüsselaustausch
- Symmetrische Verfahren zur verschlüsselten Übertragung

Zusammenfassung

Sie sollten . . .

- . . . zentrale Begriffe der Kryptographie verstanden haben (insbesondere Kerkhoffs Prinzip, Sicherheit, und perfekte Chiffren),
- . . . und bestimmte klassische Chiffren *knacken* können,
- . . . die Nachteile einer perfekten Chiffre verinnerlicht haben.