Einführung in die Kryptographie
2. Vorlesung

Ulm, 4. 5. 2006

Blockchiffren

Zur Erinnerung: ein Verschüsselungsverfahren (Kryptosystem) besteht aus:

- *Klartextraum* $\mathcal{P}$ ($p \in \mathcal{P}$: *Klartexte*)
- *Chiffretextraum* $\mathcal{C}$ ($c \in \mathcal{C}$: *Chiffretexte*)
- *Schlüsselraum* $\mathcal{K}$ ($k \in \mathcal{K}$: *Schlüssel*)
- *Verschlüsselungsfunktionen*

$$\mathcal{E} = \{ E_k : \mathcal{P} \to \mathcal{C} \mid k \in \mathcal{K} \}$$

- *Entschlüsselungsfunktionen*

$$\mathcal{D} = \{ D_k : \mathcal{C} \to \mathcal{P} \mid k \in \mathcal{K} \}$$

Für jedes $e \in \mathcal{K}$ gibt es ein $d \in \mathcal{K}$ so, dass $\forall p \in \mathcal{P}$:

$$D_d(E_e(p)) = p.$$

Blockchiffren

Blockchiffren sind Verschlüsselungsverfahren, die Blöcke fester Länge auf Blöcke derselben Länge abbilden.

Dazu fixiert man eine endliche, nichtleere Menge Σ, das *Alphabet*, und eine natürliche Zahl n, die *Blocklänge*. Dann:

$$\mathcal{P} = \mathcal{C} = \Sigma^n.$$

Typische Beispiele:

- $\Sigma = \{A, B, \ldots, Z\} \cong \{0, \ldots, 25\}$
- $\Sigma = \{0, 1\}$

Eine Blockchiffre der Länge 1 heisst *Substitutionschiffre*.

Permutationen

Sei X eine endliche, nichtleere Menge. Eine *Permutation* von X ist eine bijektive Abbildung $\sigma : X \to X$.

Wir bezeichnen mit $S(X)$ die Menge aller Permutationen von X. $S(X)$ bildet eine (i.A. nichtkommutative) Gruppe:

$$S(X) \times S(X) \to S(X), \quad (\sigma, \tau) \mapsto \sigma \circ \tau.$$

Die Anzahl der Elemente von $S(X)$ ist

$$|S(X)| = |X|! = 1 \cdot 2 \cdot \ldots \cdot |X|.$$

Blockchiffren

Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \{E_k\}, \{D_k\})$ eine Blockchiffre, mit $\mathcal{P} = \mathcal{C} = \Sigma^n$.

Da $\mathcal{P}$ und $\mathcal{C}$ endlich sind und dieselbe Kardinalität haben, sind die Ver- und Entschlüsselungsfunktionen E_k, D_k bijektiv, d.h.

$$E_k, D_k \in S(\Sigma^n).$$

Eine mögliche Wahl von $\mathcal{K}$ wäre $\mathcal{K} := S(\Sigma^n)$.

Aber: um einen Schlüssel $k \in \mathcal{K}$ zu speichern, benötigt man eine Tabelle mit $|\Sigma|^n$ Einträgen. Das ist nur dann praktikabel, wenn n sehr klein ist.

Substitutionschiffren

Wir wählen

$$\Sigma := \{A, B, \ldots, Z\} \cong \{0, 1, \ldots, 25\},$$

$n := 1$ und

$$\mathcal{K} := S(\Sigma).$$

Dann ist

$$|\mathcal{K}| = 26! \sim 4,03 \cdot 10^{26}.$$

Eine *vollständige Suche* (*exhaustive search*) im Schlüsselraum ist also praktisch unmöglich.

Trotzdem ist dieses Kryptosystem i.A. leicht mit einer Häufigkeitsanalyse zu brechen.

Die Vigenère-Chiffre

Die Schwäche der Verschiebe- und Substitutionschiffre ist: ein Klartextbuchstabe $p \in \Sigma$ wird immer auf denselben Chiffretextbuchstaben abgebildet.

Die statistischen Eigenschaften der Sprache, in der der Klartext verfasst ist, kann daher zu einem Angriff benutzt werden.

Um so einen Angriff zu erschweren, benutzte man im 18. und 19. Jhd. die sogenannte *Vigenère-Chiffre*:

$$\Sigma = \{A, B, \ldots, Z\} \cong \{0, \ldots, 25\},$$

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \{w = (w_1, w_2, \ldots, w_n)\}.$$

Die Länge n eines Klartextes $p \in \mathcal{P}$ ist beliebig. Für den Schlüssel $k \in \mathcal{K}$ wählt man ein relativ kurzes Wort, z.B.

$$k = \text{‘SCHLUESSEL’}.$$

Die Vigenère-Chiffre

Für $k = (k_1, \ldots, k_m)$ ist die Verschlüsselungsfunktion $E_k : \mathcal{P} \to \mathcal{C}$ folgendermassen definiert.

Ist $p = (p_1, \ldots, p_n) \in \mathcal{P}$ so ist

$$c = E_k(p) = (c_1, \ldots, c_n)$$

mit

$$c_i := p_i + k_j \pmod{26},$$

wobei $i = lm + j$ und $1 \leq j \leq m$, d.h.

$$j := (i \mod m) + 1.$$

Die Vigenère-Chiffre

Sie galt bis ins 19. Jhd. als sicher. Trotzdem führt eine Häufigkeitsanalyse in vielen Fällen zu einem erfolgreichen Angriff:

- Kennt man die Schüssellänge m, so kann man für jedes $j \in \{1, \ldots, m\}$ den Eintrag k_j durch eine Häufigkeitsanalyse der Folge

  $$c_j, c_{m+j}, c_{2m+j}, \ldots$$

  bestimmen (es muss $m \ll n$ gelten!).

- Die Schlüssellänge m kann man durch vollständige Suche ermitteln, oder mithilfe der folgenden Heuristik raten.

Raten der Schlüssellänge

In den meisten Sprachen sind bestimmte Folgen von Buchstaben wahrscheinlicher als andere, z.B. ‘ER’ in einem deutschen Text (*Bigramm*).

So eine ‘Regelmässigkeit’ im Klartext wird in der Regel durch die Verschlüsselung verwischt, d.h. der Chiffretext wird viel seltener ein häufig vorkommendes Bigramm enthalten als der Klartext.

Raten der Schlüssellänge

Aber: ist der Abstand zwischen zwei Positionen desselben Bigrammes ein Vielfaches von m, so entsteht auch im Chiffretext eine Wiederholung.

D.h.: Bigramme, die häufiger im Chiffretext vorkommen, als statistisch zu erwarten wäre, geben Information über die Schlüssellänge m preis.

Dieses Verfahren nennt man Parallelstellensuche:

- Babbage, ca. 1850
- Kasiki, 1863

One Time Pad

Die Vigenère-Chiffre ist unsicher für $m \ll n$.

Wie sieht es aus für $n = m$?

Wählt man den Schlüssel k zufällig, so ist das Verfahren *perfekt geheim*.

Allerdings darf man denselben Schüssel immer nur einmal verwenden.

Variante (Vernam, 1917):

$$\Sigma = \{0,1\}, \quad \mathcal{P} = \mathcal{C} = \mathcal{K} = \Sigma^n,$$

und für $k \in \mathcal{K}$ ist

$$E_k : \{0,1\}^n \to \{0,1\}^n, \quad p \mapsto p \oplus k$$

($\oplus$: exklusives Oder).

Perfekte Geheimhaltung

Es sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \{E_k\}, \{D_k\})$ ein Kryptosystem; $\mathcal{P}, \mathcal{C}, \mathcal{K}$ seien endliche Mengen.

Klartexte $p \in \mathcal{P}$ treten mit einer bestimmten Wahrscheinlichkeit $\mathrm{Pr}_{\mathcal{P}}$ auf. Die Schlüsselauswahl erfolgt ebenfalls nach einer Wahrscheinlichkeitsverteilung $\mathrm{Pr}_{\mathcal{K}}$.

Unter der Annahme, dass $p \in \mathcal{P}$ und $k \in \mathcal{K}$ unabhängig voneinander sind, erhält man eine Wahrscheinlichkeitsverteilung auf $\mathcal{P} \times \mathcal{K}$.

Perfekte Geheimhaltung

Insbesondere kann man die Wahrscheinlichkeit eines auftretenden Chiffretextes $c \in \mathcal{C}$ bestimmen:

$$\Pr(c) := \Pr(\{(p,k) \mid E_k(p) = c\}).$$

Definition: Das Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \{E_k\}, \{D_k\})$ heisst *perfekt geheim* wenn für alle $p \in \mathcal{P}$ und $c \in \mathcal{C}$ gilt:

$$\Pr(p \mid c) = \Pr(p).$$

Der Satz von Shannon

Satz: (Shannon, 1949) Sei $|\mathcal{C}| = |\mathcal{K}| = |\mathcal{P}| < \infty$, und sei $\Pr(p) > 0$ für jeden Klartext $p \in \mathcal{P}$. Dann ist das Kryptosystem genau dann perfekt geheim, wenn die Schlüssel $k \in \mathcal{K}$ gleichverteilt sind und wenn es für jedes $p \in \mathcal{P}$ und jedes $c \in \mathcal{C}$ genau ein $k \in \mathcal{K}$ gibt mit

$$E_k(p) = c.$$

Insbesondere ist das Vernam-One-Time-Pad perfekt geheim, wenn man den Schlüssel völlig zufällig wählt.