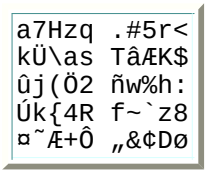
Kryptologie

Die monoalphabetische Substitution



Einleitendes Beispiel

Man verwendet als Schlüssel eine Permutation des Alphabets (ein »Tauschalphabet«), etwa konkret in der Gestalt

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
UNIVERSTABCDFGHJKLMOPQWXYZ
```

Verschlüsselt wird ein Klartext, indem jeder Buchstabe in der ersten Zeile aufgesucht und durch den darunter stehenden ersetzt wird, im Beispiel so:

```
PFING STEND ASLIE BLICH EFEST WARGE KOMME N
JRAGS MOEGV UMDAE NDAIT EREMO WULSE CHFFE G
```

Für die Entschlüsselung braucht man die Umkehrpermutation

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
IJKLEMNOCPQRSBTUVFGHADWXYZ
```

die man durch Umsortieren der Schlüsselpermutation erhält.

In der Geschichte der Kryptographie wurden oft als Geheimtextzeichen geheimnisvolle Symbole verwendet (wie z. B. solche). Das ist eine »illusorische Komplikation«, d. h., es erhöht die Sicherheit nicht nennenswert:

> **FAQ:** *Wird ein Verschlüsselungsverfahren nicht sicherer, wenn man statt normaler Buchstaben unverständliche Zeichen verwendet*?

Mathematische Beschreibung

Mit $\mathbf{S}(\Sigma)$ wird die Gruppe der Permutationen des Alphabets Σ bezeichnet, also die »volle symmetrische Gruppe«.

> Mathematischer Exkurs über Permutationen: PDF.

Eine monoalphabetische Substitution (oder Buchstabentausch) entsteht aus einer Permutation $\sigma \in \mathbf{S}(\Sigma)$ durch buchstabenweise Anwendung:

$$f_\sigma(a_1,...,a_r) := (\sigma a_1,...,\sigma a_r) \quad \text{für} \quad a = (a_1,...,a_r) \in \Sigma^r.$$

Definition: Eine **monoalphabetische Chiffre** über Σ ist eine Familie $F = (f_\sigma)_{\sigma \in K}$ von monoalphabetischen Substitutionen mit einem Schlüsselraum $K \subseteq \mathbf{S}(\Sigma)$.

Beispiele

1. Die Verschiebechiffre mit K = Menge der Rechtstranslationen.
2. Die allgemeine monoalphabetische Chiffre; hier ist $K = \mathbf{S}(\Sigma)$, also $\#K = n!$, wenn $n = \#\Sigma$.
3. Oft wird aber tatsächlich nur eine eingeschränkte Auswahl von Schlüsseln verwendet, z. B. nach der Regel: *Nimm ein Schlüsselwort, streiche alle Buchstaben, die schon weiter vorne vorgekommen sind, und hänge alle nicht benutzten Buchstaben in alphabetischer Reihenfolge an* [ARGENTI ca. 1580].

Beispiel für diese Regel, die Schlüsselpermutation zu bilden, die im einleitenden Beispiel verwendet wurde:

```
UNIVERSITAET
UNIVERSTA
UNIVERSTABCDFGHJKLMOPQWXYZ
```

Frage: Was ist an dieser Regel schlecht? Wie kann man diese Schwäche vermeiden?

Anwendung

Verschlüsselung und Entschlüsselung per WWW-Formular.

Übungsaufgabe: Verschlüssle und entschlüssle ein paar Texte mit Hilfe dieses WWW-Dienstes.

[Die Programme werden auf der nächsten Seite beschrieben und als lokal ausführbare Versionen zum Herunterladen angeboten.]

Die effektive Schlüssellänge

Bei der allgemeinen monoalphabetischen Chiffre ist die Exhaustion, also die vollständige Schlüsselsuche, nicht erfolgversprechend (auch nicht mit Computerhilfe), da

$$d(F) = {}^2\log(n!) \geq n \cdot [{}^2\log(n) - {}^2\log(e)] \approx n \cdot {}^2\log(n)$$

nach der STIRLING-Formel.

Im Falle $n = 26$ ist beispielweise

$$n! \approx 4 \cdot 10^{26}, \quad d(F) = {}^2\log(26!) \approx 88.38.$$

Anmerkung. Falls nicht alle Buchstaben im Geheimtext vorkommen, ist der Suchaufwand entsprechend kleiner, da nicht der gesamte Schlüssel bestimmt werden muss (und kann).

Autor: Klaus Pommerening, 29. September 1999; letzte Änderung: 30. Januar 2008.