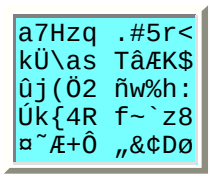
Kryptologie

Die monoalphabetische Substitution



Mit **S**(Σ) wird die Gruppe der Permutationen des Alphabets Σ bezeichnet, also die »volle symmetrische Gruppe«.

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

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

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.*

Beispiel für diese Regel, die Schlüsselpermutation zu bilden:

```
UNIVERSITAET
UNIVERSTA
UNIVERSTABCDFGHJKLMOPQWXYZ
```

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

Im Beispiel gibt man die Schlüsselpermutation in der Gestalt

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
UNIVERSTABCDFGHJKLMOPQWXYZ
```

an und verschlüsselt einen Klartext nach dem Schema

```
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.

Anwendung

Verschlüsselung und Entschlüsselung per WWW-Formular.

Die effektive Schlüssellänge

Bei der allgemeinen monoalphabetischen Chiffre ist die vollständige Schlüsselsuche (auch mit Computerhilfe) nicht erfolgversprechend, 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: 23. April 2002.

E-Mail an Pommerening@imsd.uni-mainz.de.