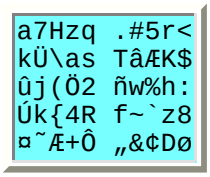
Kryptologie

Die HILL-Chiffre



Beschreibung

Alphabet: $\Sigma = \mathbf{Z}/n\mathbf{Z}$, also ein endlicher Ring.

Schlüsselraum: $K = \mathrm{GL}_l(\mathbf{Z}/n\mathbf{Z})$, die multiplikative Gruppe der invertierbaren $l \times l$-Matrizen.

Verschlüsselung blockweise, wobei l die Blocklänge ist: Für $k \in \mathrm{GL}_l(\mathbf{Z}/n\mathbf{Z})$ und $(a_1, ..., a_l) \in \Sigma^l$ ist

$$f_k(a_1, \ldots, a_l) = k \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix}$$

oder in ausgeschriebener Form

$$c_i = \sum_{j=1}^{l} k_{ij} a_j \quad \text{für } i = 1, \ldots, l.$$

Entschlüsselung mit der inversen Matrix:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix} = k^{-1} \begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix}$$

Verwandte Chiffren

Spezialfall: Wird k als die Permutationsmatrix P_σ gewählt, so ist f_k die Blocktransposition zu σ.

Verallgemeinerung: Die affine Chiffre. Hier wird ein Schlüssel

$$(k, b) \in \mathrm{GL}_l(\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})^l$$

gewählt; verschlüsselt wird nach der Formel

$$c = ka + b.$$

Hier ist als Spezialfall die BELASO-Chiffre mit Schlüssel b enthalten, wenn man k als Einheitsmatrix

wählt.

Beispiel

Sei $l = 2$ und

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Dann ist Det $k = 77 - 24 = 51 \equiv -1 \pmod{26}$ und

$$k^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

Zur Umrechnung von Buchstaben in Zahlen mod 26 braucht man die Tabelle

```
A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
```

Damit wird der Klartext `Herr` = (7,4,17,17) verschlüsselt zu

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 77+32 \\ 21+28 \end{pmatrix} = \begin{pmatrix} 109 \\ 49 \end{pmatrix} = \begin{pmatrix} 5 \\ 23 \end{pmatrix}$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 17 \\ 17 \end{pmatrix} = \begin{pmatrix} 187+136 \\ 51+119 \end{pmatrix} = \begin{pmatrix} 323 \\ 170 \end{pmatrix} = \begin{pmatrix} 11 \\ 14 \end{pmatrix}$$

also f_k(`Herr`) = (5,23,11,14) = `FXLO`.

Zur Probe die Entschlüsselung:

$$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}\begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} = \begin{pmatrix} 35+24 & 77+252 \\ 115+253 & 253+154 \end{pmatrix} = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}$$

Bewertung

+ Wesentlich stärker als die Blocktransposition und die BELASO-Chiffre.
+ Geheimtexte sehr gut gleichverteilt; Angriff mit nichts als Geheimtext fast unmöglich.
- Sehr anfällig für Angriff mit bekanntem Klartext.

Die HILL-Chiffre wurde 1929 von Lester HILL [Bild] vorgeschlagen und erregte einiges Aufsehen (vor allem bei Mathematikern), wurde aber nie ernsthaft eingesetzt.

Ihre eigentliche Bedeutung liegt darin, dass hier erstmals systematisch algebraische Methoden in die Kryptologie eingeführt wurden, und dass sie deutlich macht, welche Bedeutung Linearität für die

Kryptoanalyse hat.

Autor: Klaus Pommerening, 3. Februar 2000; letzte Änderung: 12. August 2002.

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