8.10 Kryptoanalyse der HILL-Chiffre

Die Blocklänge

Die Blocklänge l kann man dadurch bestimmen, dass alle Geheimtextlängen Vielfache von l sind – zumindest wenn das Verfaheren „in Reinkultur“, d. h. ohne verschleiernde Modifikationen, angewendet wurde. Notfalls hilft aber auch das (etwas lästige) Durchprobieren aller in Frage kommenden Längen.

Bekannter Klartext

Die Kryptoanalyse der HILL-Chiffre ist fast nur mit bekanntem Klartext erfolgversprechend – dann aber fast trivial. Zur erfolgreichen Kryptoanalyse reichen in der Regel l bekannte Klartextblöcke, also bekannter Klartext der Länge l^2. (Das ist ja im wesentlichen auch die Länge des Schlüssels, wie in Abschnitt 8.9 hergeleitet.)

Seien $(a_{11}, \ldots, a_{l1})$, $\ldots$, $(a_{1l}, \ldots, a_{ll})$ die bekannten Klartextblöcke mit den zugehörigen Geheimtextblöcken $(c_{11}, \ldots, c_{l1})$, $\ldots$, $(c_{1l}, \ldots, c_{ll})$.

Daraus ergibt sich die Matrizen-Gleichung

$$\begin{pmatrix} k_{11} & \ldots & k_{1l} \\ \vdots & \ddots & \vdots \\ k_{l1} & \ldots & k_{ll} \end{pmatrix} \begin{pmatrix} a_{11} & \ldots & a_{1l} \\ \vdots & \ddots & \vdots \\ a_{l1} & \ldots & a_{ll} \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1l} \\ \vdots & \ddots & \vdots \\ c_{l1} & \ldots & c_{ll} \end{pmatrix}$$

oder kurz geschrieben: $kA = C$ in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$. Falls zufällig A invertierbar ist, kann man sofort nach k auflösen und erhält den Schlüssel

$$k = CA^{-1}.$$

Die Matrix-Inversion ist effizient nach Abschnitt 8.7. Ferner ist A nach Abschnitt 8.9 mit hoher Wahrscheinlichkeit invertierbar. Falls das nicht der Fall ist, benötigt man geringfügig mehr bekannten Klartext. Die Details der Lösung werden hier nicht ausgeführt. Statt dessen ein Beispiel.

Beispiel

In dem Beispiel aus Abschnitt 8.8 – gedacht als Teil eines längeren Textes – sei der Klartext `Herr` bekannt. Er bildet zwei Blöcke und somit die Matrix

$$A = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

Deren Determinante ist $\operatorname{Det} A = 17 \cdot (7 \cdot 1 - 4 \cdot 1) = 17 \cdot 3 = 51 \equiv -1 \bmod 26$; der Kryptoanalytiker hat also Glück und kann sofort invertieren:

$$A^{-1} = \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix}.$$

Daraus ergibt sich die Schlüsselmatrix:

$$k = \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Die affine Chiffre

Für die affine Chiffre $c = ka + b$ braucht man im allgemeinen $l + 1$ bekannte Klartextblöcke $a_0, \ldots, a_l$. Durch Differenzenbildung erhält man

$$\begin{aligned} c_l - c_0 &= k \cdot (a_l - a_0), \\ &\ldots \\ c_l - c_{l-1} &= k \cdot (a_l - a_{l-1}). \end{aligned}$$

Dadurch ist die Kryptoanalyse auf die der Hill-Chiffre mit l bekannten Klartextblöcken reduziert.

Fazit

Linearität in einer Chiffre macht sie extrem anfällig für einen Angriff mit bekanntem Klartext, weil lineare Gleichungssysteme so leicht lösbar sind – zumindest über den Ringen, in denen man praktisch rechnen kann.

Daher wird man für die Konstruktion von sicheren Chiffren zur Vermeidung von Angriffen mit bekanntem Klartext auf Nichtlinearität setzen: Algebraische Gleichungen höheren Grades sind sehr viel schwerer lösbar. Daher der Merksatz:

Bekannter Klartext ist der natürliche Feind der Linearität.

Übungsaufgabe. Hill hatte vorgeschlagen, vor Anwendung der linearen Abbildung das Alphabet zu permutieren, d. h., eine monoalphabetische Substitution vorzuschalten. Wie wirkt sich dies auf die Kryptoanalyse aus?