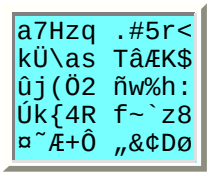

Blocklänge

Die Blocklänge *l* ist daran zu erkennen, dass alle Geheimtextlängen Vielfache von *l* sind. Notfalls hilft auch Durchprobieren der in Frage kommenden Längen.

Bekannter Klartext

Zur erfolgreichen Kryptoanalyse reichen in der Regel *l* bekannte Klartextblöcke, also bekannter Klartext der Länge l^2. (Das ist ja auch die Länge des Schlüssels.)

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

Daraus ergibt sich die Matrizen-Gleichung

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

oder kurz geschrieben: $KA = C$ in $M_{ll}(\mathbf{Z}/n\mathbf{Z})$. Falls zufällig A invertierbar ist, können wir sofort nach *K* auflösen und erhalten: den Schlüssel $K = CA^{-1}$.

Die Matrix-Inversion ist effizient nach Abschnitt 8. Ferner ist *A* nach Abschnitt 10 mit hoher Wahrscheinlichkeit invertierbar.

Beispiel

In dem Beispiel aus Abschnitt 9 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 Det $A = 17 \times [7 \cdot 1 - 4 \cdot 1] = 17 \cdot 3 = 51 \equiv -1 \bmod 26$; wir haben also Glück gehabt und können 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 und Spezialfälle

Für die affine Chiffre $c = ka + b$ braucht man l+1 bekannte Klartextblöcke a_0, ..., a_l. Daraus erhält man durch Differenzbildung

$$c_1 - c_0 = k\cdot(a_1 - a_0),$$
$$\ldots$$
$$c_l - c_{l-1} = k\cdot(a_l - a_{l-1}).$$

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

Fazit

Linearität kann gute statistische Verteilung des Geheimtexts ergeben, macht aber extrem anfällig für bekannten Klartext.

Lineare Gleichungssysteme sind leicht lösbar. Daher wird man zur Vermeidung von Angriffen mit bekanntem Klartext auf Nichtlinearität setzen: Gleichungen höheren Grades sind sehr viel schwerer lösbar.

Bekannter Klartext ist der natürliche Feind der Linearität.

Autor: Klaus Pommerening, 3. Februar 2000; letzte Änderung: 1. Juli 2002.

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