Wolfgang K. Seiler
Tel. 2515

A5, C201

18. September 2007

2. Übungsblatt Kryptologie

Aufgabe 1: (*7 Punkte*)

Lester S. Hill (1891–1961) schlug 1929 folgende Blockchiffre vor: M sei die Menge der Zahlen von 1 bis 26 und werde wie üblich mit den Buchstaben des Alphabets identifiziert. Schlüssel ist eine Matrix $A \in M^{r\times r}$ sowie ein Vektor $\vec{b} \in M^r$, wobei r die Blocklänge bezeichnet. Ein Block $\vec{x} \in M^r$ wird verschlüsselt durch $\vec{y} = A\vec{x} + \vec{b}$, wobei alle Rechenoperationen modulo 26 so ausgeführt werden, daß die Ergebnisse wieder in M liegen. Zeigen Sie:

a) Falls $\det A = \pm 1$, ist die Verschlüsselung bijektiv.

b) Wie kann die Entschlüsselungsfunktion in der Form $\vec{x} = B\vec{y} + \vec{c}$ geschrieben werden?

c) Der Chiffretext „AIXOA JEBHR LQOMK“ wurde verschlüsselt mit

$$A = \begin{pmatrix} 1 & 3 & 4 \\ 1 & 2 & 2 \\ 0 & 8 & 15 \end{pmatrix} \quad \text{und} \quad \vec{b} = \begin{pmatrix} 2 \\ 3 \\ 7 \end{pmatrix} .$$

Ermitteln Sie den Klartext!

d) Wie ist die Hill-Chiffre unter den Shannonschen Forderungen nach Konfusion und Diffusion zu beurteilen?

Aufgabe 2: (*6 Punkte*)

Der Geheimdienst von Burkina Faso hat ein Kryptogramm der deutschen Botschaft an das Auswärtige Amt aufgefangen, von dem er annimmt, daß der Klartext mit den Worten „Botschaft Ouagadougou“ beginnt und daß es mit einer Hill-Chiffre der Blocklänge vier verschlüsselt ist. Die ersten zwanzig Buchstaben der Nachricht sind „PSOWX OLRQU ZEGGV NLWCH“. Bestimmen Sie den Schlüssel $(A, \vec{b})$!

Aufgabe 3: (*2 Punkte*)

Ein DES-Schlüssel kann auch dadurch spezifiziert werden, daß man eine Folge von acht (Groß- oder Klain-)Buchstaben oder Ziffern nimmt, deren ASCII-Codes (mit Prüfbit) dann als Schlüssel verwendet werden. Um welchen Faktor erleichtert es die Arbeit eines Gegners, wenn er an Stelle der Menge aller Schlüssel nur die der so darstellbaren Schlüssel durchsuchen muß?

Aufgabe 4: (*5 Punkte*)

a) Das 1-Komplement $\overline{x}$ eines Bitvektors x ist jener Vektor $\overline{x}$, bei dem alle Nullen durch Einsen und alle Einsen durch Nullen ersetzt sind. Zeigen Sie: Stellt man eine Zahl x zwischen 0 und 15 durch einen Vektor aus vier Bit dar, so ist $\overline{x}$ der Vektor zu $15 - x$.

b) Für DES gilt: $\mathrm{DES}(\overline{s}, \overline{x}) = \overline{\mathrm{DES}(s, x)}$.

c) DES-Cracker, eine speziell zum Knacken von DES entworfene Maschine, probiert systematisch alle Schlüssel durch und sondert alle aus, bei denen eines der acht Bytes des erhaltenen Klartexts nicht mit einem Nullbit beginnt. Wie kann man *a)* benutzen, um die Arbeit von DES-Cracker zu optimieren?

Abgabe bis zum Dienstag, dem 25. September 2007, um 12.00 Uhr