Angewandte diskrete Mathematik

Wintersemester 2008/2009
Barbara Baumeister
Jürgen Schütz

Freie Universität Berlin
Institut für Mathematik

Aufgabenblatt 8

Ausgabe: 9.12.2008

Abgabe: 16.12.2008

Aufgabe 29. — 4 Punkte

Sei $K = GF(7) = \{0, 1, \ldots, 6\}$ und $(a_1, a_2, \ldots, a_6) = (1, 2, \ldots, 6)$.

a) Berechne

$$H = \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_6 \\ a_1^2 & \cdots & a_6^2 \\ a_1^3 & \cdots & a_6^3 \end{pmatrix}$$

b) Bestimme die Parameter von $C = \{c \in K^6 : Hc^T = 0\}$.

c) Decodiere die Worte $(0, 2, 5, 0, 1, 1)$ und $(5, 2, 5, 0, 1, 0)$.

Aufgabe 30. — 4 Punkte

a) Es sei $YBTCLRQXCGR$ ein Chiffretext in der Caesar-Chiffre. Bestimme den Schlüssel und den Klartext.

b) Eine Blockchiffre mit Blocklänge n über einem Alphabet Σ ist ein Kryptosystem, bei dem sowohl der Klartext- als auch der Chiffretextraum Σ^n ist.
Wie viele Verschlüsselungsfunktionen kann eine Blockchiffre mit Alphabet $\{0, 1\}$ und Blocklänge n höchstens haben?

c) Finde ein Kryptosystem, bei dem die Verschlüsselungsfunktionen nicht surjektiv sind.

Aufgabe 31. — 4 Punkte

Die Permutationschiffre ist eine Blockchiffre mit Schlüsselraum S_n und Verschlüsselungsfunktionen $e_\pi : \Sigma^n \to \Sigma^n$ für $\pi \in S_n$ mit

$$e_\pi(v_1, \ldots, v_n) = (v_{\pi(1)}, \ldots, v_{\pi(n)}).$$

Eine Blockchiffre heißt linear, falls alle Verschlüsselungsfunktionen linear sind.

Zeige, dass die Permutationschiffre linear ist.

Aufgabe 32. 4 Punkte

Betrachte das folgende Kryptosystem: Alice wählt vier natürliche Zahlen a, a', b, b' und setzt $M = ab - 1$ und weiter

$$e = a'M + a, \quad d = b'M + b, \qquad n = \frac{ed - 1}{M} = a'b'M + ab' + a'b + 1.$$

Ihr öffentlicher Schlüssel ist nun (n, e), ihr privater Schlüssel ist d. Will nun Bob den Klartext $m \in \mathbb{Z}_n$ übermitteln, sendet er $c \equiv em \pmod{n}$. Zum Entschlüsseln multipliziert Alice den empfangenen Text mit d modulo n.

a) Zeige, dass Alice mit dieser Entschlüsselungsoperation wieder den Klartext erhält.

b) Wie kann Eve dieses Kryptosystem mit Hilfe des Euklidischen Algorithmus brechen.