Martin-Luther Universität Halle-Wittenberg
Fachbereich Mathematik und Informatik
Institut für Informatik

2. Übung zur Vorlesung „Datensicherheit“

Sommersemester 2005 — 13. April 2005

Abgabe: 25.04.2004 in der Übung

Aufgabe 2.1: (4+4 Punkte)

Programmieren Sie folgende Variante des EUKLIDschen Algorithmus. Für ganze Zahlen a, b werden iterativ folgende Tripel $W_i = (t_i, u_i, v_i)$ konstruiert

$$\begin{aligned} W_0 &= (a, 1, 0), \\ W_1 &= (b, 0, 1), \\ W_{i+1} &= W_{i-1} - q_{i+1} W_i, \quad q_{i+1} = t_{i-1} \text{ div } t_i \end{aligned}$$

und zwar bis zum Schritt j wo erstmals $t_j = 0$ eintritt.
Dann gelten für $d =$ ggT (a, b) folgende Aussagen

$$d = t_{j-1} \text{ und } d = u_{j-1} a + v_{j-1} b.$$

Die letztgenannte Gleichung heißt auch BEZOUT-Gleichung der Zahlen a, b.
Zusatz* : Beweisen Sie die Gültigkeit der BEZOUT-Gleichung mit Hilfe der vollständigen Induktion, indem Sie die Behauptung für beliebiges i verallgemeinern.

Aufgabe 2.2: (5 Punkte)

Gegeben Sei das Alphabet $\Sigma = \{a, b, c, \ldots, z, \sqcup, ?, !\}$ aus 29 Symbolen, das über $\mathbb{Z}_{29}$ codiert wird, wobei die 29 Symbole den fortlaufenden Restklassen $[0]_{29}, [1]_{29}, \ldots, [28]_{29}$ entsprechen.
Die folgende Botschaft

gfpyjp␣x?uyxstladplw,

wird abgefangen. Man kennt zusätzlich folgende Informationen:

(a) Es handelt sich um eine lineare Chiffrierung mit Blocklänge 2.

(b) Die letzten fünf Buchstaben entsprechen dem Klartextnamen „karla“ der Absenderin.

e-mail: {schenzel,pries}@informatik.uni-halle.de Web: http://www.informatik.uni-halle.de/∼{schenzel,pries}