Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 5
25. November 2015

Übungen zur Algorithmischen Zahlentheorie
Lösung

Aufgabe 19

a) Wir bestimmen zunächst die Schlüssel (A_1, B_1) und (A_2, B_2) aus den folgenden Gleichungen zur Basis 16

$$\begin{aligned}
\texttt{44} \oplus (A_1 \boxtimes \texttt{61} + B_1) &= \texttt{74} \\
\texttt{73} \oplus (A_1 \boxtimes \texttt{20} + B_1) &= \texttt{1D} \\
\texttt{61} \oplus (A_2 \boxtimes \texttt{74} + B_2) &= \texttt{DD} \\
\texttt{20} \oplus (A_2 \boxtimes \texttt{1D} + B_2) &= \texttt{E3}.
\end{aligned}$$

Wir erhalten $A_1 = 3, B_1 = 14, A_2 = 59, B_2 = 26$. Damit lässt sich der Klartext bestimmen.

```
Das Konzept des sog. Feistel-Netzwerks wurde in den 1970er Jahren von dem IBM-
Mitarbeiter Horst Feistel entwickelt
```

b) Wir verschlüsseln den Klartext

```
DC:=$4461_7320_4B6F_6E7A_6570_7420_6465_7320_736F_672E_2046_6569_7374_656C_
2D4E_6574_7A77_6572_6B73_2077_7572_6465_2069_6E20_6465_6E20_3139_3730_6572_
204A_6168_7265_6E20_766F_6E20_6465_6D20_4942_4D2D_4D69_7461_7262_6569_7465_
7220_486F_7273_7420_4665_6973_7465_6C20_656E_7477_6963_6B65_6C74
```

zu

```
09FF_54D3_565F_D745_0D1F_C7B2_4232_E575_60CA_10BF_33C7_6240_3DBB_E8C9_
4767_5965_D267_6AFA_6EA9_83E8_F52D_2477_F86C_5C64_8529_ADC2_A461_CE92_5607_
6083_1BCC_F661_9C49_566A_8CD4_7EF7_2482_6E21_0E11_F836_379E_0E45_68F9_B3FD_
4762_663A_66FD_60B1_D9AE_AA13_CBB1_5167_CA1D_33F5_D995_AB6E_AA9B
```