Übungszettel 12

Henning Lehmann, Darya Nemtsava

Afg. 12.1

a)

$ggT(14,9) = 1$ ✓

$14 = 1 \cdot 9 + 5$

$9 = 1 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

$4 = 4 \cdot \underline{1} + 0$

Gesucht: $a \cdot 14 + b \cdot 9 = 1$

$1 = 5 - 1 \cdot 4$

$= 5 - 1 \cdot (9 - 1 \cdot 5)$

$= -1 \cdot 9 + 2 \cdot 5$

$= -1 \cdot 9 + 2 \cdot (14 - 1 \cdot 9)$

$= 2 \cdot 14 - 3 \cdot 9$

$\Rightarrow a = 2, \; b = -3$

$\Rightarrow x = 2 \cdot 14 \cdot 3 + (-3) \cdot 9 \cdot 4 = 3 \cdot (2 \cdot 14 + (-9) \cdot 4)$

$= 6 \cdot (14 + (-18))$

$= \underline{-24}$

Kontrolle: $-24 \bmod 14 = 4$ ✓

$-24 \bmod 9 = 3$ ✓

b) Sei x Zahlenwert der gesuchten Karte.

Sei s_1 erste vom Zuschauer angegebene Spalte und s_2 die zweite.

Es gilt: $x \equiv s_1 \mod 8$, und

$x \equiv s_2 \mod 7$

Da 7, 8 teilerfremd: $x = a \cdot 8 \cdot s_2 + b \cdot 7 \cdot s_1$ mit $a \cdot 8 + b \cdot 7 = 1$

↳ $a = 1,\ b = -1$

$\Rightarrow x = 8 s_2 - 7 s_1 \mod 56$, da $x \in \{1, \dots, 56\}$

Da $7 \mid 56$ und $8 \mid 56$, erfüllt x obiges Kongruenzsystem

Test: sei gewählte Zahl 31.

↳ $s_1 = 7,\ s_2 = 3$

↳ $x = (8 \cdot 3 - 7 \cdot 7) \mod 56 = (24 - 49) \mod 56$

$= -25 \mod 56$

$= 31$ ✓

Afg. 12.2

$R = 18,\ E = 5,\ S = 19,\ T = 20$

$n = p \cdot q = 21,\ \varphi(n) = 2 \cdot 6 = 12$

Sei $e = 5$, $\text{ggT}(12, 5) = 1$

$1 = d \cdot e + h \cdot \varphi(n)$

$12 = 2 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$\Rightarrow 1 = 5 - 2 \cdot 2$

$= 5 - 2 \cdot (12 - 2 \cdot 5)$

$= -2 \cdot 12 + \underline{5} \cdot 5$

$d = 5$ Public Key = (21, 5)

Private Key = (21, 5)

$E(R) = 18^5 \mod 21 = 9$

$E(E) = 5^5 \mod 21 = 17$

$E(S) = 19^5 \mod 21 = 10$

$E(T) = 20^5 \mod 21 = 20$