Lösungen, 18.6.2018

76.) Reflexivität $A \leq_{eff} A$ sollte klar sein:

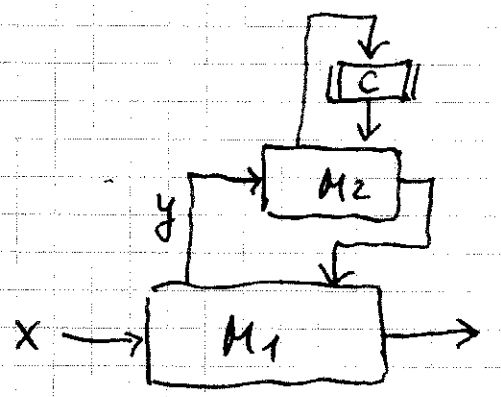
input x
frage Orakel A nach x; erhalte Lösung y
Gib y aus.

Transitivität: $A \leq_{eff} B$; $B \leq_{eff} C$ sei gegeben mittels Orakelmaschinen M_1 und M_2.

Zu zeigen ist $A \leq_{eff} C$. Das geht so:

input x
Starte Maschine M_1 bei Eingabe x;
Immer wenn M_1 eine Orakelfrage y an B stellt, starte stattdessen M_2 mit Eingabe y.
M_2 kann dabei Orakel C befragen.
Gib schließlich das Ergebnis von M_1 aus.

Skizze:



Die Kombination aus M_1 und M_2 stellt ebenfalls einen effiz. Algorithmus dar.
Also: $A \leq_{eff} C$

77.) Es gilt $m^{e \cdot d} \equiv m \pmod{n}$

Daraus folgt $m^{e \cdot d - 1} \equiv 1 \pmod{n}$

wobei hier $e \cdot d - 1 = 900 = 2^2 \cdot 225$

Wir erhalten mit $m = 4, 2, 3$:

$$4^{900} \bmod 77 = 1$$

$$4^{450} \bmod 77 = 1$$

$$4^{225} \bmod 77 = 1$$

Damit ergibt sich keine Faktorisierung von $n = 77$.

Aber mit $m = 2$:

$$2^{900} \bmod 77 = 1$$

$$2^{450} \bmod 77 = 1$$

$$2^{225} \bmod 77 = 43$$

$ggT(43-1, 77) = 7$, $ggT(43+1, 77) = 11$

Ebenso mit $m = 3$:

$$3^{900} \bmod 77 = 1$$

$$3^{450} \bmod 77 = 1$$

$$3^{225} \bmod 77 = 34$$

$ggT(34-1, 77) = 11$, $ggT(34+1, 77) = 7$

(Vgl. auch Aufgabe 72)

78.) Ausfüllen der Tabelle:

	0	⇓ 1	2	3	4	5	⇓ 6
0	0	15	30	10	25	5	20
⇒ 1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
⇒ 4	14	29	9	24	4	19	34

Es gilt „$\sqrt{1}$" ⟷ $(\pm 1, \pm 1)$

Das heißt, man muss $(1,1), (1,6), (4,1), (4,6)$ mittels Chin. Restsatz rücktransformieren. In der Tabelle kann man die 4 Lösungen 1, 6, 29, 34 ablesen.

79.) Exakte Rechnung: Wir experimentieren mit verschiedenen Werten für die (ungerade) Wiederholungszahl t. Für $\underline{\underline{t = 47}}$ erhalten wir

$$\sum_{i=0}^{\lfloor t/2 \rfloor} \binom{t}{i} \cdot (1-\varepsilon)^i \cdot (\varepsilon)^{t-i} < 0{,}01 \qquad (\text{wobei } \varepsilon = \tfrac{1}{3})$$

(Mit $t = 45$ klappt das noch nicht.)

Bei Verwenden der Abschätzung aus der Vorlesung müssen wir t so bestimmen, dass

$$\left(2 \cdot \sqrt{\varepsilon(1-\varepsilon)}\right)^t < 0{,}01$$

Dies ergibt $\underline{\underline{t = 79}}$.

80.)

	n Primzahl	$n = p \cdot q$	
Berechnen $\varphi(n)$	E	S	
$a^{n-1} \bmod n$	E	E	„square + multiply"
a Prim. wurzel	S	S	setzt Kenntnis der Faktorisierung von $n-1$ voraus
$a \in QR_n$	E	S	
$a^{-1} \bmod n$	E	E	Ext Euklid

81.) Alice könnte z.B. $x = 1, 2$ oder 3 wählen.
Dies ergibt $\tilde{x} = a^x \bmod n = 5, 2$ bzw. 10.
Damit ergibt sich $z = (\tilde{y})^x = 13, 8$ bzw. 12, wobei $\tilde{y} = 13$. Ferner ergibt sich $\tilde{m} = z \cdot m \bmod n = 15, 11, 5$.
Die möglichen Chiffren sind also $(\tilde{x}, \tilde{m}) =$ $(5, 15)$, $(2, 11)$ bzw. $(10, 5)$.

82.) Diffie-Hellman-Problem $\leq_{eff}$ El Gamal

Eingabe: $n, a, \tilde{x}, \tilde{y}$

Setze $\tilde{m} := 1$

Frage Orakel nach $n, a, \tilde{x}, \tilde{y}, \tilde{m}$ und erhalte Antwort m

Nun gilt: $\tilde{m} = 1 = m \cdot z$

Dann ist $z = m^{-1}$

Output z

El Gamal $\leq_{eff}$ Diffie-Hellman-Problem

Eingabe: $n, a, \tilde{x}, \tilde{y}, \tilde{m}$

Frage Orakel nach $n, a, \tilde{x}, \tilde{y}$ und erhalte Antwort z

$m := \tilde{m} \cdot z^{-1}$

Output m