Lösung XMAS → `"11_121_142_8"`

Musterlösung: RSA-Übung

1)

$p = 5$ und $q = 11$ → $N = p*q = 55$

→ $\varphi(N) = (q - 1)(p - 1) = 40$

→ *e* teilerfremd z.B. 7

→ <u>öffentlicher</u> Schlüssel *(e, N)* = (7, 55)

Nachricht $M = 8$ verschlüsseln nach $C = M^e \bmod N$

$= 8^7 \bmod 55 = 2$

(z.B. <u>wissenschaftlichen</u> Win-Rechner verwenden)

d ergibt sich aus dem multiplikative Inversen von *a* modulo *m:*

Variante 1 $b = a^{-1} \bmod m$, *also* $7^{-1} \bmod 40$

gleichbedeutend zu

$d*7 \bmod 40 = 1$

d.h., das Produkt *d*7* muss bei Division mit *40* den Rest *1* ergeben

dies wäre durch probieren bei 41, 81, 121, 161, … der Fall

davon ist 161 dividiert mit 7 ganzzahlig, nämlich 23

→ damit $d = 23$

oder *Variante 2* $d = \frac{n*\varphi(N)+\varphi(n)+1}{e}$ *für n = 3 ganzzahlig* → *d = 23*

2) $(e, N) = (11, 323)$

$(d, N) = (131, 323)$

Berechnung *d nach Variante 1*

Multiplikatives Inverses modulo einer Zahl *m*

Definition: Sind *a* und *m* zwei *teilerfremde* positive ganze Zahlen, so ist die multiplikative Inverse *b* zu *a* modulo *m* die eindeutig bestimmte positive Zahl $b < m$, welche die Gleichung $(b*a) \bmod m = 1$ erfüllt.

Suche das multiplikative Inverse durch Ausprobieren: Sei $a = 13$ und $m = 16$.
Wir suchen eine Zahl *b*, so dass $(13 \cdot b) \bmod 16 = 1$ ist.

$13 \cdot 2 \bmod 16 = 10$
$13 \cdot 3 \bmod 16 = 7$
$13 \cdot 4 \bmod 16 = 4$
$13 \cdot 5 \bmod 16 = 1$

Bsp.:

Wir suchen wieder eine positive Zahl $b < 160$, so dass $(13 \cdot b) \bmod 160 = 1$ gilt.

Zeile	Verfahren			Erläuterung
(I)	160	1	0	Dies steht für $\boxed{160} = \boxed{1} \cdot 160 + \boxed{0} \cdot 13$
(II)	13	0	1	Dies steht für $\boxed{13} = \boxed{0} \cdot 160 + \boxed{1} \cdot 13$
				Wie oft geht 13 in 160? 12 mal; also (III) = (I) − 12 · (II)
(III)	4	1	−12	Dies steht für $\boxed{4} = \boxed{1} \cdot 160 + \boxed{-12} \cdot 13$
				Wie oft geht 4 in 13? 3 mal; also (IV) = (II) − 3 · (III)
(IV):	$\boxed{1}$	−3	$\boxed{37}$	Dies steht für $\boxed{1} = \boxed{-3} \cdot 160 + \boxed{37} \cdot 13$

Das Verfahren hat jetzt in der ersten Spalte eine 1 erzeugt. Damit haben wir die multiplikative Inverse zu 13 mod 160 gefunden. Sie steht in der letzten Spalte des Verfahrens und lautet 37. Manchmal dauert es auch einige Schritte länger, bis die 1 in der ersten Spalte entsteht.

Für **unser** Beispiel *d*7 mod 40 = 1* bedeutet dies

I	40	=	1	*	40	+	0	*	7	
II	7	=	0	*	40	+	1	*	7	7 passt 5mal in 40 III = I - 5*II
III	5	=	1	*	40	+	-5	*	7	5 passt 1mal in 7 IV = II - 1*III
IV	2	=	-1	*	40	+	6	*	7	2 passt 2mal in 5 V = III - 2*IV
V	1	=	3	*	40	+	-17	*	7	

damit -17 mod 40 = 23 !!

Die beiden Beispiele geben ein eindeutiges Verfahren vor. Dies leitet zum neuen Themengebiet „Algorithmierung“ über.

Aufgabe: Formuliert diesen Algorithmus in verbaler Form.