KRY: Wahlfach Kryptologie
Serie 3: Chinesischer Restsatz, Attacken auf RSA

Aufgabe 1
Es sollen mit Hilfe von PARI/GP **Common Modulus Attacken** gerechnet werden. Bekannt sind dabei jeweils: Der (gemeinsame) Modulus m, Alice's öffentlicher Schlüssel e_2, sowie das eigene Schlüsselpaar d_1/e_1.

Rechnen Sie je mit den folgenden Angaben:

- $m = 91$, $e_1 = 5$, $d_1 = 29$, $e_2 = 7$. **Zugehöriges Ergebnis:** $d_2 = 103$.

v1 = 5*29-1=144
v2 = 7/(ggt(7,144)) = 7
=> x * e2 = 1 mod (v)
=> x * 7 = 1 mod (144)
=> x = 1/7 mod (144) = 103 = d2!

- $m = 221$, $e_1 = 5$, $d_1 = 269$, $e_2 = 35$. **Zugehöriges Ergebnis:** $d_2 = 11$.

v1=5*269-1=1344
ggt(35,1344)=7
v = 1344/7=192
=> x * 35 = 1 mod (192)

=> x = 11 = d2!

Aufgabe 2
Es soll mit Hilfe von PARI/GP eine **Low Exponent Attacke** für $e = 3$ durchgeführt werden. Bekannt sind dazu:

x = 2 mod 15
x = 6 mod 22
x = 121 mod 391

- die drei RSA-Module

$$m_1 = 15, m_2 = 22, m_3 = 391$$

,

M1 = 22 * 391 = 8602
M2 = 15 * 391 = 5865
M3 = 15 * 22 = 330

- die drei entsprechenden Chiffrate

$$c_1 = 2, c_2 = 6, c_3 = 121$$

.

u1 = 1/8602 mod 15 = 13
u2 = 1/5865 mod 22 = 17
u3 = 1/330 mod 391 = 141

x = 2 * (13*8602) + 6 * (17*5865) + 121 * (141*330) =

Wie lautet die gesendete Klartextnachricht?

x = 6452012 mod (15*22*391) = 512

t = x^(1/3) = 8

Aufgabe 3
Von einer Klasse mit n Personen weiss man, dass bei der Aufteilung in Zweiergruppen, Dreiergruppen, Vierergruppen jeweils eine Person übrigbleibt. Teilt man sie in Fünfergruppen, so bleiben sogar 2 übrig.

Bestimmen Sie n mit Hilfe des chinesischen Restsatzes, wenn man weiss, dass die Klasse weniger als 60 Leute hat.

x mod 60

n = 1 mod 2
n = 1 mod 3
n = 1 mod 4
n = 2 mod 5

M1 = 4*5 = 20
M2 = 3*5 = 15
M3 = 3*4 = 12

U1 = 1/20 mod 3 = 2
U2 = 1/15 mod 4 = 3
U3 = 1/12 mod 5 = 3

1*20*2 + 1*15*3 + 2*12*3 = 40+45+72 = 157 mod 3*4*5 = 37!

Lösung: n = 37