3) Elgamal

gpg.: $\mathbb{Z}_{23}^* = \{1, 2, \dots, 22\}$, $g = 5$

a)

Alice: $x = 11$ (sk)

$pk := (G, g, X) = (\mathbb{Z}_{23}^*, 5, 22)$

$X = g^x = 5^{11} \bmod 23 = 22$

b)

Bob: $m = 19$, $y = 3$, $pk := (\mathbb{Z}_{23}^*, 5, 22)$

$c = (c_1, c_2)$

$c_1 = Y = g^y \bmod 23 = 10$

$c_2 = X^Y \cdot m = (22^3 \bmod 23) \cdot 19 = 418$

$c = (10, 418)$

c)

Inverse von $c_1^x \bmod 23$ ist $c_1^{22-x} \bmod 23$

$\Rightarrow c_1^x \cdot c_1^{22-x} \pmod{23} = 1 \bmod 22$

$c_1^{x+22-x} \bmod 23 = 1 \bmod 22$

$c_1^{22} \bmod 23 = 1 \bmod 22$

$10^{22} \bmod 23 = 1 \bmod 22$ ✓ w.A.

d) Elgamal cfd.

Alice bekommt $c = (10, 418)$

$k = c_1^{sk} = y^x = g^{xy} = 10^{11} \bmod 23 = 22$

laut c) ist $k^{-1} = 10^{22-11} = 10^{11} \bmod 23 = 22$

$m = 418 \cdot 22 \pmod{23} = 19$

(c_2, k^{-1})