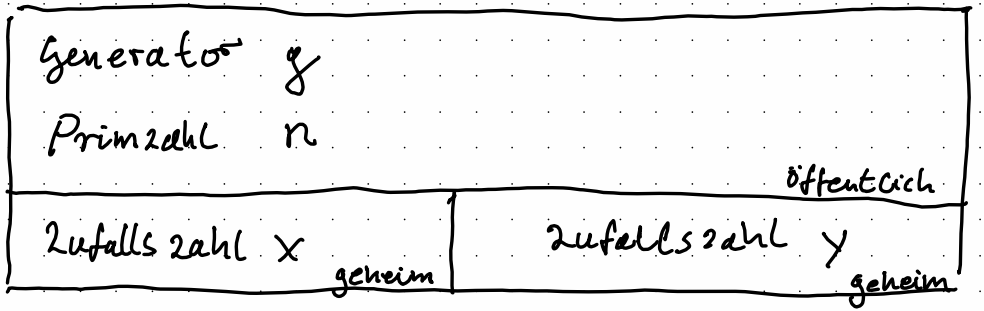
festlegen:



Alice: $X = g^x \bmod n$

Bob: $Y = g^y \bmod n$

Shared Key

$k = Y^x \bmod n$

$k = X^y \bmod n$

$g = 23$

$n = 13$

$x = 4$

$X = 23^4 \bmod 13 = 3$

$k = 12^4 \bmod 13 = 1$

$y = 9$

$Y = 23^9 \bmod 13 = 12$

$k = 3^9 \bmod 13 = 1$

Beweis:

$$k \equiv X^y \equiv g^{x^y} \equiv g^{x \cdot y} \equiv g^{y^x} \equiv Y^x \pmod{n}$$