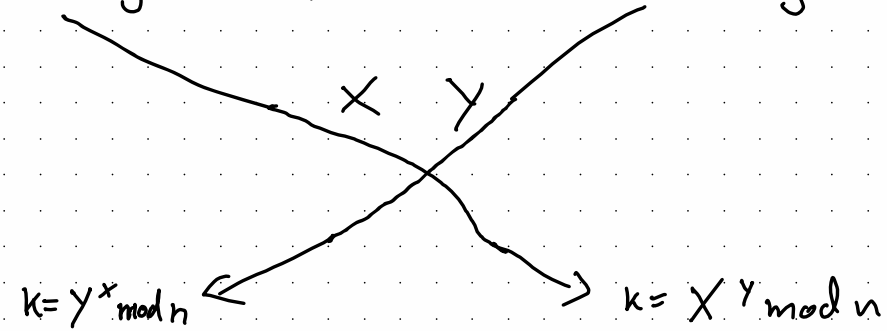
# Diffie - Hellman

festlegen:

| | | |
|---|---|---|
| Generator $g$ | | öffentlich |
| Primzahl $n$ | | |
| Zufallszahl $x$ (geheim) | Zufallszahl $y$ (geheim) | |
| Alice | Bob | |

Alice: $X = g^x \bmod n$ Bob: $Y = g^y \bmod n$




Shared key = Shared key

Beispiel:

$n = 13$ ← prime

$g = 7$ ← sollte $< n$ sein, im idealfall primitiv Wurzel

= geheim

$x = 4$

$X = 7^4 \bmod 13 = 9$

$y = 9$

$Y = 7^9 \bmod 13 = 8$

$k = 8^4 \bmod 13 = 1$

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

Beweis:

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

$$k = X^y \bmod n = g^{x^y} \bmod n = g^{y^x} \bmod n = Y^x \bmod n$$

# Diffie Hellman

- sicheres (asymetrisches) Schlüsselaustauschverfahren
- kann benutzt werden um den Schlüssel einer symetrischen Crypto auszutauschen

- Schwierige Umkehrfunktion:

$$x = \log(X) \bmod n \quad \text{oder} \quad k = g^{xy} \bmod n$$

(diskreter Logaritmus)

- Sicherheit durch große Zahlen
  Größe von $x$ und $y > 4096$