

festlegen:

generator g	
Primzahl n	
Zufallszahl x geheim	Zufallszahl y öffentlich

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

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

Shared Key

$k = Y^x \bmod n$

$k = X^y \bmod n$

$$g = 23$$

$$n = 13$$

$$x = 4$$

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

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

$$y = 5$$

$$Y = 23^5 \bmod 13 = 12$$

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

Beweis:

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