

Diffie - Hellman

festlegen:

Generator g	
Primzahl n	
öffentlich	
Zufallszahl x	Zufallszahl y
geheim	geheim
Alice	Bob

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

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

The diagram illustrates the exchange of values X and Y between Alice and Bob. Two curved arrows cross each other: one from X to Bob's calculation and one from Y to Alice's calculation. Below the crossing, the shared key is calculated as $K = Y^x \bmod n$ on the left and $K = X^y \bmod n$ on the right. These two expressions are equated with a double equals sign, and both are labeled "Shared key".

$$K = Y^x \bmod n = K = X^y \bmod n$$

Shared key

Beispiel:

$$n = 13 \leftarrow \text{prime}$$

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

= geheim

$$x = 4$$

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

$$y = 3$$

$$Y = 7^3 \bmod 13 = 8$$

$$K = \underbrace{8^4}_{X^Y} \bmod 13 = \underline{\underline{1}}$$

$$K = \underbrace{7^9}_{Y^X} \bmod 13 = \underline{\underline{1}}$$

Beweis:

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

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

Diffie Hellman

- sicheres (asymmetrisches) Schlüsselaustauschverfahren
- kann benutzt werden um den Schlüssel einer symmetrischen Crypto auszutauschen
- Schwierige Umkehrfunktion:

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

(diskreter Logarithmus)

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