

prime : $p = 2357$
 gen : $d = 2$

Alice (secret key $a = 1751$)

public key:

$$pk_A = 1185 (= d^a \bmod p)$$

pk_A, p, d →

Bob (secret key $k = 1520$)

will $m = 2035$ senden

temp. key

$$\begin{aligned} k_E &= pk_B = d^k \bmod p \\ &= 2^{1520} \bmod 2357 \\ &= 1930 \end{aligned}$$

session key

$$\begin{aligned} k_M &= pk_A^k \bmod p \\ &= 1185^{1520} \bmod 2357 \\ &= 2089 \end{aligned}$$

Cyphertext

$$\begin{aligned} \gamma &= m \cdot k_M \bmod p \\ &= 2035 \cdot 2089 \bmod 2357 \\ &= 697 \end{aligned}$$

←

$$\begin{aligned} k_M &= k_E^a \bmod p \\ &= 1930^{1751} \bmod 2357 \\ &= 2089 \end{aligned}$$

$$\begin{aligned} m &= k_M^{-1} \cdot \gamma \bmod p \\ &= 2089^{-1} \cdot 697 \bmod 2357 \\ &= \text{geht nicht?!} \end{aligned}$$