A10

A10:
a. Alice und Bob vereinbaren die Primzahl p und die Primitivwurzel g. Alice wählt a, Bob wählt b. Welche Zahlen werden veröffentlicht und wie heißt der gemeinsame Schlüssel?
a. p = 7, g = 3, a = 3, b = 4.
b. p = 23, g = 7, a = 15, b = 17.

a.

Alice: $g^a \equiv 3^3 \equiv 27 \equiv 6 \bmod 7 \Rightarrow A = 6$

Bob: $g^b \equiv 3^4 \equiv 9 \cdot 9 \equiv 2 \cdot 2 \equiv 4 \bmod 7 \Rightarrow B = 4$

öffentlich: A B p g

de

gemeinsame Schlüssel: $K \equiv B^a \bmod p$

$K \equiv 4^3 \bmod 7 \equiv 16 \cdot 4 \equiv 2 \cdot 4 \equiv 1 \bmod 7 \Rightarrow K = 1$

b.

Alice: $g^a \equiv 7^{15} \bmod 23$ $\quad 15 = (1111)_2$

$7^1 \equiv 7$
$7^2 \equiv 49 \equiv 3$
$7^4 \equiv 9$
$7^8 \equiv 81 \equiv 12$

$7^{15} \equiv \underbrace{7 \cdot 3 \cdot 9}_{5} \cdot \underbrace{12}_{4} \equiv 60 \equiv 14$

$\Rightarrow A = 14$

Bob: $g^b \equiv 7^{17}$ $\quad 7^{17} \equiv 7^{15} \cdot 7^2 \equiv 14 \cdot 3 \equiv 42 \equiv 19$

$\Rightarrow B = 19$

gemeinsamer Schlüssel: $K \equiv B^a \equiv 19^{15}$

$19^1 \equiv 19 \equiv -4$
$19^2 \equiv 16 \equiv -7$
$19^4 \equiv 49 \equiv 3$
$19^8 \equiv 9$

$19^{15} \equiv \underbrace{(-4)(-7)}_{5} \cdot \underbrace{3 \cdot 9}_{4} \equiv 20$