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) $A \equiv 3^3 \mod 7$
$\equiv 27 \equiv 6$

$B \equiv 3^4 \equiv 6 \cdot 3 \equiv 18 \equiv 4 \mod 7$

öffentlich: A B p g

$K \equiv 4^3 \mod 7$
$\equiv 16 \cdot 4 \equiv 2 \cdot 4 \equiv 1$ gemeinsamer Schlüssel

b) $A \equiv 7^{15} \mod 23$

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

$7^1 \equiv 7 \mod 23$
$7^2 \equiv 49 \equiv 3$
$7^4 \equiv 9$
$7^8 \equiv 81 \equiv 12$

$B = 7^{17} \mod 23$
$\equiv 7^{15} \cdot 7^2 \equiv 14 \cdot 49 \equiv 14 \cdot 3 \equiv 19$

p. g. A und B werden veröffentlicht

$K \equiv 19^{15} \equiv 28 \cdot 3 \cdot 9 \equiv 5 \cdot 4 \equiv 20$

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