A11

A11:
Alice und Bob vereinbaren p = 11 und g = 2. Alice schicht an Bob A = 5 und Bob meldet an Alice B = 8. Da die Zahlen klein sind, kann die Diffie-Hellman Verschlüsselung geknackt werden. Wie heißt der Schlüssel K?

	1	2	3	4	5	6	7	8	9	10
2^x mod 11	2	4	8	5	10	9	7	3	6	1

Alice: $g^a \equiv A \mod 11$ $\quad 2^a \equiv 5 \mod 11$

Tabelle: $a = 4$

$K \equiv B^a \equiv 8^4 \mod 11$

$\equiv 4 \mod 11$

$8^1 \equiv 8 \equiv -3 \mod 11$

$8^2 \equiv 9 \equiv -2$

$8^4 \equiv 4$

$K = 4$