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. Nutze die Tabelle. Wie heißt der Schlüssel K?

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

Tabelle: $a = 4$

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

$\equiv 4 \mod 11$

$K = 4$

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

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

$8^4 \equiv 4$

$\mathbb{Z}_{11}$

Spalte hoch Zeile

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	1	4	9	5	3	3	5	9	4	1
3	1	8	5	9	4	7	2	6	3	10
4	1	5	4	3	9	9	3	4	5	1
5	1	10	1	1	1	10	10	10	1	10
6	1	9	3	4	5	5	4	3	9	1
7	1	7	9	5	3	8	6	2	4	10
8	1	3	5	9	4	4	9	5	3	1
9	1	6	4	3	9	2	8	7	5	10
10	1	1	1	1	1	1	1	1	1	1