Aufgabe Diffie-Hellman-Schlüsselvereinbarung

Öffentliche Daten

p = 23 g= 9

Geheim a=15 Anton berechnet: $\alpha = g^{15} \equiv_{23} 6$	Geheim b= 17 Berta berechnet: $\beta = g^{17} \equiv_{23} 3$
Anton bekommt von Berta 3	Berta bekommt von Anton 6
Anton berechnet: $3^{15} \equiv_{23} 12$	Berta berechnet: $6^{17} \equiv_{23} 12$

Tipp: Sie können das in mehreren Schritten berechnen: Z.B.

$x \equiv_{23} g^5 \equiv_{23} 8$ $\alpha \equiv_{23} x^3 \equiv_{23} 6$ $\beta \equiv_{23} \alpha \cdot g^2 \equiv_{23} 3$ $6^7 \equiv_{23} 3$ $6^{10} \equiv_{23} 4$

Anmerkung: in der Klausur sind die Zahlen kleiner!!!!!!

Der Angriff von Mister X
Öffentliche Daten

p = 19 g= 13

Geheim a=?????? $a = 7$ Anton berechnet: $\alpha = 13^a \equiv_{19} 10$	Geheim b= ????? $b = 11$ Berta berechnet: $\beta = 13^b \equiv_{19} 2$
Anton bekommt von Berta $\beta = 2$	Berta bekommt von Anton $\alpha = 10$
Anton berechnet: $2^7 \equiv_{19} 14$	Berta berechnet: $10^{11} \equiv_{19} 14$

Mister X zapft die Leitung an, mit der Anton und Berta kommunizieren. Er weiß nun die vier angegebenen Zahlen. p=19, g=13, α=10 ,β= 2.

Um nun an a und b heranzukommen, muss er den "modularen Logarithmus" bestimmen. Da bleibt ihm nichts anderes übrig, als unter den Potenzen von 13 modulo 19 zu suchen.
Die Liste dieser Potenzen ist : 13, 17, 12, 4, 14, 11, 10, 16, 18, 6, 2, 7, 15, 5, 8, 9, 3, 1

(1) (7) (11)

Was sind nun also a und b und welches ist der Schlüssel, den sich Mister X nun beschafft hat?

Warum hat Mister X in den wahren kryptografischen Anwendungen keine effektive Chance, sich den Schüssel auf diese Weise zu beschaffen?

Weil p und g etwa 200 Stellen haben, kann er die Liste der Potenzen nicht herstellen, sie hat 10^{200} Einträge.