Aufgabe Diffie-Hellman-Schlüsselvereinbarung

 Anton	Öffentliche Daten p = 23 g= 9	 Berta
Geheim a=15 Anton berechnet:		Geheim b= 17 Berta berechnet:
Anton bekommt von Berta		Berta bekommt von Anton
Anton berechnet:		Berta berechnet:

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

$x \equiv_{23} g^5$ $\alpha \equiv_{23} x^3$ $\beta \equiv_{23} \alpha \cdot g^2$

 Anton	Der Angriff von Mister X Öffentliche Daten p = 19 g= 13	 Berta
Geheim a=?????? Anton berechnet: $\alpha = 13^a \equiv_{19} 10$		Geheim b= ????? Berta berechnet: $\beta = 13^b \equiv_{19} 2$
Anton bekommt von Berta $\beta =$ 2		Berta bekommt von Anton $\alpha = 10$
Anton berechnet:		Berta berechnet:

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

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?