

Hilfen zur Bearbeitung:

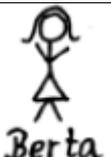
Aufgabe Diffie-Hellman-Schlüsselvereinbarung

Öffentliche Daten	
 Anton	 Berta
$p = 23$	$g = 9$
Geheim $a=15$ Anton berechnet: $\alpha = 9^{15} \equiv 6 \pmod{23}$	Geheim $b=17$ Berta berechnet: $\beta = 9^{17} \equiv 3 \pmod{23}$
Anton bekommt von Berta 3	Berta bekommt von Anton 6
Anton berechnet: $3^{15} \equiv 12 \pmod{23}$	Berta berechnet: $6^{17} \equiv 12 \pmod{23}$

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

$$\begin{aligned}
 & x \equiv 9^5 \equiv 8 \pmod{23} & \alpha & \equiv x^3 \equiv 6 \pmod{23} & \beta & \equiv \alpha \cdot 9^2 \equiv 3 \pmod{23} & 6^7 & \equiv 3 \pmod{23} \\
 & & & & & & 6^{10} & \equiv 4 \pmod{23}
 \end{aligned}$$

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

Der Angriff von Mister X Öffentliche Daten	
 Anton	 Berta
$p = 19$	$g = 13$
Geheim $a=?????$ $a=7$ Anton berechnet: $\alpha = 13^a \equiv 10 \pmod{19}$	Geheim $b=?????$ $b=11$ Berta berechnet: $\beta = 13^b \equiv 2 \pmod{19}$
Anton bekommt von Berta $\beta = 2$	Berta bekommt von Anton $\alpha = 10$
Anton berechnet: $2^7 \equiv 14 \pmod{19}$	Berta berechnet: $10^{11} \equiv 14 \pmod{19}$

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

 Um nun 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 Schlüssel auf diese Weise zu beschaffen?

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