Pohlig-Hellman - Exam April 2015 - 2b

We have $\mathbb{F}_{337}^*$. With $g = 19$ with order 336. The public key is $g_c = 123$.

First we factor 336:

```
factor(336)
```

```
[2 4]

[3 1]

[7 1]
```

Thus, we have $336 = 2^4 + 3 + 7$.

We now want to calculate:

$$\begin{aligned} x_2 &\equiv x \mod 2^4 \\ x_3 &\equiv x \mod 3 \\ x_7 &\equiv x \mod 7 \end{aligned}$$

We start with $x_2 = c_0 + 2 \cdot c_1 + 4 \cdot c_2 + 8 \cdot c_3$, with $c_0, c_1, c_2, c_3 \in \{0, 1\}$.

For c_0, c_1, c_2, c_3 we solve:

$$\begin{aligned} 123^{168} &= 19^{c_0 \cdot 168} \\ 1 &= 336^{c_0} \Rightarrow c_0 = 0 \end{aligned}$$

$$\begin{aligned} 123^{84} &= 19^{c_1 \cdot 168} \\ 336 &= 336^{c_1} \Rightarrow c_1 = 1 \end{aligned}$$

$$\begin{aligned} 123^{42} &= 19^{c_0 \cdot 168} \\ 336 &= 336^{c_2} \Rightarrow c_2 = 1 \end{aligned}$$

$$\begin{aligned} 123^{21} &= 19^{c_0 \cdot 168} \\ 336 &= 336^{c_3} \Rightarrow c_3 = 1 \end{aligned}$$

Thus, $x_2 = 0 + 2 \cdot 1 + 4 \cdot 1 + 8 \cdot 1 = 14$

Now x_3, we solve:

$$\begin{aligned} 123^{336/3} &= 19^{x_3 \cdot 112} \\ 1 &= 128^{x_3} \Rightarrow x_3 = 0 \end{aligned}$$

Now x_7, we solve:

$$\begin{aligned} 123^{336/7} &= 19^{x_3 \cdot 48} \\ 295 &= 79^{x_7} \Rightarrow x_7 = 4 \end{aligned}$$

Thus, we get:

$$\begin{aligned} 14 &\equiv x \mod 2^4 \\ 0 &\equiv x \mod 3 \\ 4 &\equiv x \mod 7 \end{aligned}$$

Which we solve using the chinese remainder theorem:

```
chinese([Mod(14,16), Mod(0,3), Mod(4,7)])
```

```
Mod(270, 336)
```

```
Mod(19^270,337)
```

```
Mod(123, 337)
```

Which gives us $123 \equiv 19^{270} \mod 337$.