

ECE 6280 - Project

Full name : WILD Adam

gtid : 903343514

Due date : Friday, December 15, 2017

Code : github.com/adamwild/ECE6280

We want to solve $\beta = \alpha^a$. We have $\alpha = 2317547 = m * n = 139 * 16673$ and 139 is a primitive element. The problem is therefore the following :

$$\beta = \alpha^a = m^a . n^a \Leftrightarrow \log_m \beta = a(\log_m m + \log_m n) = a(1 + \log_m n)$$

To solve the problem we need to find $\log_m \beta = \log_{139}(4867455)$ and $\log_m n = \log_{139}(16673)$

By running `get_factored(4867455, p, 139, factor_b)`, we get $\beta.p^s = 4867455.139^{65} = 307200 = 2^{12}3^{15}5^2$.
Therefore $\log_{139}(4867455) = 12.\log_{139}(2) + \log_{139}(3) + 2.\log_{139}(5) - 65[p - 1]$

By running `get_factored(16673, p, 139, factor_b)`, we get $\beta.p^s = 16673.139^{2134} = 243000 = 2^33^55^3$.
Therefore $\log_{139}(16673) = 3.\log_{139}(2) + 5.\log_{139}(3) + 3.\log_{139}(5) - 2134[p - 1]$

By running `compute_numbase(139, p, factor_b)`, we get the following system :

$$\begin{bmatrix} 3 & 1 & 6 \\ 3 & 9 & 1 \\ 1 & 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} \log_{139}(2) \\ \log_{139}(3) \\ \log_{139}(5) \end{bmatrix} = \begin{bmatrix} 37419 \\ 48349 \\ 57952 \end{bmatrix}$$

By running `invmatmod.py`, we get the following results :

$$\begin{bmatrix} \log_{139}(2) \\ \log_{139}(3) \\ \log_{139}(5) \end{bmatrix} = \begin{bmatrix} 3 & 1 & 6 \\ 3 & 9 & 1 \\ 1 & 2 & 4 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 37419 \\ 48349 \\ 57952 \end{bmatrix} = \begin{bmatrix} 1197906 & 9283768 & 1347643 \\ 898429 & 1497382 & 3743455 \\ 10182197 & 2395811 & 5989528 \end{bmatrix} \cdot \begin{bmatrix} 37419 \\ 48349 \\ 57952 \end{bmatrix} = \begin{bmatrix} 130390 \\ 2855269 \\ 6752422 \end{bmatrix}$$

That is :

$$\begin{cases} \log_{139}(2) = 130390 \\ \log_{139}(3) = 2855269 \\ \log_{139}(5) = 6752422 \end{cases}$$

Therefore :

$$\begin{cases} \log_{139}(4867455) = 12.\log_{139}(2) + \log_{139}(3) + 2.\log_{139}(5) - 65[p - 1] = 6993840 \\ \log_{139}(16673) = 3.\log_{139}(2) + 5.\log_{139}(3) + 3.\log_{139}(5) - 2134[p - 1] = 2129983 \end{cases}$$

The problem we need to solve is then :

$$\begin{aligned} \beta = \alpha^a &\Leftrightarrow \beta = m^a . n^a \\ &\Leftrightarrow \log_m \beta = a(1 + \log_m n) \\ &\Leftrightarrow 6993840 = a(1 + 2129983)[p - 1] \\ &\Leftrightarrow a = 41192 \end{aligned}$$

We can check the final result, we have :

$$\alpha^a = 2317547^{41192} = 4867455[10930889] = \beta[p]$$