resitev

January 28, 2024

1 Day 25: Combo Breaker

(Povezava na nalogo)

V bistvu je bilo potrebno razbiti Diffie-Hellmanov postopek izmenjave ključev za podano bazo, modul in javne ključe.

Za kaj gre, si lahko preberemo v originalni nalogi ali na Wikipediji. Izračunati je potrebno diskretni logaritem in nato potenco z modulom. Diskretni logaritem moramo sprogramirati sami in ker številke niso prevelike, deluje hitro. Potenciranje z modulom pa Python že ima: funkcija `pow(x, y, m)` vrne `x ** y % m`, le da to izračuna hitrejše, kot če bi najprej računala potenco in potem ostanek. Rešitev je torej:

[7]:
```
from itertools import count

def disc_log(base, x, m):
    n = 1
    for y in count():
        if n == x:
            return y
        else:
            n = (n * base) % m

m = 20201227
d = disc_log(7, 5764801, m)
print(pow(17807724, d, m))
```

```
14897079
```