Opa Wichtel hat noch eine Amateurfunk Station und schnappt einen verschlüsselten Funkspruch auf. Die Übertragung könnte interessant sein. Opa Wichtel hat die Zahlen 212919 notiert.

Ihr vermutet, dass die Nachricht an den Grinch addressiert ist. Sein öffentlicher Schlüssel ist bekannt und lautet $(e, N) := (5, 3548669)$.

Tipps:

- Grinch hat den Verschlüsselungsexponenten 5 (und nicht 3) gewählt, weil 5 seine Lieblingszahl ist. (Und nicht etwa, weil Aaron erst um 2 in der Nacht gemerkt hat dass 3 und $\varphi(N)$ nicht teilerfremd sind)
- Wolfram Alpha faktorisiert diese Zahl immer noch instant
- Wenn du andere Tipps geben willst: Es wird vermutet das Grinch ein Fan der Amerikanischen Unabhängigkeit ist. Daraus könnte man folgern: eine Primzahl ist 1777, es ist nämlich die nächste Primzahl zu 1776.
- Die andere Primzahl ist 1997. Damit kann man vielleicht auch was tipsen.
- Es gibt Online-Rechner, um modulare inverse zu berechnen.

Lösung:

- $\phi(N) = (p-1)(q-1) = 3544896$
- Modulares Inverses von 5 mod $\varphi(N)$ ist 2835917
- $212919^{2835917} \equiv 3224624 \pmod{N}$
- `212919**2835917 % 3548669` dauert schon ein bisschen in Python hihi
- In binär $01100010011010000110000_2$
- oder die Buchstaben 1, 4, 0