Zadání domácí úlohy na příklady z 5. týdne.

V tabulce

`https://docs.google.com/spreadsheets/d/1wE4jrBFOajWdrAA8bdBIZ_HutiMEDSoI2zcUeF_DTl0/edit?usp=sharing`

najdete u svého jména 3 čísla p, q, e, která jsou použita v zadání.

1. V šifrovacím systému RSA s veřejným klíčem skládajícím se z modulu n a exponentu e došlo k prozrazení faktorizace $n = p \cdot q$ na součin prvočísel. S její pomocí dešifrujte zprávu $c \equiv 21 \pmod{p \cdot q}$. Při výpočtu mocniny $c^d \pmod{p \cdot q}$ počítejte zvlášť modulo p a modulo q a tyto mezivýsledky pak dejte dohromady (jako v posledním příkladu ze cvičení).