

## Zadání domácí úlohy na příklady z 6. týdne.

V tabulce

[https://docs.google.com/spreadsheets/d/16YU1-X\\_savAf3n1kMhr98FHP\\_Z894fia7Fg3Ju--jII/edit?usp=sharing](https://docs.google.com/spreadsheets/d/16YU1-X_savAf3n1kMhr98FHP_Z894fia7Fg3Ju--jII/edit?usp=sharing)

najdete u svého jména čísla  $p$ ,  $g$ ,  $g^x$ ,  $y$ ,  $g^y$ ,  $c$  která jsou použita v zadání.

1. V ElGamalově šifrovacím systému si Alice zvolila veřejný klíč sestávající z prvočísla  $p = 997$ , primitivního kořene  $g$  a jeho mocniny  $g^x$  (kde exponent  $x = 23$  je soukromý). Bob si pro komunikaci s Alicí zvolil soukromý klíč  $y = 25$  a poslal jí svůj veřejný klíč  $g^y$ . Pomocí společného soukromého klíče  $g^{xy}$  pak zašifroval zprávu  $m$  a výslednou zprávu  $c$  poslal Alici. Jak ji bude Alice dešifrovat?