12. domácí úloha z MB141, jaro 2020

Příklad. 1. Šifrou RSA s veřejným klíčem $n = 133$ a $e = 49$ bylo posláno číslo $Z = 43$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 132\}$.

Příklad. 2. Alice a Bob komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 53$ a na primitivním kořenu $g = 10$. Alice si za svůj tajný klíč zvolila číslo 11. Ověřte, že 4104 je skutečně primitivní kořen modulo 53. Jaký údaj poskytla Alice Bobovi? Bob jí posléze poslal zprávu $(24, 7)$. Pomozte Alici s dešifrováním zprávy.

Příklad. 3. V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 19$ a $q = 31$. Veřejným klíčem je součin $n = pq = 589$. Zašifrujte zprávu $M = 327$ a ukažte, jak se bude dešifrovat.