12. cvičení z MB141, jaro 2020

Příklad. 1. Šifrou RSA s veřejným klíčem $n = 95$ a $e = 55$ bylo posláno číslo $Z = 42$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 94\}$.

Příklad. 2. Šifrou RSA s veřejným klíčem $n = 115$ a $e = 15$ bylo posláno číslo $Z = 47$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 114\}$.

Příklad. 3. Alice a Bob komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 41$ a na primitivním kořenu $g = 11$. Alice si za svůj tajný klíč zvolila číslo 10. Jaký údaj poskytla Bobovi? Bob jí posléze poslal zprávu $(22, 6)$. Pomozte Alici s dešifrováním zprávy.

Příklad. 4. V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 23$ a $q = 31$. Veřejným klíčem je součin $n = pq = 713$. Zašifrujte zprávu $M = 327$ a ukažte, jak se bude dešifrovat.