ZKRY 2024: Sada uloh 5

Instrukcie:

- Vyrieste nizsie uvedene ulohy a vase riesenia odovzdajte do im prisluchajucich miest odovzdania v AISe do 28.10. do 23:59.

Uloha 1:
Vyrieste Problem 7.1 na strane 235 v knihe.

Uloha 2:
Vyrieste Problem 7.2.3 na strane 235 v knihe. To znamena, ze mate pouzit square-and-multiply algoritmus na vypocet $x^e \mod m$. Pre nasledujuce hodnoty:
$x = 5$
$e = 54$
$m = 151$

Uloha 3:
Vyrieste Problem 7.3.2 na strane 235 v knihe. To znamena, ze mate vykonat sifrovanie a desifrovanie pomocou RSA s nasledujucimi hodnotami:
$p = 5$
$q = 11$
$e = 3$
$x = 9$

Uloha 4:
Vyrieste Problem 7.7 na strane 236 v knihe.