ZKRY 2024: Sada uloh 7

Instrukcie:

- Vyrieste nizsie uvedene ulohy a vase riesenia odovzdajte do im prisluchajucich miest odovzdania v AISe do 11.11. do 23:59.

Uloha 1:
Vyrieste Problem 8.5.1 na strane 271 v knihe. To znamena, ze mate vypocitat zdielany kluc k_{AB} v DHKE scheme s nasledujucimi hodnotami:
$p = 467$
$\alpha = 2$
$a = 3$
$b = 5$

Uloha 2:
Vyrieste Problem 8.7 na strane 271 v knihe.

Uloha 3:
Vyrieste Problem 8.13.1 na strane 272 v knihe. To znamena:
a) Zasifrujte spravu $x=33$ pomocou Elgamalovho kryptosystemu s hodnotami:
$p = 467$
$\alpha = 2$
$k_{pr} = d = 105$
$i = 213$
b) Vysledny ciphertext nasledne desifrujte.