

ZKRY 2024: Sada uloh 9

Instrukcie:

- Vyrieste nizsie uvedene ulohy a vase riesenia odovzdajte do im prisluchajucich miest odovzdania v AISE do 25.11. do 23:59.

Uloha 1:

Vyrieste Problem 10.2 na strane 331 v knihe.

Uloha 2:

Vyrieste Problem 10.4.1 na strane 331 v knihe. To znamena, ze mate vykonat podpisovanie a overovanie podpisu pomocou RSA s nasledujucimi hodnotami:

$$n = 2183$$

$$e = 97$$

$$d = 409$$

$$x = 55$$

Na vykonanie potrebnych vypoctov mozete pouzit lubovolny softver. Napriklad mozete pouzit SageMath (<https://www.sagemath.org/>). Vo vasom rieseni uvedte vsetky vypocty, ktore ste pomocou softveru vykonali, spolu s vysledkami, ktore vam softver pre spominane vypocty dal.

Uloha 3:

Vyrieste Problem 11.6 na strane 375 v knihe. Okrem vysledkov odovzdajte aj screenshoty vasich programov.