ZKRY 2024: Sada uloh 3

Instrukcie:

- Vyrieste nizsie uvedene ulohy a vase riesenia odovzdajte do im prisluchajucich miest odovzdania v AISe do 7.10. do 23:59.

Uloha 1:
Vyrieste Problem 4.6 na strane 143 v knihe. Vo vasom rieseni mozete na urcenie multiplikativne inverzneho prvku pouzit tabulku 4.2 v knihe. (Cielom tejto ulohy je, aby ste si osviezili aritmetiku v poli GF(2^8) a aby ste si zvykli na to, ze nasobenie prvkom a^{-1} sa niekedy zapisuje ako delenie prvkom a .)

Uloha 2:
Predpokladajme, ze chceme zasifrovat 128-bitovy plaintext x sifrou AES so 128-bitovym klucom k. Predpokladajme, ze pri generovani kluca k boli splnene nasledujuce 2 podmienky:

1. kazdy bit kluca k je generovany rovnomerne nahodne (t.j. pravdepodobnost, ze bit je rovny 0 je 0.5, a pravdepodobnost, ze bit je rovny 1 je tiez 0.5)
2. kazdy bit kluca k je generovany nezavisle od ostatnych bitov kluca k (t.j. pre kazdy bit kluca k plati, ze proces generovania tohto bitu nie je ovplyvneny procesmi generovania ostatnych bitov klucu k)

Nech z oznacuje 128-bitovy medzistav, ktory sa pri sifrovani sifrou AES vytvori po pridani podkluca k_0 (ako je znazornene na obrazku 4.2 na strane 115 v knihe). Nech $i \in \{0,1,\ldots,127\}$ a nech z_i oznacuje i-ty bit medzistavu z a x_i oznacuje i-ty bit plaintextu x . Odpovedzte na nasledujuce otazky:

a) Aka je pravdepodobnost, ze bit z_i je rovny 0 ?

b) Je pravdepodobnost, ze bit z_i je rovny 0, ovplyvnena hodnotou bitu x_i ?

c) Je pravdepodobnost, ze bit z_i je rovny 0, ovplyvnena hodnotami ostatnych bitov medzistavu z ?

Uloha 3:
Vyrieste Problem 4.12 na stranach 144 a 145 v knihe. (Pri rieseni tejto ulohy mozete napriklad vyuzit vizualizaciu sifry AES v nastroji Cryptool 2, ktory si mozete stiahnut na https://www.cryptool.org/en/)