Domácí úlohy 5.

odevzdat do 15.6. 14:00

do schránky na KA nebo na stanovsk@karlin.mff.cuni.cz

Úkoly můžete řešit ve dvojici, v takovém případě odevzdávejte jedno řešení se dvěma podpisy. Oba uveďte přezdívku, pod kterou uvidíte výsledky na webu.

Nemusíte vše počítat ručně. Můžete si leccos naprogramovat nebo použít Wolfram Alpha. V takovém případě odevzdejte i program a doklad o jeho běhu, např. printscreen s odpovědí.

1. (8 bodů) V dvoupatrovém úřadě v Kocourkově sídlí 20 úředníků, v každém patře 10, a ředitel. Úřad smí vydat rozhodnutí s kulatým razítkem, je-li přítomno aspoň 5 úředníků z 1. patra a 3 z 2. patra, nebo aspoň 2 z 1. patra, 8 z 2. patra a ředitel. Navrhněte schéma sdílení klíče k sejfu s kulatým razítkem. (Podobnost s Rektorátem Univerzity Karlovy je čistě náhodná.)

2. (6 bodů) Uvažujte Hammingův $(4, 7)$-kód, který jsem ukazoval. Dostali jste zprávu

$$0010001001110100111011011011110110001010001001100110 0111$$

Předpokládejte, že v každé sedmici je nejvýše jedna chyba. Najděte původní zprávu.

3. (6 bodů) Uvažujte těleso $\mathbb{F}_4 = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$, kde prvek $a + b\alpha$ zapisujeme jako slovo ab délky 2. Uvažujte Reed-Salomonův kód nad tímto tělesem, kde délka plaintextu je $2d = 4$ bitů a délka codetextu je $2n = 8$ bitů (body $a_1, ..., a_4$ zvolte v pořadí 00,01,10,11). Z teorie plyne, že by tento kód měl odhalovat jednu chybu, ale vse skutečnosti je to lepší, jednu chybu opravuje. Dokažte to. Dekódujte zprávu

$$01001010$$