2. vnitrosemestrální práce MB104, 14. 4. 2014
skupina A

Příklad 1. (4b.) V šifře ElGamal Honza zveřejnil klíč $(73, 5, 14)$. Přijal od Martina šifru $(2, 18)$. Jakou zprávu mu Martin zaslal? (víte, že $5^5 \equiv -14 \pmod{73}$).

Řešení. $2^{41} \equiv 32 \pmod{73}$, $32^{-1} \equiv 16 \pmod{73}$, $16 \cdot 18 \equiv 69 \pmod{73}$.

Příklad 2. (4b.) Určete generující matici G a kontrolní matici H lineárního $(8, 3)$ kódu generovaného polynomem $x^5 + x^4 + x + 1$. V tomto kódování jste obdrželi kódové slovo 01100111. Určete tříbitovou odeslanou zprávu za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Řešení.

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

syndrom 10011, vedoucí representant 00000001, odeslaná zpráva 110.

Příklad 3. (2b.) Kolik existuje dvojic podmnožin množiny $\{1, 2, \ldots, n\}$ takových, že průnikem množin v jedné dvojici je jednoprvková množina $\{1\}$ a jejich sjednocením pak celá množina $\{1, 2, \ldots, n\}$?

Řešení. 2^{n-1}.