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

Příklad 1. (3b.) V šifře ElGamal Honza zveřejnil klíč $(83, 2, 19)$. Přijal od Martina šifru $(3, 16)$. Jakou zprávu mu Martin zaslal? (uvažte, že $2^6 \equiv -19 \pmod{83}$).

Řešení. $3^{47} \equiv 65 \pmod{83}$, $65^{-1} \equiv 23 \pmod{83}$, $23 \cdot 16 \equiv 36$.

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 10111011. 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 (10001), vedoucí representanti 10001000, 00010001, 00100010, 01000100, možné odeslané zprávy 011, 010, 001, 111.

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

Řešení. 2^{n-2}.