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

Příklad 1. (4b.) V šifře ElGammal Honza zveřejnil klíč $(53, 2, 19)$. Přijal od Martina šifru $(2, 16)$. Jakou zprávu mu Martin zaslal? (víte, že $2^{11} \equiv -19 \pmod{53}$).

Řešení. $2^{37} \equiv 19 \pmod{53}$, $19^{-1} \equiv 14 \pmod{53}$, $14 \cdot 16 \equiv 12 \pmod{53}$.

Příklad 2. (4b.) Určete generující matici G a kontrolní matici H lineárního $(8, 3)$ kódu generovaného polynomem $x^5 + x^4 + x^2 + 1$. V tomto kódování jste obdrželi kódové slovo 01010010. Určete tříbitovou odeslanou zprávu za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Řešení.

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

syndrom 10101, vedoucí representant 00000100, odeslaná zpráva 110.

Příklad 3. (2b.) Určete, kolik existuje různých dvojic disjunktních podmnožin množiny $\{1, 2, \ldots, n\}$ takových, že prvky 1 a 2 nejsou v žádné dvojici ve stejné podmnožině?

Řešení. $3^n - 2 \cdot 3^{n-2}$.