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

Příklad 1. (4b.) V šifře ElGamal Honza zveřejnil klíč $(43, 3, 15)$. Přijal od Martina šifru $(4, 17)$. Jakou zprávu mu Martin zaslal? (víte, že $3^5 \equiv -15 \pmod{43}$).

Řešení. $4^{26} \equiv 35 \pmod{43}$, $35^{-1} \equiv 16 \pmod{43}$, $16 \cdot 17 \equiv 14 \pmod{43}$.

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 01111111. 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 (11111), vedoucí representant 00000010, odeslaná zpráva 101.

Příklad 3. (2b.) Kolik existuje různých rozesazení k chlapců a k dívek do k lavic po dvou žácích takových, že v každé lavici sedí dívka s chlapcem, ale Pepíček nesedí s Mařenkou a Adam nesedí s Evou. (V dané skupině se každé zmíněné jméno vyskytuje právě jednou.)

Řešení. $2^k(k!)^2 - 2 \cdot 2^k k!(k-1)! + 2^k k!(k-2)!$.