2. vnitrosemestrální práce MB104, 20. 4. 2015
skupina A

Příklad 1. (3b.) Veřejný klíč Honzy pro šifru RSA je $(91, 29)$. Zachytili jste jemu určenou zprávu 80. Dešifrujte ji.

Řešení. $29^{-1} \equiv 37 \pmod 6)4$, $80^5 \equiv 19 \pmod{91}$.

Příklad 2. (2b.) Určete nejmenší primitivní kořen modulo 43.

Řešení. $2^{14} \equiv 1 \pmod 4)3$, tedy 2 není primitivní kořen, $3^6 \not\equiv 1 \pmod 4)3$, $3^{14} \not\equiv 1 \pmod 4)3$, $3^{21} \equiv -1 \pmod 4)3$, tedy 3 je nejmenší primitivní kořen modulo 43.

Příklad 3. (2b.) Určete generující matici G a kontrolní matici H lineárního $(9, 3)$ kódu generovaného polynomem $x^6 + x^3 + x + 1$. V tomto kódování jste obdrželi slovo 101110111. Určete tříbitovou odeslanou zprávu za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Řešení. Syndrom 001101, vedoucí reprezentant 000000001, odesílaná zpráva 110.

Příklad 4. (3b.) Určete počet binárních slov délky 12, jejichž Hammingova vzdálenost od kteréhokoliv ze slov 110000000001 a 111111111110 nepřevyšuje 6.

Řešení. Slova v deseti bitech, součet Hammingovy vzdálenosti nějakého slova od těchto částí je tedy vždy deset. Podle podmínek úlohy je jsou tedy tyto vzdálenosti buď 5 a 5 nebo 4 a 6. V prvním případě ještě můžeme přidat jednu změnu v některém ze dvou shodných bitů. Celkem

$$3 \cdot \binom{10}{5} + 2 \cdot \binom{10}{4}.$$