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

Příklad 1. (3b.) Váš veřejný klíč pro šifru RSA je $(85, 45)$. Obdrželi jste zprávu 3. Dešifrujte ji.

Řešení. $45^{-1} \equiv 37 \pmod 6 4$, $80^5 \equiv 73 \pmod{85}$

Příklad 1. (2b.) Určete nejmenší primitivní kořen modulo 31.

Řešení. 3.

Příklad 2. (2b.) Určete generující matici G a kontrolní matici H lineárního $(9, 3)$ kódu generovaného polynomem $x^6 + x^3 + x^2 + 1$. V tomto kódování jste obdrželi slovo 011111011. Určete tříbitovou odeslanou zprávu za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Řešení. Syndrom 000010, vedoucí reprezentant 000010000, odesílaná zpráva 011.

Příklad 3. (3b.) Určete počet binárních slov délky 13, jejichž Hammingova vzdálenost od kteréhokoliv ze slov 1110000000011 a 1111111111110 nepřevyšuje 6.

Řešení. $2 \cdot 5 \cdot \binom{9}{4} + 2 \cdot \binom{9}{3}$

Více komentářů viz skupina A.