2.zkoušková práce MB104, 24. 6. 2015

Příklad 1. (3b.) Veřejný klíč Honzy pro šifru RSA je $(209, 103)$. Zachytili jste jemu určenou zprávu 9. Dešifrujte ji.

Řešení. $103^{-1} \equiv 7 \pmod 1)80$, $9^7 \equiv 4 \pmod{209}$.

Příklad 2. (5b.) Určete $7^{8^{9^{10}}} \mod 77$.

Řešení. 42.

Příklad 3. (5b.) Určete generující matici G a kontrolní matici H lineárního $(10, 3)$ kódu generovaného polynomem $x^7 + x^5 + x + 1$. V tomto kódování jste obdrželi slovo 0101001101. Určete tříbitovou odeslanou zprávu za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Řešení. Syndrom 0110001, vedoucí reprezentant 000000010, odesílaná zpráva 111.

Příklad 4. (5b.) Jaká může být nejmenší možná délka kódového slova kódu sestávajícího ze čtyř slov, který opravuje dvojnásobné chyby? Udejte příklad takového kódu.

Řešení. 8. Např. 11111111, 11100000, 00011000, 00000111.