

Zadání cvičení pro 7. týden: 3.4.-6.4.

V tomto týdnu můžete ještě případně dokončovat šifrování (RSA, Diffie-Hellman, El Gamal, Rabin), příklady obdobné jako minule. Pokud není třeba, pak se věnujte polynomiálním a lineárním (samoopravným) kódům. V tomto týdnu odpadla přednáška, takže bude cvičení předbíhat přednášky (což beztak skoro vůbec nevádí).

Příklad. Vysvětlete, jak polynom $x + 1$ generuje pro všechna $n \geq 3$ známý $(n, n - 1)$ -kód kontroly parity.

Poznámka. Viz str. 699 učebnice.

Příklad. (11.147)

Množinu 4 slov chceme přenášet binárním kódem opravujícím jednoduché chyby. jakou nejmenší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

Poznámka. Vysvětlete Hammingovu vzdálenost a přímou dedukcí určete $n \geq 5$.

Příklad. (11.136)

Vysvětlete $(5, 3)$ -kód nad \mathbb{Z}_2 generovaný polynomem $x^2 + x + 1$. Vypište všechna kódová slova, najděte generující matici a matici kontroly parity.

Poznámka.

Příklad. (11.141)

Určete generující matici a matici kontroly parity $(7, 2)$ -kódu generovaného polynomem $x^5 + x^4 + x^2 + 1$. Dekódujte slovo 0010111 (tj. najděte původní dvoubitovou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu počtu chyb.

Přidejte další příklady z učebnice nebo jiné (např. 11.142-6)