

Druhá domácí úloha

Příklad. Zakódujte binární zprávu 11010 pomocí kódu generovaného polynommem $p(x) = x + x^3$. Určete také genrující matici a matici kontroly parity tohoto kódu.

Poznámka. Z počtu bitů a řádu polynomu nejprve určete typ kódu.

Příklad. V protokolu ElGamal použijte prvočíslo 29, zvolte si primitivní kořen a šifrování použijte k zašifrování zprávy $m = 8$.