Druhá domácí úloha

Příklad. *Zakódujte binární zprávu 11011 pomocí kódu generovaného polynomem $p(x) = x + x^3$. Určete generující matici a matici kontroly parity tohoto kódu. Ukažte, jak se bude zaslaná zpráva dekódovat. A ukažte, co se stane, když se chybně zašle třetí bit zprávy.*

Poznámka. Z počtu bitů a řádu polynomu nejprve určete typ kódu. Poslední úkol směřuje k opravě chybné zprávy.

Příklad. *Demonstrujte protokol výměny klíčů Diffie-Helman s parametry $p = 61$, $g = 7$ a uveďte způsob použití v El Gamal protokolu.*

Poznámka. Zvolte si vlastní a a b a ukažte použití El Gamal na jednoduché zprávě.