

Errata do livro “Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos”:

- pág. 71, linha 7:  $M^{(i)}$  ao invés de  $M^i$
- pág. 71, linha -3: módulo  $p^m - 1$
- pág. 89: remover o segundo parágrafo
- pág. 91, linha 15:  $\mathbb{F}_q$  ao invés de  $\mathbb{F}_{q^n}$
- pág. 92, linha -9: remover “para assinatura digital”
- pág. 93, linha -14: consiste
- pág. 108, linha 17: “...o esquema de codificação... é dado por...”
- pág. 119, linha -4 e -3:  $M^{(s)}$  ao invés de  $M^s$