Instituto de Computação Universidade Estadual de Campinas

Lista de Exercícios I
MO422/MC938 – Algoritmos Criptográficos
Prof. Ricardo Dahab
13/10/2016

Esta lista traz uma seleção do tipo de questões que estarão presentes na primeira prova, cujo conteúdo se limitará aos assuntos cobertos em aula exceto o de curvas elípticas.

Como é evidente, há muitos mais exercícios nesta lista do que o número de questões de uma prova de duração de 2 horas; entretanto, o tipo de questões da prova será muito similar aos que se encontram aqui. Aproximadamente um terço do conteúdo da prova pedirá que se faça alguma demonstração razoavelmente simples de algum fato matemático; um terço pedirá que você execute algum algoritmo dos estudados em sala; e um terço pedirá que você examine algum algoritmo dado, sugerindo alguma modificação ou melhora.

Observação importante: Você poderá trazer uma folha tamanho A4 ou carta, preenchida à mão, para servir de consulta durante a prova.

Exercícios seguidos por [IMC] são do livro "Introduction to Mathematical Cryptography", de Hoffstein, Pipher e Silverman, edição de 2014. Aqueles referenciados por [ICCT-Cap. N] são do Capítulo N do livro "Introduction to Cryptography with Coding Theory", de Trappe e Washington.

1. *Algoritmo de Euclides, versões simples e estendida.*
   - Dados $a = 261$ e $b = 652$, calcule $d = \text{mdc}(a, b)$ e x, y tais que $d = x \cdot a + y \cdot b$. Se $d = 1$, encontre $261^{-1} \pmod{652}$.
   - Exercícios 1.11 e 1.13 [IMC]
   - Exercício 6 [ICCT/Cap. 3]
2. *Aritmética modular*
   - Exercícios 1.18 a 1.24; 1.27 [IMC]
   - Exercícios 10, 11 [ICCT/Cap. 3]
3. *Primalidade, fatoração e corpos finitos*
   - Exercícios 1.28, 1.35, 1.36 [IMC]
4. *Logaritmos discretos, Diffie-Hellman e ElGamal*

- Exercícios 2.3, 2.5, 2.7(a), 2.9, 2.10 [IMC]

5. *Teoria de grupos*
   - Exercício 2.13 [IMC]
6. *Algoritmos para o problema do logaritmo discreto*
   - Exercício 2.17(a) [IMC]
7. *Teorema Chinês do Resto*
   - Exercícios 2.18, 2.24, 2.25 [IMC]
8. *Pohlig-Hellman*
   - Exercícios 2.26, 2.28 [IMC]
9. *Teorema de Euler e raízes* $\pmod{p \cdot q}$
   - Exercícios 3.4, 3.5 [IMC]
10. *Criptossistema RSA*
    - Exercícios 3.8, 3.9(a), 3.11, 3.12 [IMC]
11. *Algoritmos para testes de primalidade*
    - Exercícios 3.14, 3.15 [IMC]
12. *Algoritmos para fatoração e sua complexidade*
    - Exercícios 3.22, 3.29, 3.30 [IMC]