4ª Lista de Exercícios de SMA-180 Matemática Discreta

Eugenio Massa

Criptografia

1. Exercícios 2,3,4 nas páginas 59,60 do livro (seção 2.1, pp72-74 do inlgês).

2. Exercícios 12,13,14 nas páginas 91,92 do livro (seção 2.4, pp 114,115 do inlgês).

3. Escreva um programa que calcula $a^e \ (mod\ d)$ onde a, e, d são unsigned int (32 bits), $a < d$, $d, e < 256^2$ (16 bits). (Atenção: escreva o código usando apenas unsigned int mas precisa cuidar que em nenhum momento dê overflow!)
   Teste o código com as potências de lista 3.

4. Usando o código do exercício 3, implemente uma versão de RSA com chave de 16 bits:
   – Escolha dois primos p, q tais que $n = pq$ caiba em 16 bits, escolha um e invertível em $\mathbb{Z}_{(p-1)(q-1)}$ e implemente a função de codífica.
   – Calcule o inverso de e em $\mathbb{Z}_{(p-1)(q-1)}$ e implemente a função de decodífica.

OBS: Para os exercícios a seguir, exceto onde indicado, pode usar o código do exercício 3, um algoritmo de Euclides estendido e um de fatoração: programe eles ou use os vistos na sala

5. Codifique as seguintes mensagens usando o RSA de chave pública $n = 13067$, $e = 5$
   a) m= 10101 b) m=20 c) m=9999 d) m=13066
   Notou algo estranho no caso d? Explique!

6. A chave pública de um sistema RSA é $n = 1241$, $e = 5$. Você intercepta a mensagem codificada 695. Quebre o código e descubra a mensagem.

7. A chave pública de um sistema RSA é $n = 1247$, $e = 17$. Quebre o código e envie a mensagem 430 de forma que resulte assinada com a chave secreta.

8. A chave pública de um sistema RSA é $n = 1741991$, $e = 17$. Descubra p e q sabendo que $\phi = 1739232$ (para este exercício não use um algoritmo de busca de primos).

9. Quais dos números 645, 567, 701 são pseudoprimos com respeito à base 2? E com respeito à base 3? quais são primos?

10. Quais dos números 645, 2047, 2309 são fortemente pseudoprimos com respeito à base 2? E com respeito à base 3? quais são primos?

11. Para os d a seguir:
    $d = 645,\ 613,\ 1105,\ 121,\ 223,\ 703,$
    escreva $d = 2^k q + 1$ com q ímpar, $k \geq 1$, depois escreva a sequência

$$b^{2^i q} \ (mod\ d): \quad i = 0, .., k$$

com $b = 2$ e $b = 3$.

Quais são pseudoprimos com respeito a estas bases? quais fortemente pseudoprimos? Quais são certamente compostos?

Gabarito

Exercício 5 a) $c = 2363$, d) $c = 13066$!!!!