Universidade do Minho

Departamento de Matemática — Lic. Ciências da Computação – 3° ano

Teoria de Números Computacional

teste prático — 18 junho '08

A duração deste teste é de 2 (duas) horas.
Justifique todas as suas respostas convenientemente.
Grave as suas respostas num ficheiro com o nome `aXXXX.txt` usando o seu número de aluno.
Escreva o seu número e nome no início do ficheiro.

Dos 5 exercícios seguintes, resolva apenas 3.

1. A chave pública RSA é

   [n,e]=[1749887123803837464940920150621145530 7, 858241237382944719998261754701968799]

   (a) Cifre x=382318220533465709302921420220241 8806

   (b) Decifre y=112232064782691744997602723700933642 05, sabendo que 3853567945973531083 divide n.

2. Encontre um factor não trivial de 455266534277 usando o algoritmo $p-1$–Pollard.

3. Encontre um factor não trivial de 455266534277 usando o algoritmo ρ–Pollard, usando a sequência pseudo-aleatória dada por $x_0 = 2$ e gerada da forma usual por $f(x) = x^2 + 1$..

4. Encontre o menor pseudoprimo forte de base 2.

5. Publique uma chave Elgamal, com $2^{32} \leq p$.
   Bónus: crie funções `gerachave, cifra, decifra` para o Elgamal.

Alguns comandos úteis:
`isprime, random, nextprime, znprimroot, znorder, factor, Mod`
`?comando`

Cotação:
cada questão: 2 valores