Prova P1 03/04/2012

UFRJ - Num. Inteiros e Criptografia

Prof. Luis Menásche

1)

a)Descreva as diferenças entre criptografia 'chave simétrica' e criptografia de 'chave pública'.Cite um exemplo de cada uma.

b)Descreva as diferenças entre 'decodificar' e 'decifrar'. Diga o que deveriamos fazer para decifrar uma mensagem criptografada com RSA.

2)

a)Relate os erros na função em Axiom abaixo e reescreva esta função de forma correta.

```
Func( a :: nni, b :: nni) :: nni
        m :: nni = 0
        i :: nni = 1
 while ( i <= b )
       m = i
       i = i + 1
 return m
```

b)Escreva uma função em Axiom que tem como entrada dois inteiros positivos,e retorne um Record com dois inteiros positivos (respectivamente mdc(a,b) e mmc(a,b)).

3)Se a equação diofantina 282899x +3596311y = 68103 tiver solução, indique a familia de infinitas soluções.

4)

a)Diga dois fatores do número 3596311.

b)Explique o que é primorial de um numero inteiro positivo, e a partir daí prove por contradição que existem infinitos números primos.