






Teoria de Números Computacional

exame de recurso

21 de junho de 2018

A duração da prova é de 180 minutos. Justifique todas as suas respostas convenientemente.

1.  Considere a chave pública RSA dada por $(n, e) = (5814269, 11)$.
 - (a) Cifre $x=1234$. 1 valor
 - (b) Encontre um factor não trivial de n usando 4 valores
 - i. a factorização de Fermat;
 - ii. o algoritmo de factorização ρ -Pollard, com a sucessão pseudo-aleatória dada por $x_0 = 8$ e $f(x) = x^3 + x^2 + 1$.
 - (c) Decifre $y=3005572$, sabendo que 2281 divide n . 2 valores
2. Considere $n = 203873$.
 - (a)  Verifique que n passa o teste de Miller-Rabin de base 2. O que pode concluir sobre a primalidade de n ? Construa a respectiva sequência-B. 2 valores
 - (b)  Use o algoritmo de Lucas para mostrar que n é primo, usando a base $a = 3$. 2 valores
 - (c)  Verifique que n passa o teste de Solovay-Strassen de base 2. 1 valor
 - (d) Sabendo que n é primo, verifique se 465 é resíduo quadrático módulo n . 2 valores
 - (e)  Sabendo que n é primo e que $r = 3$ é uma raiz primitiva módulo n , e ainda que $r^{32} = 162995 = b$, considere a chave pública (n, r, b) de um sistema criptográfico ElGamal. Decifre a mensagem recebida (86924, 60851). 2 valores
3. Suponha que n admite uma raiz primitiva r . Mostre que $\{r^1, r^2, \dots, r^{\phi(n)}\}$ é um sistema reduzido de resíduos módulo n . 2 valores
4. Mostre, detalhadamente, que qualquer primo ímpar passa o teste de primalidade probabilístico Solovay-Strassen. 2 valores