Criptografia
Tópicos Especiais em Sistemas de Informação
Sistemas de Informação

Moésio M. de Sales[1]

Atividade Tema I. Nos exercícios desenvolva um código em `python` e `C++`. Utilize para criação de seus programas os arquivos já indicados neste repositório.

1. (**mdc**) Programa que lê um dois inteiro positivos a e b e imprime o máximo divisor comum (mdc) de a e b.
2. (**mdc-euclides**) Dados dois números inteiros positivos, determinar o máximo divisor comum entre eles usando o algoritmo de Euclides.
3. (**fatores**) Programa que lê um número inteiro positivo n e determina a sua decomposição em fatores primos calculando também a multiplicidade de cada fator.
4. (**diofantina**) Programa que lê três número inteiro positivo a, b, c, com $mdc(a, b) = 1$ e determina a solução mínima x, y inteira para equação $ax + by = c$.
5. (**funcao-euler**) Programa que lê um número inteiro positivo n e determina $\phi(n)$.
6. (**ordem**) Programa que lê dois números inteiros positivos n, a, com $mdc(n, a) = 1$ e determina o menor o tal que $a^o \equiv 1 \pmod{n}$.
7. (**inverso**) Programa que lê dois números inteiros positivos n e a, com $mdc(n, a) = 1$ e determina seu inverso b, ou seja, um inteiro b tal que $a\dot{b} \equiv 1 \pmod{n}$.
8. (**sistema-invertiveis**) Programa que lê um número inteiro positivo n e determina seu Conjunto de Invertíveis Módulo n, ou seja, $\{b_1, b_2, \cdots, b_{\varphi(n)}\}$ tal que $b_i \equiv b_j \pmod{n}$ implica $i = j$.

[1] moesio@ifce.edu.br