UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

Cálculo do Inverso de um módulo

1) Para que calcular?
É utilizado, por exemplo, na resolução de equações diofantinas e na criptografia

2) O que é o inverso?
São as soluções de $au \equiv 1 \pmod{m}$

3) Ferramentas da Álgebra: *Domínio Euclidiano; Teorema do resto; Algoritmo de Euclides estendido*

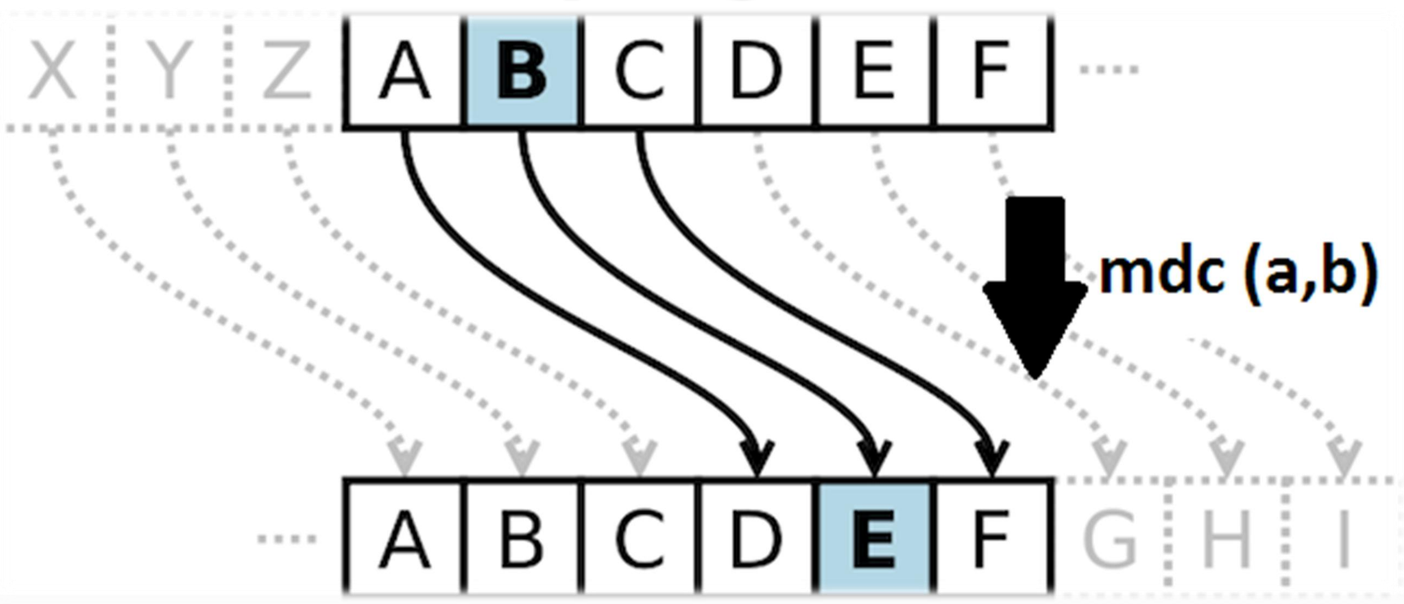
4) Principais teoremas? *Garantia da unicidade das soluções de "u"; quando "a" será invertível; quais os tipos de solução encontradas; generalização do mdc entre dois números para Domínios Euclidianos.*

5) Como calcular?
Através de algoritmos de programação que calcula o mdc entre dois números em tempo polinomial.

Equações diofantinas

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases}$$

Chaves Criptográficas



Paola Rossato Bernardo

Orientador: Vilmar Trevisan