Projeto 3

Paillier Cryptosystem

Felipe Dal Mas Eulálio 155299
Guilherme Lucas da Silva 155618
Vitor Falcão da Rocha 157537

Paillier Cryptosystem

Overview

GMP

Propriedade homomórfica

Aplicações

Paralelização

Usados 2 cores

- Cada core descobria um número primo

Paralelização

Problemas

- 512MB -> *Overflow*
- 1024MB -> *Program counter* não alcançava as posições de memória

Periférico

Melhora de partes críticas

Dificuldades

Resultados

Tempo	Instruções
7m37.774s	29139738154

Execução base

Tempo	Instruções
0m1.458s	70

Execução com o periférico

Conclusão

Perguntas?

Obrigado!