UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

NÚMEROS PRIMOS E CRIPTOGRAFIA:

CRIPTOGRAFIA RSA E ALGORITMO AKS

DISCENTE: ALAN DE ARAÚJO GUIMARÃES

ORIENTADOR: DIOGO DINIZ PEREIRA DA SILVA E SILVA

CAMPINA GRANDE, 26 DE MAIO DE 2010

1. TÍTULO

Números Primos e Criptografia: Criptografia RSA e Algoritmo AKS

2. OBJETIVOS

Fazer um estudo de alguns tópicos da Teoria Aritmética dos Números (Aritmética modular, em especial), a fim de estudar o funcionamento do algoritmo RSA de criptografia. E, também, estudar Grupos abelianos, Anéis, Ideais e polinômios, com o propósito de conhecer o funcionamento do Algoritmo AKS de primalidade.

3. PROGRAMA DE ESTUDO

Para conhecer o algoritmo RSA de criptografia, estudamos:

- Aritmética Modular;
- Inversos Modulares;
- Algoritmo Chinês do Resto;
- Potências Modulares e
- Criptografia RSA

Para conhecermos o funcionamento do Algoritmo AKS de primalidade, estudaremos:

- Grupos abelianos;
- Anéis, Ideais e polinômios;
- Testes de primalidade;
- Algoritmo AKS

4. CRONOGRAMA

	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Estudo do algoritmo RSA de criptografia	X	X							
Sumarização do estudo feito e elaboração de apresentação			X	X					
Estudo do algoritmo AKS de primalidade					X	X	X	X	
Sumarização do estudo feito e elaboração de apresentação									X

5. BIBLIOGRAFIA

COUTINHO, S.C. **Números inteiros e criptografia RSA. Série de Computação e Matemática** n. 2, IMPA e SBM, segunda edição, 2000.

COUTINHO, S.C. **Criptografia (Programa de Iniciação Científica OBMEP)**; OBMEP. Rio de Janeiro, 2008.

COUTINHO, S.C. **Primalidade em Tempo Polinomial: Uma introdução ao Algoritmo AKS.** SBM; Rio de Janeiro, 2004.

GONÇALVES, Adilson. **Introdução à álgebra**. Projeto Euclides, 5°ed. Rio de Janeiro: IMPA, 2008.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2003.

_____

Orientador: Diogo Diniz Pereira da Silva e Silva

_____

Discente: Alan de Araújo Guimarães