RELATÓRIO FINAL
DE ORIENTAÇÃO DE INICIAÇÃO CIENTÍFICA
DO PET-MATEMÁTICA UFCG

I – Dados do Projeto	
Título: Números Primos e Criptografia: Criptografia RSA e Algoritmo AKS	
Período: 2010.1; 2010.2; 2011.1	
Bolsista: Alan de Araújo Guimarães	
Orientador de Iniciação Científica: Prof. Dr. Diogo Diniz Pereira da Silva e Silva	

I.1 Resumo do Projeto	

Nosso projeto foi subdividido em duas etapas. Na primeira delas, o objetivo era estudar uma versão bastante elementar do Algoritmo RSA de criptografia. Neste momento, estudamos tópicos de Aritmética que, em geral, são vistos em um primeiro curso de Fundamentos de Matemática. Na segunda etapa do projeto, objetivávamos o estudo do Algoritmo AKS de primalidade. Para este fim, trabalhamos com os seguintes temas matemáticos: grupos abelianos, anéis, ideais, ideais quocientes.

I.2 Objetivos Propostos	

Tínhamos por objetivos: estudar os temas matemáticos supracitados para ter maior embasamento matemático; conhecer o Algoritmo RSA de criptografia; conhecer o Algoritmo AKS de primalidade.

I.3 Resultados Obtidos	

Tivemos a oportunidade de estudar temas importantes de Aritmética e Álgebra Abstrata, quais sejam: pequeno teorema de Fermat, aritmética modular, grupos abelianos, anéis, ideais, dentre outros. Como fruto do estudo, realizamos duas apresentações: a primeira foi uma palestra no Departamento de Matemática da UFCG, intitulada ‘Matemática e Criptografia’ e a segunda foi uma apresentação em forma de pôster no III Encontro de Matemática Pura e Aplicada (III EMPA), realizado na Universidade Estadual da Paraíba (UEPB).

II- CRONOGRAMA
O CRONOGRAMA DE TRABALHO PROPOSTO FOI CUMPRIDO? **(X)SIM** **( ) NÃO. NESSE CASO DETALHAR OS MOTIVOS.**

III- Justificar Alterações no Projeto (se for o caso)

IV- Parecer do orientador sobre o desempenho do aluno
O aluno teve um excelente desempenho, demonstrou maturidade na matemática necessária para desenvolver o projeto, bem como proatividade e dedicação ao projeto.

_____

Discente: Alan de Araújo Guimarães

_____

Orientador Científico: Prof. Dr. Diogo Diniz Pereira da Silva e Silva

_____

Tutor do PET Matemática UFCG: Prof. Dr. Daniel Cordeiro de Morais Filho