UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE TECNOLOGIA

CURSO DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

RELATÓRIO PARCIAL – PROJETO DE GRADUAÇÃO I

PERÍODO: Agosto de 2016 a Novembro de 2016

Criptografia de chave pública com primos de Gauss

LUIS ANTONIO COÊLHO

Relatório parcial referente ao período de agosto de 2016 a novmbro de 2016, submetido ao sistema de TCC do Curso de Análise e Desenvolvimento de Sistemas da Universidade Estadual de Campinas, como requisito parcial para obtenção do grau de Analista e Desenvolvedor de Sistemas.

Orientadora: Profa. Dra. Juliana Bueno

Limeira – São Paulo
2016

1 INTRODUÇÃO

O projeto será conduzido pelo aluno Luis Antonio Coêlho, sob a orientação da Profa. Dra. Juliana Bueno e será focado na comparação de algoritmos de criptografia de chave pública com relação a segurança dos dados.

2 ATIVIDADES EXECUTADAS NO PERÍODO

Pesquisa sobre números primos de Gauss e sobre algoritmos de criptografia. Desenvolvimento de uma aplicação baseada na criptografia RSA e uma aplicação para obtenção de números primos de Gauss.

3 PRINCIPAIS RESULTADOS OBTIDOS

Introdução do TCC. Algoritmo para obtenção de primos de Gauss.

4 ORGANIZAÇÃO PARA CONCLUSÃO DO TRABALHO

Desenvolvimento da criptografia com primos de Gauss. Testes de efetividade do algoritmo. Escrita final do projeto.

5 CRONOGRAMA

Quadro CRONOGRAMA.1. Cronograma de Atividades.

ITEM	ATIVIDADES	PERÍODOS (meses)									
		ago	set	out	nov	dez	jan	mar	abr	mai	jun
1	Levantamento de literatura		X								
2	Montagem do Projeto			X							
3	Apresentação do Projeto				X						
4	Desenvolvimento de aplicações				X						
5	Elaboração do Relatório Parcial				X						
6	Apresentação do Relatório Parcial				X						
7	Desenvolvimento do algoritmo de criptografia com primos de Gauss						X	X			
8	Testes do algoritmo							X	X		

9	Elaboração do Relatório Final								X	X	
10	Revisão do texto									X	
11	Entrega do trabalho final										X
12	Apresentação do trabalho final										X

6 PRINCIPAIS DIFICULDADES ENCONTRADAS NO PERÍODO

Desenvolver o algoritmo para obtenção dos primos de Gauss.

REFERÊNCIAS BIBLIOGRÁFICAS

Diffie, Whitfield e Martin Hellman. “New directions in cryptography”. Em: IEEE transactions on Information Theory 22.6 (1976), pp. 644–654.

Gauss, Carl Friedrich. Methodus nova integralium valores per approximationem inveniendi. apvd Henricvm Dieterich, 1815. Millennium Problems — Clay Mathematics Institute. Acessado em 15/11/2016.

Riemann, Bernhard. “Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse”. Em: Ges. Math. Werke und Wissenschaftlicher Nachlaß 2 (1859), pp. 145–155.

Rivest, Ronald L, Adi Shamir e Leonard Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. Em: Communications of the ACM 21.2 (1978), pp. 120–126.

Shannon, Claude E. “Communication theory of secrecy systems”. Em: Bell system technical journal 28.4 (1949), pp. 656–715. Sinkov, Abraham e Todd Feil. Elementary cryptanalysis. Vol. 22. MAA, 2009.