

DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA — CTC — UFSC
RATIFICAÇÃO DE PLANO DE TRABALHO DO SEMESTRE PARA DESENVOLVIMENTO DE TCC

Disciplina: INE5433 — Trabalho de Conclusão de Curso I
Curso: Ciência da Computação
Autor: Gustavo Zambonin
Título: Esquemas de assinatura digital baseados em funções de resumo criptográficas
Professor responsável: Ricardo Felipe Custódio

Objetivos

Objetivo geral. Apresentar um estudo detalhado sobre esquemas de assinatura digital baseados em funções de resumo criptográficas, partindo de esquemas de assinatura única, observando o refinamento destes, até o estado da arte, onde não é necessário saber quantas assinaturas foram geradas anteriormente, bem como implementações em linguagem de alto nível para a fácil compreensão destes esquemas.

Objetivos específicos. Descrever os esquemas de assinatura digital única Lamport-Diffie e Winternitz; descrever os esquemas de assinatura digital baseado em árvores de Merkle — *Merkle Signature Scheme*, *eXtended Merkle Signature Scheme*; implementar os esquemas supracitados; comparar o desempenho destes algoritmos entre si, utilizando funções de resumo criptográficas e parâmetros internos aos algoritmos distintos, onde aplicável.

Cronograma

Etapas	2017						2018					
	jul.	ago.	set.	out.	nov.	dez.	jan.	fev.	mar.	abr.	mai.	jun.
Fundamentação teórica												
Revisão do estado da arte												
Desenvolvimento do TCC												
Implementação												
Relatório de TCC I												
Ajustes na implementação												
Redação da monografia												
Ajustes na monografia												
Relatório de TCC II												
Defesa pública												
Ajustes finais do TCC												

Preenchimento pelo professor responsável pelo TCC

() Ciente e de acordo. Assinatura:
Data: __ / __ / ____