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

Disciplina:	INE5434 — Trabalho de Conclusão de Curso II
Curso:	Ciência da Computação
Autor:	Gustavo Zambonin
Título:	Esquemas de assinatura digital baseados em funções de resumo criptográfico
Professor responsável:	Ricardo Felipe Custódio

Objetivos

Objetivo geral. Apresentar um estudo detalhado sobre esquemas de assinatura digital baseados em funções de resumo criptográfico, partindo de esquemas de assinatura única, observando o refinamento destes, até o estado da arte, nos quais 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* e SPHINCS; implementar alguns dos esquemas supracitados; comparar o desempenho destes algoritmos entre si, utilizando funções de resumo criptográficas e parâmetros internos aos algoritmos distintos, onde aplicável; otimizar a utilização da assinatura única de Winternitz no contexto destes esquemas baseados em árvores de Merkle.

Cronograma

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

Preenchimento pelo professor responsável pelo TCC

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