CI1355 / INFO7056: Tópicos em Algoritmos - Fundamentos da Criptografia 2026/1

Projeto Semestral

Professor: Nicollas Mocelin Sdroievski

Este documento descreve o projeto semestral da disciplina de Tópicos em Algoritmos. O projeto pode ser desenvolvido em grupos de até três alunos, e possui três entregas, descritas a seguir. As entregas devem ser realizadas para o e-mail *nmsdroievski[arroba]ufpr.br* nos prazos indicados na página da disciplina (https://www.inf.ufpr.br/nicollas/topicos/index.html).

Objetivo

O objetivo deste projeto é aprofundar os conhecimentos desenvolvidos durante a disciplina através do estudo e apresentação de um artigo teórico da área de criptografia ou então da implementação e apresentação de algum protocolo criptográfico ou ataque que leva a quebra de segurança de um protocolo criptográfico.

O projeto é dividido em três partes, que serão corrigidas separadamente. Na segunda e terceira entregas, espera-se que as questões apontadas na correção da entrega anterior sejam corrigidas.

Primeira Entrega: Proposta do Projeto

Para a primeira entrega, o grupo deve apresentar um documento PDF formatado com LaTeX, com até duas páginas, apresentando uma proposta de projeto. Para projetos teóricos, a proposta deve explicar, em alto nível, as contribuições principais do(s) artigo(s) escolhido(s), e em quais partes os alunos pretendem se aprofundar. Para projetos práticos, a proposta deve também explicar, em alto nível, a implementação / ataque a ser realizado.

Observação: alguns dos temas sugeridos são complexos. Minha sugestão é ler a introdução de alguns artigos que julgue interessantes, escolher algum que chame a atenção, e então conversar comigo para decidir um escopo viável.

Segunda Entrega: Relatório Parcial e Ajustes

Para a segunda entrega, o grupo também deve apresentar um documento PDF formatado com LaTeX, com o progresso do projeto até então. Para projetos teóricos, esta entrega deve apresentar as definições das primitivas criptográficas utilizadas pelo(s) artigo(s) escolhido(s), além de formalizar os modelos de segurança escolhidos na primeira entrega. Para projetos práticos, deve-se, de maneira similar, indicar as definições de segurança subjacentes. Por exemplo, um projeto que implementa um ataque deve deixar claro o modelo de segurança que é quebrado pelo ataque, e um projeto de implementação deve deixar claro qual primitiva será implementada e o modelo de segurança que é esperado ou conjecturado da implementação. Por fim, deve ser incluída uma seção indicando as dificuldades encontradas até o momento.

Entrega Final e Apresentação

A entrega final possui dois componentes: um documento PDF em formato de artigo LaTeX, e uma apresentação oral (utilizando slides e/ou quadro) para a turma.

A parte escrita da entrega final deve possuir as seguintes seções

1. Introdução, com a motivação e explicação de alto nível das construções apresentadas.
2. Preliminares matemáticas, incluindo as definições de segurança e das primitivas utilizadas.
3. Para projetos teóricos: uma seção com as demonstrações formais apresentadas no artigo original, explicadas, na medida do possível, com as palavras dos membros dos grupos.
4. Para projetos práticos: detalhes da implementação realizada, incluindo link para repositório público com o código da implementação e instruções de execução.
5. Conclusão, incluindo também potenciais contribuições futuras na área identificadas pelos autores originais ou pelo próprio grupo.

Para a apresentação oral, espera-se que cada grupo apresente uma visão geral da motivação, definições centrais, intuição da prova ou funcionamento do ataque/construção, e resultados/conclusões obtidas. Cada grupo terá entre 20 e 30 minutos de apresentação, e mais 5 minutos para perguntas.