Elementos/Fundamentos de Criptografia
Projectos Práticos Avançados

Manuel Bernardo Barbosa @ di.uminho.pt

Março de 2004

Os seguinte projectos destinam-se a ser realizados no âmbito da disciplina de Elementos/Fundamentos de Criptografia para obtenção de classificação prática de forma alternativa ao enunciado já publicado.

Máquina de Cifragem/Decifragem Enigma

Pretende-se neste projecto o estudo da Máquina de Cifragem/Decifragem Enigma, utilizada pelo exército Alemão durante a 2º Guerra Mundial nas seguintes vertentes:

- Contextualização histórica.
- Estudo do funcionamento da máquina Enigma.
- Desenvolvimento de um emulador.
- Estudo das técnicas de criptoanálise que permitem a realização de ataques a este sistema.

Esteganografia

A esteganografia é a ciência de esconder informação, de forma segura, em suportes digitais, como sejam ficheiros de imagem. O que se pretende com este projecto é o estudo da esteganografia como tecnologia de suporte à comunicação segura, no sentido criptográfico do termo. Depois de uma análise de bibliografia relevante, o objectivo será a implementação de um sistema de troca de informação segura com base em técnicas de esteganografia.

Livraria para Votação Electrónica

Pretende-se com este projecto implementar uma livraria em JAVA que possa ser utilizada em *applets* distribuídos como parte de sistemas de votação electrónica.

A livraria deverá conter implementações das primitivas criptográficas utilizadas nas diversas variantes deste tipo de sistemas: não só cifras, mas também esquemas mais complexos como blind signatures, bit commitments, provas de conhecimento zero, etc. Na fase final deverá ser desenvolvido um pequeno applet que exemplifique as potencialidades da biblioteca desenvolvida.