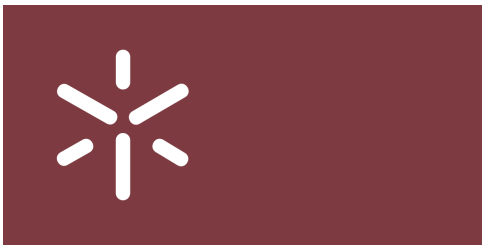

O Sistema Merkle-Hellman Knapsack

Bernardo Rodrigues
a79008@alunos.uminho.pt

César Silva
a77518@alunos.uminho.pt

Maria Franisca Tavares?
a99999@alunos.uminho.pt

Universidade do Minho — 29 de Abril de 2019

Conteúdo

Resumo

Coisas nunca antes ditas

Capítulo 1

Introdução

Este trabalho foi desenvolvido no ambito da Unidade Curricular de `Teoria de Números Computacional`. De entre as escolhas possiveis, foi escolhido estudar o sistema *Merkle-Hellman Knapsack*.
Este foi um dos pioneiros da criptografia de chave pública, inventado por **Ralph Merkle** e por **Martin Hellman** em 1978. A ideia por detrás deste sistema é mais simples do que a de sistemas como o *RSA*, assentando no problema (tendo já sido quebrado – meter isto noutro sitio??).

Capítulo 2

Corpo do Trabalho??

Capítulo 3

Conclusões

Capítulo 4

Bibliografia??

Meter o latex a fazer isto por nós

Apêndice A

Código??

Será que vai num ficheiro separadamente?