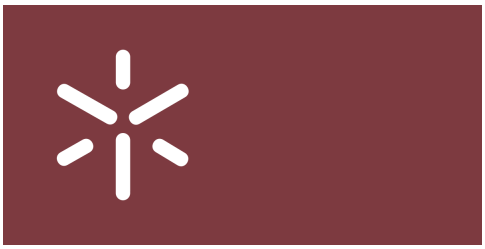

O Sistema Merkle-Hellman Knapsack

Bernardo Rodrigues
a79008@alunos.uminho.pt

César Silva
a77518@alunos.uminho.pt

Maria Francisca Fernandes
a72450@alunos.uminho.pt

Universidade do Minho — 1 de Maio 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??

Algorithm 1 Solução da soma do subconjunto super crescente

1: $i \leftarrow n$
2: **while** $i \geq 1$ **do**
3: **if** $s \geq b_i$ **then**
4: $x_i \leftarrow 1$
5: **else**
6: $x_i \leftarrow 0$
7: **end if**
8: $i \leftarrow i - 1$
9: **end while**

Capítulo 3

Conclusões

Capítulo 4

Bibliografia??

Meter o latex a fazer isto por nós

Apêndice A

Código??

Será que vai num ficheiro separadamente?