

Introdução

Criptografia  
Clássica

Criptoanálise  
Criptoanálise das  
Cifras Clássicas

Cifras por  
Blocos

Cifras de  
Chaves  
Simétricas

Cifras de  
Chaves  
Públicas

Funções de  
Dispersão

MDCs

MACs

## Exercício Prático 2

Implemente o método de ataque directo para a cifra de deslocamento simples.

- Alfabeto Português incompleto  $\mathcal{A} = \{a-z\}$ .
- Cifração carácter a carácter.
- Utilize uma lista de palavras Portuguesas para, de forma automática, avaliar que a cifra foi, ou não, quebrada.
- Interface Entrada/Saída: ficheiros e linha de comando.
- Implementação em C (ou C++).