Departamento de Matemática da Universidade de Coimbra		
2015/2016	**Métodos de Programação I**	**Projecto 1**

Criptografia/Criptoanálise

Na *Era da Informação* a protecção da informação vital ganha uma enorme importância, daí vem a necessidade de contar com métodos criptográficos e, em sentido inverso, métodos criptoanalíticos [1, 2, 3].[1]

Definição 1 (Criptografia) *Criptografia é o estudo das técnicas matemáticas relacionadas com os aspectos de segurança da informação tais como: confidencialidade, integridade da informação, autenticação de entidades e da origem da informação.*

Definição 2 (Criptoanálise) *Criptoanálise é o estudo dos procedimentos necessários para tentar comprometer as técnicas criptográficas, e mais genericamente, os serviços de segurança da informação.*

Pretende-se implementar a *Cifra de Deslocamento Linear*

$$E_{(a,b)}(x) = (ax + b) \bmod |\mathcal{A}|$$

assim como o método criptoanalítico *Método da Força Bruta* (tentativas exaustivas no espaço das chaves).

Temos então, três programas:

- `encriptarDL` – para encriptar, dado um texto e uma chave, encriptá-lo através da cifra de deslocamento linear;
- `desencritarDL` – para desencriptar, dado um texto cifrado e uma chave, decifrá-lo, através da cifra de deslocamento linear;
- `forcaBrutaDL` – criptoanálise, dado um texto cifrado (e não tendo a chave de desencriptação), tentar todas as chaves possíveis.

Temos então:

- construir os três programas para textos (alfabeto ASCII) contendo somente minúsculas. Os espaços e outros caracteres não pertencentes ao alfabeto não serão cifrados.
- os programas construídos deverão permitir que:
  - dado um texto claro (não cifrado) e a respectiva chave, se obtenha o texto cifrado correspondente;
  - dado um texto cifrado e a respectiva chave, se obtenha o texto claro correspondente;
  - dado um texto cifrado, se obtenha um texto com todas as possíveis desencriptações do mesmo.

1. Documente o seus programas, tanto em termos de documentação interna, como de documentação externa.

[1] Apontamentos da disciplina de Códigos e Criptografia, 2012/2013

2. A documentação externa, relatório, deve ter no máximo 10 páginas. O relatório deve estar correctamente identificado.

3. Deve entregar (por correio electrónico) um arquivo (formato `ZIP`) contendo os ficheiros referentes ao programa (`Makefile, *.c, *.h`), assim como o ficheiro referente ao relatório (formato `PDF`), até às 24h00 do último dia do prazo.

Referências

[1] Pedro Quaresma and Elsa Lopes. Criptografia. *Gazeta de Matemática*, 154:7 – 11, Março 2008.

[2] Pedro Quaresma and Augusto Pinho. Criptoanálise. *Gazeta de Matemática*, 157:22 – 31, 2009.

[3] Richard Spillman. *Classical and Contemporary Criptology*. Pearson Prentice-Hall, Upper Saddle River, NJ 07458, 2005.