Departamento de Matemática da Universidade de Coimbra		
2014/2015	**Programação Orientadas para os Objectos**	**Projecto 2**

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 construir uma biblioteca de métodos criptográficos e criptoanalíticos para apoio à encriptação/desencriptação de textos em Português.

Temos então:

- construir uma biblioteca de métodos criptográficos e correspondentes métodos criptoanáliticos, para textos em Português (codificação ISO-8859-1), `libCripto`:

```
int comprimentoAlfabeto;
char cifraDS(int,char);
char decifraDS(int,char);
void encriptarDS(int,ifstream,ofstream);
void desencriptarDS(int,ifstream,ofstream);
char cifraDL(int,int,char);
char decifraDL(int,int,char);
void encriptarDL(int,int,ifstream,ofstream);
void desencriptarDL(int,int,ifstream,ofstream);
void forcabrutaDS(ifstream,ofstream);
void forcabrutaDL(ifstream,ofstream);
```

- construir um programa que permita fazer o interface com a biblioteca de forma a que:
  - escolhida a opção de cifrar: dado um texto claro (não cifrado) e escolhido o método de encriptação e respectiva chave, se obtenha o texto cifrado correspondente;
  - escolhida a opção de decifrar: dado um texto cifrado e escolhido o método de desencriptação e respectiva chave, se obtenha o texto claro correspondente;
- construir um programa que permita fazer o interface com a biblioteca de forma a que:
  - dado um texto cifrado e escolhido o método de criptoanálise a utilizar se obtenha uma lista de todos os possíveis textos claros.

Por questões de simplicidade nesta primeira aproximação à biblioteca `libCripto` as cifras a implementar são a Cifra de Deslocamento Simples e Cifra de Deslocamento Linear e os métodos de criptoanálise são os métodos de Força Bruta (exaustão no espaço das chaves de encriptação) respectivos.

1. Documente o seus programas, tanto em termos de documentação interna, como de documentação externa.
2. Documente a biblioteca `libCripto` de forma a que a mesma possa ser usada por outros programadores.
3. Na documentação externa (relatório, max 10pg) deve incluir o diagrama UML referente às classes construídas assim como um pequeno manual de utilização. O relatório deve estar correctamente identificado.
4. Deve entregar (por correio electrónico) um arquivo (formato `ZIP`) contendo os ficheiros referentes ao programa (`Makefile, *.cpp, *.hpp`), assim como o ficheiro referente ao relatório (formato `PDF`), até às 24h00 do último dia do prazo.

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

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.