Ficha de atividade 3

Prazo de submissão: 15/10/2024

Exercício 1: Crie um programa em `python`[1] capaz de cifrar e decifrar ficheiros de texto (em formato `txt`) usando o `Advanced Encryption Standard (AES)` (ver documentação on-line) em um dos modos de operação discutidos em aula, *i.e.,* `CBC`, `CFB`, `OFB` e `CTR` (ver documentação on-line). O programa deverá receber três parâmetros, o primeiro corresponde ao caminho para ficheiro a ser processado pelo programa, o segundo corresponde ao ficheiro onde o resultado deverá ser escrito e o terceiro parâmetro indica a operação a executar (*i.e.,* `cifrar` ou `decifrar`).

Exemplo de utilização do programa para cifrar e decifrar um ficheiro, respetivamente.

```
# cifrar o conteúdo do ficheiro texto_original.txt
$ python meu_programa.py texto_original.txt texto_cifrado.bin cifrar

# decifrar o conteúdo do ficheiro texto_cifrado.bin
$ python meu_programa.py texto_cifrado.bin texto_decifrado.txt decifrar
```

Para o *exercício 1*, pode considerar que as chaves estão fixadas no próprio código.

Exercício 2: Modifique o programa do *exercício 1* para evitar o uso de chaves fixas no código. Para isso, o seu programa deverá receber como parâmetro um `segredo` a ser convertido em uma chave de tamanho correspondente ao usado pela configuração escolhida do `AES` (*i.e.,* 128, 192 ou 256 bits). Uma sugestão é usar usar funções de síntese seguras (ver link.)
Note que o `vetor de inicialização` deve ser composto por bytes aleatórios e que não precisa ser mantido em segredo, ou seja, pode ser armazenado com o criptograma.

Exemplo de utilização do programa para cifrar e decifrar um ficheiro, respetivamente.

```
# cifrar o conteúdo do ficheiro texto_original.txt
$ python meu_programa.py texto_original.txt texto_cifrado.bin cifrar segredo

# decifrar o conteúdo do ficheiro texto_cifrado.bin
$ python meu_programa.py texto_cifrado.bin texto_decifrado.txt decifrar segredo
```

[1] *O trabalho pode ser feito em uma outra linguagem de programação a escolha.*