Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

Laboratório sobre mecanismos criptográficos

---

1. Considere a classe `CipherLab` disponível no ficheiro `CipherLab.java` (em anexo) a qual implementa um esquema de cifra simétrico. A primitiva criptográfica é o algoritmo DES, modo de operação ECB e não é usado *padding*.

   1.1. Crie o ficheiro `message.txt` com texto em claro (e.g. `"123456789"`). Compile e execute a classe `CipherLab`. Verifique o resultado em `decipher.txt`.

   1.2. Corrija o código fonte tendo em conta que os pontos 2.1 a 2.3 devem manipular apenas os bytes efectivamente lidos do ficheiro. Compile e execute a classe `CipherLab`. Encontre a origem da exceção.

   1.3. Modifique a identificação da transformação para incluir *padding* (e.g. `DES/ECB/PKCS5Padding`). Compile e execute a classe `CipherLab`. Verifique o resultado em `decipher.txt`.

   1.4. Introduza padrões no texto em claro. Verifique que estes padrões passam para o texto cifrado. Corrija o problema usando outro modo de operação.

2. Implemente uma aplicação para gerar *hashs* criptográficos de ficheiros. Gere o *hash* do certificado raíz do IPL (IPL.cer em anexo). Confirme o valor gerado usando o visualizador de certificados do sistema operativo.

ISEL, 2 de Outubro de 2012.