

# Instituto Superior de Engenharia de Lisboa



**ISEL**  
INSTITUTO SUPERIOR DE  
ENGENHARIA DE LISBOA

## Segurança Informática

### *Trabalho 1*

*João Bonacho Nº A49437*

*André Gonçalves Nº A49464*

*Ana Carolina Pereira Nº A49470*

LEIC51D Grupo 07

Semestre de Inverno 2023/2024

28 de Outubro de 2023

## **Parte 1**

### **Exercício 1**

O esquema não cumpre os objetivos uma vez que parte do esquema MAC (*Message Authentication Code*) é utilizado como chave do esquema simétrico, acarretando possíveis vulnerabilidades de segurança. Um atacante pode utilizar os primeiros *bits* do MAC como chave e, de seguida, decifrar o criptograma enviado, dado que o MAC é enviado em claro. As chaves devem ser aleatórias e usadas por pouco tempo.

### **Exercício 2**

A cifra simétrica é menos segura, mas mais rápida que a cifra assimétrica, necessitando apenas de, por exemplo, operações como XOR's e deslocação de bits. Enquanto a cifra assimétrica é mais segura, mas mais lenta que a cifra simétrica, necessitando de, por exemplo, factorização de números primos e multiplicações.

Como habitualmente, os dados são textos em claro de maior dimensão, deve ser utilizada inicialmente uma cifra simétrica de forma a cifrar esses dados. Posteriormente deve ser utilizada cifra assimétrica para cifrar a chave simétrica utilizada, habitualmente de dimensão mais pequena em relação aos dados enviados.

### **Exercício 3**

Os esquemas MAC (*Message Authentication Code*) e Assinatura Digital apresentam semelhanças e diferenças.

Relativamente às **semelhanças** ambas garantem integridade/autenticidade (a mensagem enviada é autêntica) e não garantem confidencialidade (a mensagem não é cifrada).

Relativamente às **diferenças**, o esquema MAC (*Message Authentication Code*) usa chaves simétricas, em oposição à Assinatura Digital que utiliza chaves assimétricas (pública e privada). Outra diferença consiste na validação, i.e., idealmente no MAC apenas o emissor pode autenticar e o recetor validar, enquanto na Assinatura Digital só o emissor pode autenticar, mas qualquer intermediário pode validar a mesma mensagem.

### **Exercício 4.1**

Os certificados podem ser de confiança para um sistema (e.g.:  $S_a$ ) e não de confiança para outro (e.g.:  $S_b$ ) dado que não depende do certificado, mas sim do sistema. Estes podem ter diferentes raízes de confiança que estão instaladas implicitamente.

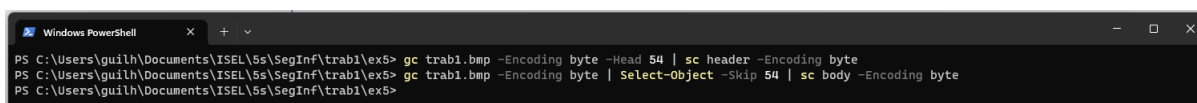
## Exercício 4.2

O mecanismo previsto nos certificados X.509 e no perfil PKIX consiste numa restrição ao uso do certificado (*Basic Constraints*) em que não pode haver certificados folha a meio da cadeia. Cada certificado tem uma extensão que indica se pode assinar certificados.

*“The cA boolean indicates whether the certified public key may be used to verify certificate signatures. If the cA boolean is not asserted, then the keyCertSign bit in the key usage extension MUST NOT be asserted. If the basic constraints extension is not present in a version 3 certificate, or the extension is present but the cA boolean is not asserted, then the certified public key MUST NOT be used to verify certificate signatures.” RFC 5280*

## Parte 2

### Exercício 5.1



```
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> gc trab1.bmp -Encoding byte -Head 54 | sc header -Encoding byte
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> gc trab1.bmp -Encoding byte | Select-Object -Skip 54 | sc body -Encoding byte
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>
```

Figura 1 - comandos Windows PowerShell para separar os bytes do cabeçalho e do corpo da imagem trab1.bmp

## Exercício 5.2

```
Win64 OpenSSL Command Pr X + v
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>openssl enc -des-ecb -e -in body -out body_des_ecb.cif -K 18047f5e9778ee41
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>dir
Volume in drive C is Windows-SSD
Volume Serial Number is 589F-2647

Directory of C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5

29/09/2023 11:49 <DIR>      .
29/09/2023 11:42 <DIR>      ..
29/09/2023 11:45          892,796 body
29/09/2023 11:49          892,800 body_des_ecb.cif
29/09/2023 11:44           54 header
29/09/2023 11:46 <DIR>      prints
29/09/2023 11:42          892,850 trab1.bmp
                4 File(s)      2,678,500 bytes
                3 Dir(s)      749,094,543,360 bytes free

C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>
```

Figura 2 - comando Openssl para cifrar o corpo do BMP com algoritmo DES e modo de operação ECB

```
Win64 OpenSSL Command Pr X + v
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>openssl enc -aes-128-ecb -e -in body -out body_aes_128_ecb.cif -K 42c2771f807215802dff1329fa7bf2cf
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>dir
Volume in drive C is Windows-SSD
Volume Serial Number is 589F-2647

Directory of C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5

29/09/2023 11:53 <DIR>      .
29/09/2023 11:42 <DIR>      ..
29/09/2023 11:45          892,796 body
29/09/2023 11:53          892,800 body_aes_128_ecb.cif
29/09/2023 11:49          892,800 body_des_ecb.cif
29/09/2023 11:44           54 header
29/09/2023 11:50 <DIR>      prints
29/09/2023 11:42          892,850 trab1.bmp
                5 File(s)      3,571,300 bytes
                3 Dir(s)      749,091,049,472 bytes free

C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>
```

Figura 3 - comando Openssl para cifrar o corpo do BMP com algoritmo AES e modo de operação ECB

```
Win64 OpenSSL Command Pr X + v
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>openssl enc -des-cbc -e -in body -out body_des_cbc.cif -iv 7766554433221100 -K 0011223344556677
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>dir
Volume in drive C is Windows-SSD
Volume Serial Number is 589F-2647

Directory of C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5

29/09/2023 11:56 <DIR>      .
29/09/2023 11:42 <DIR>      ..
29/09/2023 11:45          892,796 body
29/09/2023 11:53          892,800 body_aes_128_ecb.cif
29/09/2023 11:56          892,800 body_des_cbc.cif
29/09/2023 11:49          892,800 body_des_ecb.cif
29/09/2023 11:44           54 header
29/09/2023 11:54 <DIR>      prints
29/09/2023 11:42          892,850 trab1.bmp
                6 File(s)      4,464,100 bytes
                3 Dir(s)      749,087,895,552 bytes free

C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>
```

Figura 4 - comando Openssl para cifrar o corpo do BMP com algoritmo DES e modo de operação CBC

```
Win64 OpenSSL Command Pr X + v
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>openssl enc -aes-128-cbc -e -in body -out body_aes_128_cbc.cif -iv 0ed425637bb85abc9798858627b2355d -K 42c2771f807215802dff1329fa7bf2cf
C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>dir
Volume in drive C is Windows-SSD
Volume Serial Number is 589F-2647

Directory of C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5

29/09/2023 11:57 <DIR>      .
29/09/2023 11:42 <DIR>      ..
29/09/2023 11:45          892,796 body
29/09/2023 11:57          892,800 body_aes_128_cbc.cif
29/09/2023 11:53          892,800 body_aes_128_ecb.cif
29/09/2023 11:56          892,800 body_des_cbc.cif
29/09/2023 11:49          892,800 body_des_ecb.cif
29/09/2023 11:44           54 header
29/09/2023 11:56 <DIR>      prints
29/09/2023 11:42          892,850 trab1.bmp
                7 File(s)      5,356,900 bytes
                3 Dir(s)      749,084,078,080 bytes free

C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5>
```

Figura 5 - comando Openssl para cifrar o corpo do BMP com algoritmo AES e modo de operação CBC

## Exercício 5.3

```
Windows PowerShell
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> gc header, body_des_ecb.cif -Encoding byte | sc trab1_des_ecb.bmp -Encoding Byte
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> gc header, body_aes_128_ecb.cif -Encoding byte | sc trab1_aes_ecb.bmp -Encoding Byte
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> gc header, body_des_cbc.cif -Encoding byte | sc trab1_des_cbc.bmp -Encoding Byte
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> gc header, body_aes_128_cbc.cif -Encoding byte | sc trab1_aes_cbc.bmp -Encoding Byte
PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> dir

Directory: C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5

Mode                LastWriteTime         Length Name
----                -
d-----          29/09/2023      11:58             prints
-a-----          29/09/2023      11:45             body
-a-----          29/09/2023      11:57      892880 body_aes_128_cbc.cif
-a-----          29/09/2023      11:53      892880 body_aes_128_ecb.cif
-a-----          29/09/2023      11:56      892880 body_des_cbc.cif
-a-----          29/09/2023      11:49      892880 body_des_ecb.cif
-a-----          29/09/2023      11:44             64 header
-a-----          29/09/2023      11:42      892850 trab1.bmp
-a-----          29/09/2023      12:04      892854 trab1_aes_cbc.bmp
-a-----          29/09/2023      12:03      892854 trab1_aes_ecb.bmp
-a-----          29/09/2023      12:03      892854 trab1_des_cbc.bmp
-a-----          29/09/2023      12:02      892854 trab1_des_ecb.bmp

PS C:\Users\guilh\Documents\ISEL\5s\SegInf\trab1\ex5> |
```

Figura 6 - comandos Windows PowerShell para juntar os resultados anteriores com o cabeçalho



Figura 7 – Imagem DES+ECB



Figura 8 - Imagem AES+ECB

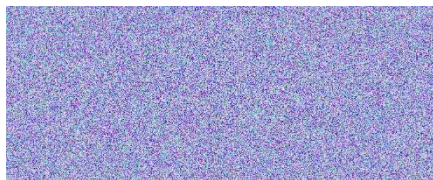


Figura 9 – Imagem DES+CBC

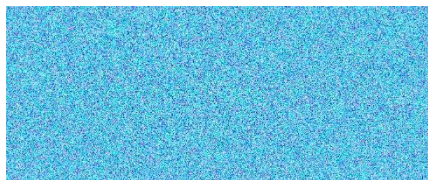


Figura 10 – Imagem AES+CBC

### Observações e conclusões:

1. Comparação: **DES+ECB** (fig. 7) e **DES+CBC** (fig. 9) ou **AES+ECB** (fig. 8) e **AES+CBC** (fig. 10)

Usando **primitivas iguais e modos de operação diferentes** são notórias as vantagens na escolha do modo de operação. Por exemplo, com o modo de operação ECB o atacante consegue interpretar a mensagem.

2. Comparação: **DES+ECB** (fig. 7) e **AES+ECB** (fig. 8) ou **DES+CBC** (fig. 9) e **AES+CBC** (fig. 10)

Usando **primitivas diferentes e modos de operação iguais** não são notórias as vantagens na escolha da primitiva.

### Exercício 6.3

Numa cadeia de 100 blocos, se existir uma mudança de valor da transação no bloco 10, o *hash* do bloco 11 não vai coincidir com o *hash* calculado do bloco 10. Desta forma, a alteração seria detetada no processo de validação/comparação.

### Exercício 6.4

Para poder fazer uma alteração legítima ao valor da transação, é necessário alterar o bloco 11, porque o *hash* do bloco 10 alterou. No entanto, como as outras seguintes dependem dos anteriores, todos os *hashes* dos blocos seguintes ao bloco 10 têm de ser recalculados para que a cadeia permaneça válida.