Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Primeiro Trabalho

Grupo 14 – LEIC53D

47076	Mariana Munoz
47272	João Brito
49751	Beatriz Filipe

Docente: Diego Passos

Realizado no âmbito de Segurança Informática,
do curso de licenciatura em Engenharia Informática e de Computadores
Semestre de Inverno 2023/2024

Outubro de 2023

Parte 1

1.

O esquema não cumpre os objetivos, pois não segue nenhuma das abordagens para a combinação dos esquemas Cifra e MAC. Ou seja, não segue nem a abordagem Encrypt-then-MAC nem a abordagem MAC-then-encrypt.

2.

Porque a cifra assimétrica tem um elevado custo computacional. Assim, como o uso de chaves simétricas tem um menor custo, mas uma menor segurança, é utilizada a cifra assimétrica para o transporte das chaves simétricas, de maneira a protegê-las.

3.

Semelhanças:

- Ambos os esquemas são utilizados para verificar a integridade da mensagem, permitindo ao recetor determinar se os dados não foram alterados durante a transmissão.
- Para além disso, são também usados para verificar a autenticidade dos dados.

Diferenças:

- Um esquema de assinatura digital usa uma chave privada no processo de assinatura (usada apenas pelo remetente), e uma chave pública no processo de verificação (todos podem verificar). Um esquema MAC usa a mesma chave entre o remetente e o recetor, sendo igual no processo de autenticação e verificação.
- Um esquema de assinatura digital usa o par de chaves durante um largo período de tempo enquanto que num esquema MAC, as chaves são normalmente usadas durante pouco tempo.

4.

4.1)

Como o certificado C é emitido por uma Autoridade de Certificação (AC) específica, o sistema S_a pode ter essa AC na sua lista de ACs confiáveis, o que torna os certificados emitidos por essa AC confiáveis para este sistema. Caso o sistema S_b não tenha essa AC na sua lista, os certificados emitidos por ela não serão considerados confiáveis para o sistema S_b.

4.2)

O uso de CRLs (Certificate Revocation List), que são listas emitidas pelas autoridades de certificação, estas, contém informações sobre os certificados que foram invalidados antes da sua data de expiração. O sistema pode então verificar se o certificado aparece na lista para garantir a sua validade.

Questão 5

Para cifrar o corpo do BMP, usámos os seguintes comandos:

- **Cifra AES e CBC:**

  enc -aes-256-cbc -in body -out AESCBC -e -K 00112233445566778899AABBCCDDEEFF00112233445566778899AABBCCDDEEFF -iv AABBCCDDEEFF0011

- **Cifra AES e ECB:**

  enc -aes-256-ecb -in body -out AESECB -e -K 00112233445566778899AABBCCDDEEFF00112233445566778899AABBCCDDEEFF

- **Cifra DES e CBC:**

  enc -des-cbc -in body -out DESCBC -e -K 0123456789ABCDEF -iv AABBCCDDEEFF0011

- **Cifra DES e ECB:**

  enc -des-ecb -in body -out DESECB -e -K 0123456789ABCDEF

Ao juntar cada um dos resultados anteriores ao cabeçalho, obtivemos as seguintes imagens:

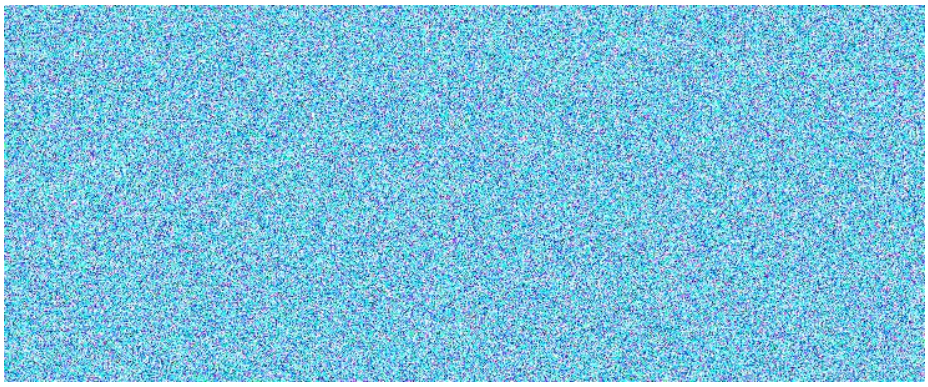

Figura 1 - Cifra AES e CBC

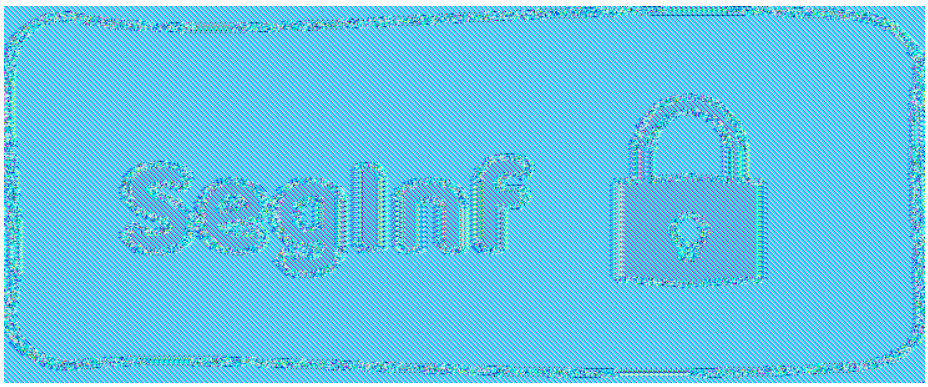

Figura 2 - Cifra AES e ECB

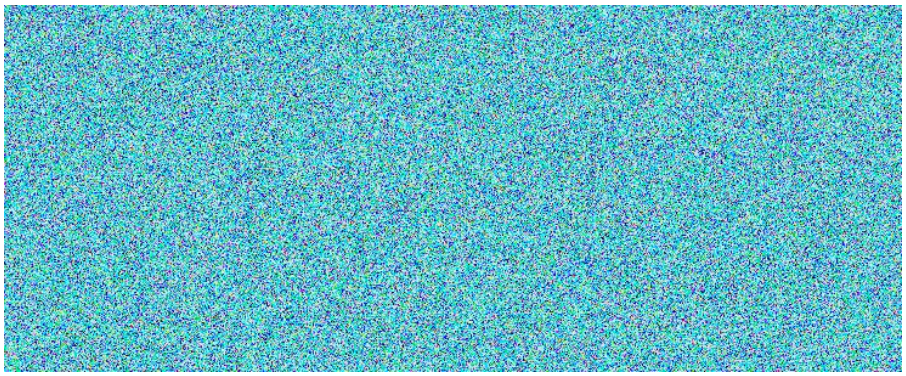

Figura 3 - Cifra DES e CBC

Figura 4 - Cifra DES e ECB

Ao observar as imagens, podemos concluir que, no caso de mensagens com repetição de padrões, o modo ECB é inadequado para manter a confidencialidade, porque os blocos idênticos na mensagem em claro resultam em blocos de criptografia idênticos. Já o modo CBC, por outro lado, devido ao uso do iv e de XOR, os blocos idênticos resultam em blocos de criptografia diferentes.

No caso do uso de AES e DES, o uso de AES permite uma maior segurança. Isto deve-se ao facto de que na cifra AES se pode usar uma chave de dimensão muito maior do que na cifra DES.

Questão 6

6.3)

Um hash de um bloco é calculado através do hash do bloco anterior, o processo de validação irá verificar o hash de cada bloco e confirmá-lo.

Se um atacante alterar o valor da transação do bloco 10, o hash calculado para o bloco 10 será diferente do hash que foi originalmente armazenado no bloco 11. Logo, quando o processo de validação atingir o bloco 11 e calcular o hash do bloco 10, este não irá corresponder ao valor esperado.

O processo de validação, neste ponto, deve parar e sinalizar um erro de integridade, indicando que a cadeia de blocos foi comprometida.

6.4)

Ao realizar uma alteração legítima do valor da transação do bloco 10, o seu hash terá de ser recalculado e o seu valor irá mudar. Como um hash é calculado baseado no hash do bloco anterior, o valor de hash do bloco 11 terá de ser modificado para a cadeia continuar válida, e assim por diante. Logo, todos os blocos a partir deste até ao último bloco da cadeia teriam de ter os seus valores de hash recalculados e atualizados.