CIC0201 - Segurança Computacional - Turma 01

Saulo Oliveira de Freitas - 211000176

Advanced Encryption Standard (AES)

1. Introdução

Considerada padrão para a indústria de criptografia de dados, a Advanced Encryption Standard (AES) é um tipo de cifra de bloco de chave simétrica que utiliza um algoritmo de cifragem de fluxo de substituição-transposição (S-box) para substituir cada byte de texto por outro byte, e um algoritmo de mistura de colunas para misturar os bytes do texto cifrado. Através destes processos é possível realizar a cifrar dados de forma eficiente e segura.

1.1 Objetivos

Para demonstrar as propriedades conceituais e práticas deste recurso, a AES será implementada com a opção de cifragem em formato ECB e CTR. Espera-se que o produto final seja capaz de:

- Cifragem e Decifragem de texto em modo ECB
- Cifragem e Decifragem de texto em modo CTR
- Cifragem e renderização de imagem

2. Metodologia

A linguagem adotada para este projeto foi Python, devido a sua simplicidade de uso e sintaxe familiar. Além do AES foram também desenvolvidas implementações dos algoritmos de Optimal asymmetric encryption padding (OAEP) e RSA (Rivest–Shamir–Adleman) para viabilizar o processo.

OAEP.py A função do OAEP é prover o preenchimento e formatação dos dados que serão utilizado pelo algoritmo de RSA, garantindo maior segurança ao resultado final do processo de cifragem. Pontos principais de sua implementação são:

- A mensagem é preenchida com valores randômicos para aumentar seu tamanho e entropia
- A mensagem então é cifrada utilizando a chave pública, obtida através do RSA.
- Para a decifragem, a chave privada é utilizada, realizando o processo de cifragem no sentido inverso.
- Os preenchimentos são extraidos e a mensagem original é recuperada.

RSA.py O RSA é um algoritmo de cifragem assimétrico amplamente utilizado para a transmissão segura de dados. Sua implementação envolve o uso de números primos para geração de um par de chaves público-privada. Sua implementação pode ser dividida em:

- Gere um par de chaves público-privada utilizando a função `spawn_keys()` e as extraia
- Converta a mensagem em formato textual para uma representação numérica.
- Cifre o resultado utilizando a chave pública e a função `cypher(key, msg)`
- Decifre utilizando a chave privada e a função `decypher(key,ciphered_text)`
- Converta a representação numérica resultante para seu formato original

AES.py A AES será implementada no tamanho de 128 bits para bloco e chave. Um processo de implementação convencional geralmente envolve os seguintes passos:

- Geração de chave no tamanho desejado através da função `expand_key(key)`
- Geração do vetor de inicialização
- Aplicar os paddings e conversões necessárias
- Cifrar e/ou decifrar utilizando a função `cipher(block, keys)`

3. Resultados

```
-------------------------------------------------
Trabalho 2  - Segurança Computacional
Advanced Encryption Standard (ECB, CTR)
Aluno: Saulo Freitas - 211000176
-------------------------------------------------
INICIAR AS CHAVES? (S/N)
```

3.2 Cifragem/Decifragem

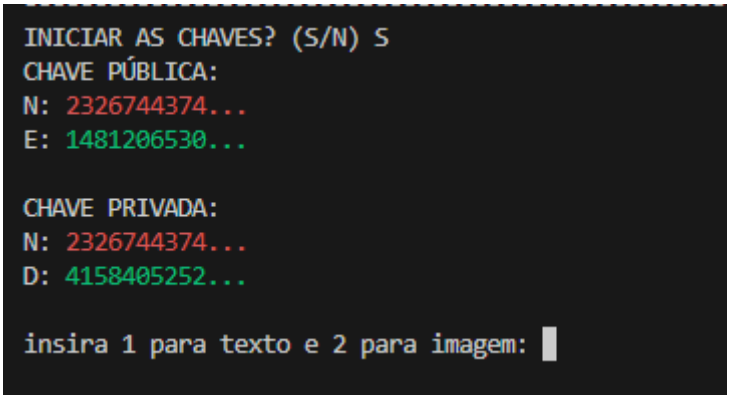

Figure 1: Geração de chaves

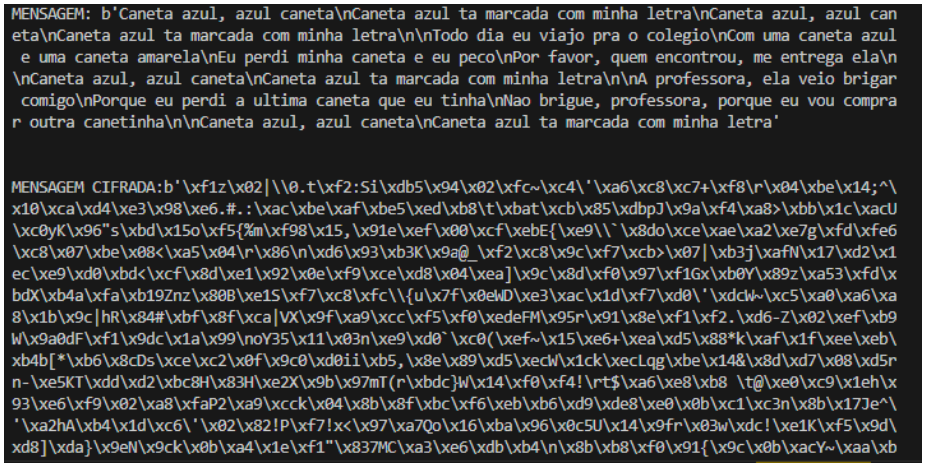

Figure 2: Cifragem do arquivo

Figure 3: Produtos do processo de cifragem

```
NOME DO ARQUIVO A SER DECIFRADO: bluepen.txt
Verificando assinatura...


Assinatura confere

MENSAGEM:

b'Caneta azul, azul caneta\nCaneta azul ta marcada com minha letra\nCaneta azul, azul caneta\nCanet
a azul ta marcada com minha letra\n\nTodo dia eu viajo pra o colegio\nCom uma caneta azul e uma can
eta amarela\nEu perdi minha caneta e eu peco\nPor favor, quem encontrou, me entrega ela\n\nCaneta a
zul, azul caneta\nCaneta azul ta marcada com minha letra\n\nA professora, ela veio brigar comigo\nP
orque eu perdi a ultima caneta que eu tinha\nNao brigue, professora, porque eu vou comprar outra ca
netinha\n\nCaneta azul, azul caneta\nCaneta azul ta marcada com minha letra'
```

Figure 4: Decifragem do arquivo

```
insira 1 para texto e 2 para imagem: 2

NOME DO ARQUIVO A SER CIFRADO: image.jpg
Round 1: Image encrypted and saved as c:\Users\saulo\Desktop\slides matéria\SC\SC-Trab2\image.jpg.e
ncrypted_round_1
Round 5: Image encrypted and saved as c:\Users\saulo\Desktop\slides matéria\SC\SC-Trab2\image.jpg.e
ncrypted_round_5
Round 9: Image encrypted and saved as c:\Users\saulo\Desktop\slides matéria\SC\SC-Trab2\image.jpg.e
ncrypted_round_9
Round 13: Image encrypted and saved as c:\Users\saulo\Desktop\slides matéria\SC\SC-Trab2\image.jpg.
encrypted_round_13
Deseja Decifrar? (S/N)
```

Figure 5: Cifragem de Imagem em modo CTR