

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 extraídos 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

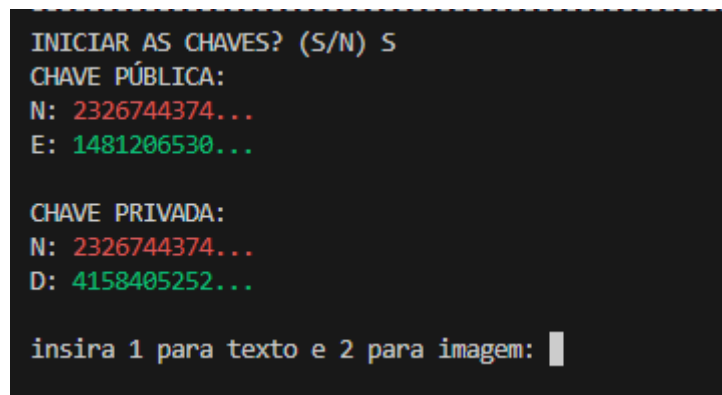


Figure 1: Geração de chaves

```

MENSAGEM: b'Caneta azul, azul caneta\nCaneta azul ta marcada com minha letra\nCaneta azul, azul caneta\nCaneta azul ta marcada com minha letra\n\nTodo dia eu viajo pra o colegio\nCom uma caneta azul e uma caneta amarela\nEu perdi minha caneta e eu peço\nPor favor, quem encontrou, me entrega ela\n\nCaneta azul, azul caneta\nCaneta azul ta marcada com minha letra\n\nA professora, ela veio brigar comigo\nPorque eu perdi a ultima caneta que eu tinha\nNao brigue, professora, porque eu vou compra r outra canetinha\n\nCaneta azul, azul caneta\nCaneta azul ta marcada com minha letra'

MENSAGEM CIFRADA: b'\xf1z\x02|\0.t\xf2:Si\xdb5\x94\x02\xfc~\xc4\''\xa6\xc8\xc7+\xf8\r\x04\xbe\x14;\^\\x10\xca\x04\xe3\x98\xe6.#.: \xac\xbe\xaf\xbe5\xed\x08\t\xbat\xcb\x85\xdbpJ\x9a\x04\xfa8+\xb8\x1c\xacU\x00yK\x96"s\xbd\x15o\x0f5{\%m\x0f98\x15,\x91e\xef\x00\xcf\xebE{\xe9\\'\x8d\xce\xae\x02\x07\xfd\xfe6\x08\x07\xbe\x08<\xa5\x04\r\x86\n\x06\x93\x03K\x9a@\_ \xf2\x08\x9c\x07\xcb>\x07|\xb3j\xafN\x17\x02\x1ec\x09\x0d\x0bdc\x0f\x0d\x0e1\x92\x0e\x0f9\xce\x08\x04\x0a]\x9c\x0d\x0f9\x07\x01Gx\x089z\xa53\xfd\xbdX\x04a\xfa\x0b19Znz\x0808\xe15\x0f7\x08\x0c\x0f{\u\x07f\x0eW\x03\x0c\x0d\x0f\x0d0'\x0dclw~\xc5\x0a0\xa6\xa8\x1b\x0c|hR\x84#\xbfx8f\x0ca|VX\x0f\x09\x0c\x0f5\x0f0\x0eFm\x095r\x091\x0e\x0f1\x0f2.\x06-Z\x02\x0ef\x0b9W\x09a0dF\x0f1\x09dc\x1a\x09\n0Y35\x11\x03n\x09\x0d0'\x0c0(\x0f~\x15\x0e6+\x0a\x0d5\x088*k\x0af\x1f\x0e\x0b\x0b4b[*\xb6\x08Ds\x0c\x02\x0f\x09c0\x0d0i'\xb5,\x0e\x089\x0d5\x0ecW\x1ck\x0ecLqg'\xb0\x14&\x0d\x07\x08\x0d5r n~\x0e5KT\x0d\x02\x0b8H\x03H\x0e2X\x09b\x097mT(r\x0bdc)W\x14\x0f0\x0f4!\rt$ \xa6\x08\x0b8 \t0\x0e\x0c9\x1eh\x093\x0e6\x0f9\x02\xa8\x0faP2\xa9\x0cck\x04\x08b\x08f\x0c\x0f6\x0eb\x06\x0d9\x0e8\x0e0\x0b\x0c1\x0c3n\x08b\x17Je^'\xa2hA\x0b4\x1d\x0c6'\x02\x082!P\x0f7!x<\x07\xa7Qo\x16\x0ba\x06\x0c5U\x14\x09fr\x03w\x0dc!\xe1K\x0f5\x09d\x0d8]\x0da}\x0eN\x09ck\x0b\xa4\x1e\x0f1"\x037MC\xa3\x06\x0db\x04n\x08b\x0b8\x0f0\x091{\x0c\x0b\x0cY~\xaa\x0b

```

Figure 2: Cifragem do arquivo

```

CHAVE DA SESSÃO: b'\xb8\x05I\x05\x06\x03\xab\x89\xcb\x90GB\x0c\x97\x93b\W\x0fjx\x02\x0c\x91\x07tW\x89\x12U`e'

CHAVE DA SESSÃO CIFRADA: LsBz4CDqMM7FwIV/2GeBjOY4U/F3mat3LRMatJMMRazA5/voOGmmdb27WuTabME0JBw5NIRvK1-Z2B9o1OGRr7ocZdx269WJUpTrdt1KMfL5kVoD3NjvX1dGjY0afULDoZ8sBGKaqlDUwnRjHwHAmB2+XJy2Pz+3ImZa1NCALAwZ-31sJE8/wmsPC89/rrDrqLbkX0JLsbUMS1ZuNYXo4IamT1mUPTWAN773cv24dzKotBWS9ahUzz5tTt11j02mMd8Z03CedWPFtFJdPN1ja27VMTgszukXgv7gtgvb9yxK2VUK4Att5uZFVeohHPcB+XJhZtLd6rpu2AgNa0g==

ASSINATURA: psCwQB7FBU+PMU/3a1zcXqLA0iXu/K196Trq7TznoRAqcrj3KQrewGrG2qVVeRhpBYLpyKkUXGcN9AOCNnyBKz1rfk+8a1QvrZtXvjbCBXH17IAd3dosmnuHi5dtRXaldHcpkko9n4JLB5PpgFJw+AkM3bgkMXXPuFnQ3Z3zz6QshgTGC2/LE7wEBxoJFPWbXqd4u3DEFFdB7qGmOvbwCOWUNmiYWeakcXUY6mEbZgIzPz2pgyM/UrUDkInEp6uv8dqBjuShh3YP1ZB59IYz7K9it9AtUQF66y7Gnt5Art93DMIM9S5GzEk+ReUwbEekdPeOyDGBJGRNX5vV3sIQ==

Deseja decifrar? (S/N)

```

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 peço\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