

Relatório Segurança de Sistemas

AES CBC e CTR:

Encriptação e Decriptação

Hugo Neto¹

¹Escola Politécnica - Faculdade de Informática (PUCRS)

Porto Alegre – RS – Brazil

Github: <https://github.com/hugonn/aes-sha>

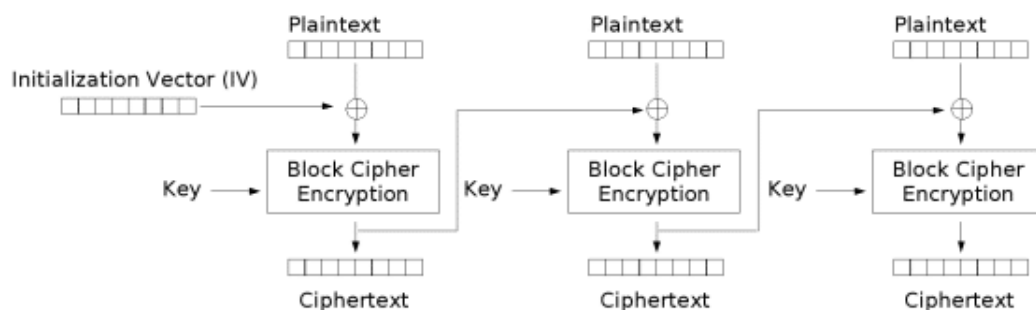
1. Introdução

O intuito deste relatório é demonstrar, resumidamente, o funcionamento e a implementação de um sistema que encripta/decrypta mensagens utilizando a técnica de encriptação AES e demonstrar dois modos de operação, CBC e CTR. A tecnologia escolhida foi a linguagem Python que faz uso da biblioteca PyCrypto. O AES é um método de encriptação simétrica que faz o uso de blocos de 16 bytes e um "bloco falso" (IV/ Vetor de Inicialização) que é utilizado no início do processo de encriptação de cada encriptação dos blocos. Esta técnica é extremamente segura. Tendo em vista que, na força bruta, é muito difícil de quebrar uma cifra que foi encriptada com o método AES.

2. Modos de Operação AES

O AES possui vários modos de operação, mas apenas dois foram explorados nesse sistema:

- CBC: Na encriptação, todos os blocos não cifrados realizam uma operação de XOR com os 16 bytes iniciais do bloco anterior. O primeiro bloco faz esta operação utilizando o IV, enquanto que os blocos subsequentes utilizam os 16 bytes iniciais do bloco antecedente. Isso garante a aleatoriedade e segurança da cifra.



Cipher Block Chaining (CBC) mode encryption

Figura 1. Modo: CBC

- CTR: Esse modo cria uma cifra de fluxo onde, para cada bloco de texto não criptografado, é feita uma operação XOR com um contador que é incrementado antes de cada cifragem nos blocos subsequentes.

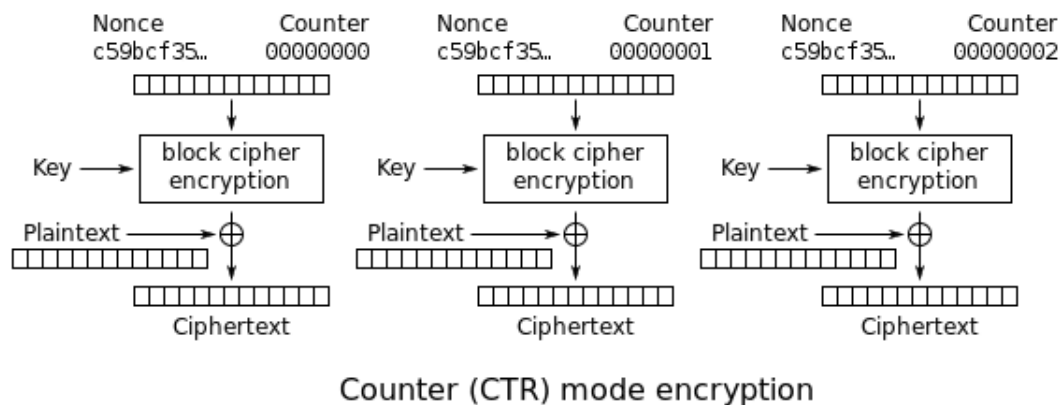


Figura 2. Modo: CTR

3. Implementação

A tecnologia escolhida foi Python em conjunto com a biblioteca PyCrypto. O intuito de utilizar essa tecnologia foi aprender uma linguagem na qual não possuía conhecimento.

As imagens abaixo demonstram partes da implementação do sistema de encriptação/decriptação:

```
def encrypt(key, source, encode=True):
    source = unhexlify(source)
    key = unhexlify(key)
    IV = Random.new().read(16) # Gera IV
    encryptor = AES.new(key, AES.MODE_CBC, IV) #Encripta
    padding = AES.block_size - len(source) % AES.block_size # Calcula PAD
    source += bytes([padding]) * padding # Padding
    data = IV + encryptor.encrypt(source) # IV + Cifra
    return hexlify(data)
```

Figura 3. Modo: CBC Encrypt

```
#Arquivo que contem o decriptador AES_hex
def decriptar_hex(cifra, chave):
    cifra = unhexlify(cifra) #Transforma em bytes a informação que está hexa
    chave = unhexlify(chave) #Transforma em bytes a informação que está hexa
    IV = cifra[:16] #Recupera o IV dos 16 primeiros bytes
    aes_obj = AES.new(chave, AES.MODE_CBC, IV) #Utiliza função do PyCrypto
    texto = aes_obj.decrypt(cifra[16:]) #Decripta a mensagem sem o IV
    padding = texto[-1] #Retira o pad
    return bytes.decode(texto[:-padding]) #Decodifica os Bytes
```

Figura 4. Modo: CBC Decrypt

As partes do código mostradas acima, são responsáveis pela encriptação e decriptação, respectivamente, utilizando o método AES com modo de operação CBC. Dentro do problema proposto, foi necessário transformar as cifras/texto claro da base hexadecimal para base decimal e, subsequentemente, criar um IV randômico para encriptar e para decriptar recuperar os primeiros 16 bytes do primeiro bloco da cifra. Foi utilizado PKCS5 para encriptar as cifras no modo CBC.

```
def int_of_string(s):  
    return int(binascii.hexlify(s), 16) # Contador aleatorio por conta do CTR  
  
def encrypt_CTR(key, texto):  
    texto = unhexlify(texto) #Transforma em bytes a informação que está hexa  
    key = unhexlify(key) #Transforma em bytes a informação que está hexa  
    iv = Random.new().read(16) #Cria o "bloco falso"  
    ctr = Counter.new(128, initial_value=int_of_string(iv)) #cria objeto que encripta no modo CTR  
    aes = AES.new(key, AES.MODE_CTR, counter=ctr) #encripta cifra  
    return hexlify(iv + aes.encrypt(texto))
```

Figura 5. Modo: CTR Encrypt

```
def int_of_string(s):  
    return int(binascii.hexlify(s), 16) #contador aleatorio por conta do CTR  
  
def decrypt_CTR(key, cifra):  
    cifra = unhexlify(cifra) #Transforma em bytes a informação que está hexa  
    key = unhexlify(key) #Transforma em bytes a informação que está hexa  
    iv = cifra[:16] #Cria o "bloco falso"  
    ctr = Counter.new(128, initial_value=int_of_string(iv)) #Cria objeto AES em modo CTR  
    aes = AES.new(key, AES.MODE_CTR, counter=ctr) # Decripta cifra  
    return bytes.decode(aes.decrypt(cifra[16:]))
```

Figura 6. Modo: CTR Decrypt

As imagens acima demonstram como foi feita a encriptação/decriptação utilizando a técnica AES em modo CTR. O contador randômico é utilizado para encriptar blocos subsequentes. Na decriptação, a cifra é transformada de hexadecimal para decimal e, após isso, é criado o objeto AES que decripta as mensagens propostas no trabalho.

Abaixo, estão os resultados das encriptações e decriptações do AES tanto no modo CTR quando no CBC.

3.1. Encriptação Modo CBC

- Chave : "140b41b22a29beb4061bda66b6747e14"
- Mensagem Clara: "Next Thursday one of the best teams in the world will face a big challenge in the Libertadores da America Championship."
- Mensagem Cifrada: "d9087517ebc8ed2fb3f6f450377bc86c4c0b25110537d67685a60f6f1ce5d241c10cda4b6d59cf8540082c907e2f1d64f02c4381220b853ec3a04dc7df37ea39977d619320cdf8eca989f20e245f3efc7849a234260639f28"

dad4cd28d705f70839cd0b82ef9458b7dcdd4f8502527b251a3
dfcecca694e0c642382da0fe174909745c773f7be66dfadde23d1e0a309"

3.2. Decriptação Modo CBC

- Chave: "140b41b22a29beb4061bda66b6747e14"
- Mensagem Cifrada: "4ca00ff4c898d61e1edbf1800618fb2828a226d160dad07883d04e008a7897ee2e4b7465d5290d0c0e6c6822236e1daafb94ffe0c5da05d9476be028ad7c1d81"
- Mensagem Clara: "Basic CBC mode encryption needs padding."

- Mensagem Cifrada: "5b68629feb8606f9a6667670b75b38a5b4832d0f26e1ab7da33249de7d4afc48e713ac646ace36e872ad5fb8a512428a6e21364b0c374df45503473c5242a253"
- Mensagem Clara: "Our implementation uses rand. IV"

3.3. Encriptação Modo CTR

- Chave: "36f18357be4dbd77f050515c73fcf9f2"
- Mensagem Clara: "This is a sentence to be encrypted using AES and CTR mode."
- Mensagem Cifrada: "131b32ca4dae290b6c6c28095954a6a8649f253b0fe12c856be7706b6f848936737ffa6363c19b9abd1ae530ca96581bc849ff285d652257ea78a53f6df539f1e4e0ef91ffe50aadba12"

3.4. Decriptação Modo CTR

- Chave: "36f18357be4dbd77f050515c73fcf9f2"
- Mensagem Cifrada: "69dda8455c7dd4254bf353b773304eec0ec7702330098ce7f7520d1cbbb20fc388d1b0adb5054dbd7370849dbf0b88d393f252e764f1f5f7ad97ef79d59ce29f5f51eeca32eabedd9afa9329"
- Mensagem Clara: "CTR mode lets you build a stream cipher from a block cipher."

- Mensagem Cifrada: "770b80259ec33beb2561358a9f2dc617e46218c0a53cbeca695ae45faa8952aa0e311bde9d4e01726d3184c34451"
- Mensagem Clara: "Always avoid the two time pad!"

4. Conclusão

A metodologia de encriptação AES continua sendo muito utilizada nos dias de hoje devido a sua eficiência e segurança dos dados. Pode-se dizer que é impossível quebrar as cifras AES tendo em vista que só consegue-se saber o que tem nas mensagens cifradas caso a chave seja conhecida. Sendo assim, este trabalho foi motivador e foi de suma importância para a aprendizagem desse método de encriptação.

Referências

Morais, J. (2017). Criptografia aes. Último Acesso: 20 Novembro de 2018.