Relatório - Cifra de bloco

INGRID LORRAINE RODRIGUES DA SILVA - 160125260
JOÃO VICTOR R. DA SILVA - 160127815

Dep. Ciência da Computação - Universidade de Brasília (UnB)

1. Introdução

O presente documento visa descrever a implementação dos processos de codificação e decodificação utilizando a cifra de bloco AES (Advanced Encryption Standard), para os modos ECB (Electronic CodeBook) e CTR (Counter). Abaixo, iremos descrever brevemente a Cifra de Vigenère, as decisões tomadas para implementação de cada algoritmo (codificação, decodificação e ataque) e suas particularidades.

2. Cifra de bloco AES

Estabelecida em 2001 pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) [NIST 2001], a cifra de bloco AES é uma variante da cifra de bloco Rijndael criada pelos criptógrafos Joan Daemon e Vincent Rijmen [Daemon 2003]. A cifra AES, no seu modo de 128 bits (AES-128), trabalha sobre matrizes 4x4 de 16 bytes denominadas de estados, durante a cifragem e decifragem são aplicados 10 rodadas do algoritmo correspondente, tendo como entrada o texto claro como entrada durante a cifragem e o texto cifrado na decifragem.

A descrição em alto nível do algoritmo de cifragem segue abaixo:

1. Expansão de chave: a partir da chave informada são derivadas chaves a serem aplicadas em cada rodada usando o algoritmo de expansão de chave AES key schedule.
2. Rodada inicial: XOR bit a bit entre o estado e a chave para a rodada 0.
3. Rodadas intermediárias (1 a 9):
    a. Substituição de bytes: cada byte do estado é substituído por um correspondente de acordo com a tabela Rijndael S-box.
    b. Deslocamento de linhas: Deslocamento à esquerda das linhas 1 a 3 do estado, os elementos da linha são deslocados de acordo com o número da linha, ou seja, uma posição para linha 1, dois para a linha 2 e por fim três posições para a linha 3.
    c. Combinação de colunas: Produto de matrizes entre o estado e a matriz Rijndael MixColumns. Essa pode ser simplificada usando uma implementação baseada nas tabelas das multiplicações, dessa forma as multiplicações sobre o campo Galois de Rijndael são substituídas por consultas nas tabelas correspondentes.
    d. Somar chave da rodada: XOR bit a bit entre o estado e a chave para a rodada *n*.
4. Rodada final:
    a. Substituição de bytes.
    b. Deslocamento de linhas.
    c. Somar chave da rodada.

De forma análoga a cifragem, o processo de decifragem segue os mesmos passos da cifragem em ordem reversa com algumas modificações. O algoritmo em alto nível da decifragem segue abaixo:

1. Expansão de chave: a partir da chave informada são derivadas chaves a serem aplicadas em cada rodada usando o algoritmo de expansão de chave AES key schedule.
2. Rodada inicial: XOR bit a bit entre o estado e a chave para a rodada 10.
3. Rodadas intermediárias (9 a 1):
    a. Substituição de bytes inversa: cada byte do estado é substituído por um correspondente de acordo com a tabela Rijndael Inverse S-box.
    b. Deslocamento de linhas inverso: Deslocamento à direita das linhas 1 a 3 do estado, os elementos da linha são deslocados de acordo com o número da linha, ou seja, uma posição para linha 1, dois para a linha 2 e por fim três posições para a linha 3.
    c. Combinação de colunas inversa: Produto de matrizes entre o estado e a matriz Rijndael Inverse MixColumns. Assim como a combinação de colunas da cifragem, essa pode ser simplificada usando uma implementação baseada nas tabelas das multiplicações, dessa forma as multiplicações sobre o campo Galois de Rijndael são substituídas por consultas nas tabelas correspondentes.
    d. Somar chave da rodada: XOR bit a bit entre o estado e a chave para a rodada *n*.
4. Rodada final:
    a. Substituição de bytes inversa.
    b. Deslocamento de linhas inverso.
    c. Somar chave da rodada.

3. Modo contador (CTR)

O modo contador muda a forma de funcionamento da cifra AES de uma cifra de blocos para uma cifra de fluxos de dados, pois nesse modo a cifra tem como entrada um vetor de entrada qualquer, também conhecido como *nonce*, que é somado ao valor de um contador. Todas as etapas seguem como no modo ECB, porém o bloco cifrado foi gerado a partir do *nonce* somado ao contador, para cifrar o texto claro, ao final da cifragem do bloco é feito o XOR bit a bit entre o bloco cifrado e o texto claro.

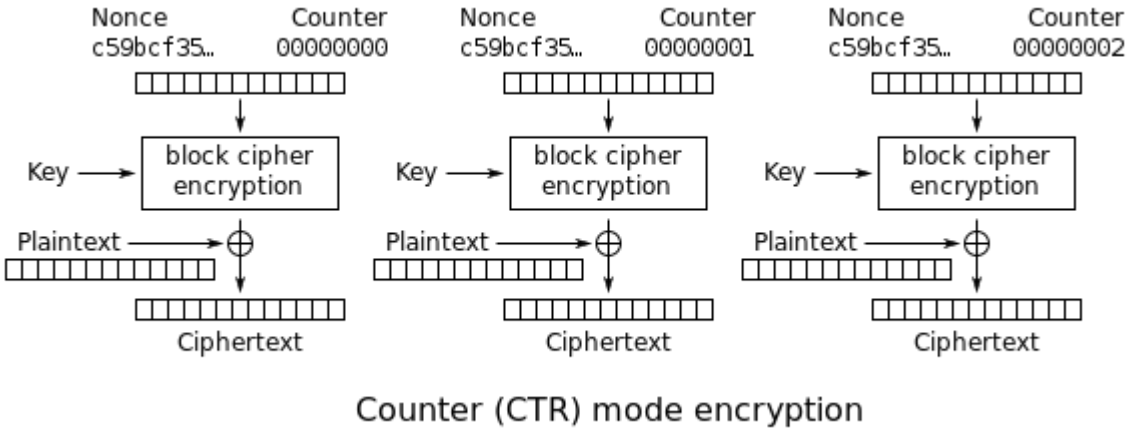

Figura 1. Exemplo da cifragem usando AES em modo CTR

4. Resultados

Os algoritmos de cifragem, decifragem e modo CTR foram testados com os vetores de testes presentes no projeto, tendo resultado de acordo com o esperado. Embora os algoritmos citados possam ser implementados com paralelismo para acelerar a cifragem e decifragem, a abordagem utilizada durante a implementação não utilizou paralelismo, isso pode impactar o desempenho do programa para grandes arquivos. Para os vetores de testes utilizados, não foi notado um impacto significativo da falta de paralelismo.

O código fonte está disponível no repositório do github no seguinte link: https://github.com/joao-victor-silva/simple-aes.

5. Conclusões

A cifra de bloco AES é um método sofisticado e eficiente de cifragem e decifragem, especialmente do ponto de vista de performance. Para a época que foi criada, a cifra era eficiente, porém ainda apresentava falhas como possibilidade de identificação de padrões no modo ECB. Sua eficiência pode ser melhorada utilizando o modo CTR, tornando a cifra menos vulnerável a identificação de padrões, ainda mantendo sua ótima performance por permitir o paralelismo durante a cifragem e decifragem.

6. Referências

[NIST 2001] United States National Institute of Standards and Technology (NIST). (2001). "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). Federal Information Processing Standards Publication 197.

[Daemon 2003] Daemen, Joan, Rijmen, Vincent. (2003). "AES Proposal: Rijndael" (PDF). National Institute of Standards and Technology. p. 1.