Entendendo e Implementando AES-256

Objetivo

Explorar o funcionamento interno do algoritmo de criptografia simétrica AES-256 e praticar sua aplicação através de um exemplo de código em uma linguagem de sua escolha.

Enunciado

1. **Introdução Teórica**
    - Explique, com suas próprias palavras, os fundamentos do AES (Advanced Encryption Standard):
        - **Estrutura de bloco**: tamanho do bloco, chave e número de rodadas em AES-256.
        - **SubBytes, ShiftRows, MixColumns e AddRoundKey**: descreva cada etapa do ciclo de criptografia.
        - **Expansão de chave (Key Schedule)**: como a chave de 256 bits é derivada para as subchaves de cada rodada.
        - **Modo de operação**: escolha um (por exemplo, CBC, GCM ou CTR) e justifique sua seleção, explicando brevemente como ele garante confidencialidade (e autenticação, se aplicável).
2. **Exemplo Prático**
    - Implemente um pequeno programa que:
        - Gera (ou recebe) uma **chave de 256 bits** (32 bytes).
        - Recebe uma **mensagem de texto** do usuário (mínimo 16 bytes; se precisar, aplique padding PKCS#7).
        - Criptografa essa mensagem usando AES-256 no modo escolhido.
        - Exibe o **ciphertext** (por exemplo, em Base64 ou hexadecimal).
        - Descriptografa o ciphertext de volta ao texto original e exibe-o para validação.
    - **Requisitos do código**:
        - Use uma biblioteca de criptografia amplamente adotada na linguagem escolhida (por exemplo, `javax.crypto` em Java, `cryptography` em Python, `crypto` em Node.js, `System.Security.Cryptography` em C#, etc.).
        - Inclua **comentários** em cada bloco de código, explicando:

- Como você configurou o cipher (tamanho de chave, modo, IV).
- Como o padding e a geração do IV foram tratados.
- Como o processador de blocos realiza cada etapa do AES.

3. **Entrega**
    - Documento em PDF ou Markdown contendo:
        - A **explicação teórica** completa (mínimo 400 palavras).
        - O **código-fonte** comentado.
        - **Prints** ou logs demonstrando a criptografia e a descriptografia funcionando corretamente.
4. **Critérios de Avaliação**
    - **Clareza e profundidade** da explicação teórica (30%).
    - **Correção e boas práticas** de implementação (40%).
    - **Qualidade dos comentários** e demonstrações (30%).

Prazo de entrega: Conforme Tarefa do Teams

—

Esta tarefa visa consolidar seu entendimento de cifragem de blocos e a importância de parâmetros como chave, IV e modo de operação no uso seguro do AES-256. Boa sorte!