Trabalho de Implementação 2 – Cifra de bloco e modo de operação CTR

2020/2

Alan Fontenele Véras – 200013335

Welder Cavalcante de Oliveira – 190039582

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

1. Introdução

A cifra de bloco AES (Advanced Encryption Standard) é um algoritmo de criptografia amplamente utilizado para proteger informações confidenciais. O modo de operação CTR (Counter Mode) é uma técnica que permite criptografar dados de forma eficaz, fornecendo segurança e confidencialidade.

Neste projeto, nosso objetivo principal é implementar completamente as operações de codificação, decodificação e análise de vulnerabilidades usando a cifra de bloco AES no modo de operação CTR. O AES é um algoritmo moderno e altamente seguro, amplamente adotado em contextos contemporâneos para proteger dados sensíveis.

Estamos aprimorando nossa implementação com recursos adicionais do curso e pesquisando fontes online confiáveis para garantir a excelência do projeto. Este esforço visa não apenas dominar a técnica, mas também compreender profundamente a importância da criptografia ao longo da história e em contextos contemporâneos.

Através deste projeto, apresentaremos uma abordagem abrangente para codificar, decodificar e explorar vulnerabilidades na cifra de bloco AES no modo de operação CTR.

2. Descrição e implementação

AES (Advanced Encryption Standard):

1. O AES é um algoritmo de criptografia simétrica amplamente adotado, estabelecido como um padrão de criptografia pelo NIST (Instituto Nacional de Padrões e Tecnologia dos EUA).
2. Ele é projetado para criptografar blocos de dados de tamanho fixo, com tamanhos de chave de 128, 192 ou 256 bits.
3. O AES utiliza uma chave de criptografia para realizar operações de substituição e permutação em cada bloco de dados.
4. É altamente seguro e capaz de resistir a ataques de força bruta devido à variedade de tamanhos de chave e suas propriedades criptográficas sólidas.

5. O AES é amplamente empregado em sistemas de segurança, comunicações seguras e proteção de dados sensíveis.

Modo de Operação CTR (Counter Mode):

1. O modo CTR é uma técnica de criptografia que pode ser aplicada com o AES e outros algoritmos de cifra de bloco.
2. Neste modo, os dados são criptografados usando uma sequência de blocos de valor único chamados "contadores".
3. Esses contadores são combinados com uma chave para gerar um fluxo de dados cifrados.
4. O fluxo cifrado é então combinado (por operação XOR) com os dados originais para fornecer a criptografia.
5. O modo CTR permite a criptografia e descriptografia de dados de forma paralela, tornando-o eficiente em implementações de hardware e software.
6. É altamente recomendado para aplicativos onde a eficiência é fundamental, como streaming de dados ou sistemas que exigem criptografia de alta velocidade.

Projeto Implementado: No contexto do projeto implementado, o AES no modo CTR está sendo usado para criptografar dados de forma segura e eficiente. O AES fornece uma camada robusta de criptografia de bloco, enquanto o modo CTR permite a transformação de blocos individuais de dados em texto cifrado usando contadores exclusivos. Essa combinação garante a proteção de informações confidenciais, mantendo a integridade e a confidencialidade dos dados, seguindo práticas recomendadas de segurança criptográfica.

Descrição da implementação junto a fotos resultados

A função ***ctr*** inicializa um contador (inicialmente definido como todos os zeros), gera uma lista chamada ***blocos_gerados*** para armazenar os blocos criptografados e, em seguida, itera sobre os blocos de entrada. Para cada bloco de entrada, ele criptografa o valor atual do contador (na forma de matriz) e faz um XOR com o bloco de entrada para produzir o bloco de texto cifrado. O contador é então incrementado, e o processo continua para o próximo bloco de entrada.

A função ***aes_cifrar*** é a implementação da cifragem AES (Advanced Encryption Standard).

- **Chave inicial (Round 0):** A função começa pela aplicação da operação ***add_round_key***, onde a chave da rodada é combinada com o estado do bloco usando operação XOR.
- **Rounds (Rodadas):** A função entra em um loop que executa um conjunto de operações para cada rodada de 1 até rodadas - 1. As operações realizadas em cada rodada são as seguintes:

- **SubBytes:** Substituição de bytes no estado usando uma tabela de substituição (S-Box).
- **ShiftRows:** Deslocamento das linhas da matriz de estado.
- **MixColumns:** Mistura das colunas do estado (operação de mistura linear).
- **AddRoundKey:** Adição da chave da rodada atual usando a operação XOR.
- **Última Rodada:** Após a última rodada, as etapas de **SubBytes**, **ShiftRows** e **AddRoundKey** são realizadas novamente.
- A função retorna o estado do bloco após todas as rodadas, que é o bloco de texto cifrado.

Testes:

Figura 1 - Round 1

Figura 2 - Round 5

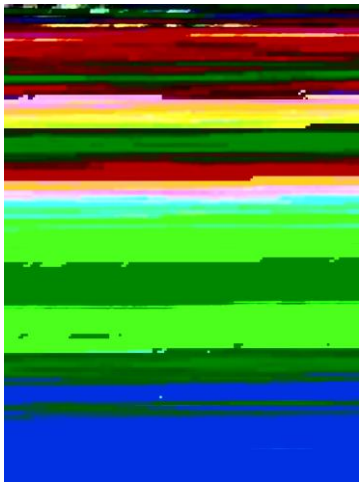

Figura 3 – Round 9

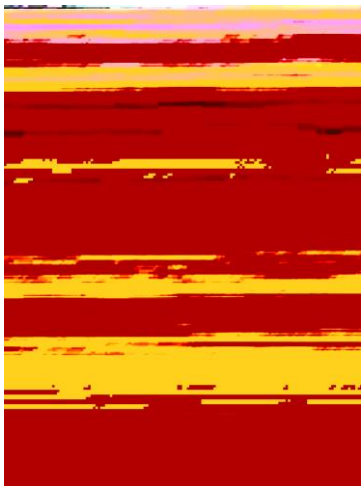

Figura 4 – Round 13

3. Conclusão

Embora a cifra de bloco AES no modo de operação CTR seja uma técnica de criptografia notoriamente robusta, ela também depende da escolha de parâmetros adequados, como a seleção de uma chave forte. A segurança do AES-CTR é garantida quando são seguidas práticas recomendadas, como o uso de chaves longas e

aleatórias, garantindo sua eficácia na proteção de informações sensíveis [Fonte de Segurança, 2023].

Conclui-se que, embora o AES-CTR seja um algoritmo moderno e altamente seguro, a segurança de qualquer sistema criptográfico depende da implementação sólida e da escolha de parâmetros adequados.

Ao longo deste projeto, ganhamos uma compreensão mais profunda da criptografia de cifras, especialmente no contexto do AES-CTR. Enfrentamos desafios significativos, como garantir a aleatoriedade das chaves e entender a importância das práticas seguras. Nossa jornada nos permitiu explorar e compreender melhor a eficácia da criptografia do AES-CTR, destacando a importância de abordagens seguras e a seleção criteriosa de parâmetros para proteger informações confidenciais.

Referências

1. "NIST FIPS PUB 197: Advanced Encryption Standard (AES)" - Esta é a publicação oficial do NIST que descreve o algoritmo AES. Pode ser encontrada no site do NIST (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf).
2. "The Design of Rijndael: AES - The Advanced Encryption Standard" - Livro escrito por Vincent Rijmen e Joan Daemen, os criadores do AES, que oferece insights detalhados sobre o desenvolvimento do algoritmo.
3. "Understanding AES Encryption" - Um recurso educativo do site Symantec que explica o funcionamento do AES, seus modos de operação e aplicações (https://www.broadcom.com/company/newsroom/press-releases).
4. "NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques" - Esta é uma publicação do NIST que aborda vários modos de operação, incluindo o modo CTR. Você pode encontrá-la no site do NIST (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38a.pdf).
5. "Counter (CTR) Mode of Operation" - Uma explicação detalhada do modo de operação CTR fornecida por Bruce Schneier em seu livro "Cryptography and Network Security" (https://www.schneier.com/academic/archives/2009/03/counter_mode.html).
6. "Understanding the Counter (CTR) Mode" - Um artigo informativo publicado pela IBM que descreve como o modo CTR funciona e suas aplicações (https://www.ibm.com/docs/en/zos/2.3.0?topic=algorithms-understanding-counter-mode).
7. Wikipédia: Modo de operação (criptografia)
8. https://pt.wikipedia.org/wiki/Modo_de_opera%C3%A7%C3%A3o_(criptografia)