**Relatório Lista de Exercícios 2**

Lucas Lício - 211043342

No decorrer desta atividade, foi implementada uma versão simplificada do algoritmo de criptografia Advanced Encryption Standard (AES) com o objetivo de consolidar os conceitos aprensetados em sala de aula. Para tanto, segue uma tabela que compara a versão simplificada implementada e a versão comercial:

|  |  |  |
| --- | --- | --- |
| Característica | S-AES | AES |
| Tamanho do Bloco | 16 bits (2 bytes) | 128 bits (16 bytes) |
| Tamanho da Chave | 16 bits | 128, 192 ou 256 bits |
| Número de Rodadas | 2 | 10 (AES-128), 12 (AES-192), 14 (AES-256) |
| S-Box | 4 bits (16 valores fixos) | 8 bits (256 valores, gerados via GF(2⁸)) |
| MixColumns | GF(2⁴) com matriz 2×2 | GF(2⁸) com matriz 4×4 |
| ShiftRows | Troca simples entre os dois nibbles da linha inferior | Rotação das linhas da matriz 4×4 |
| Key Expansion | Gera 3 subchaves de 16 bits | Gera 11, 13 ou 15 subchaves de 128 bits |
| Segurança | Vulnerável | Altamente seguro, aprovado pelo NIST |
| Desempenho | Rápido e de baixa complexidade | Mais complexo, mas otimizado em hardware |
| Aplicabilidade | Educação, simulações e testes didáticos | TLS, IPsec, VPNs, discos criptografados, Wi-Fi, etc. |
| Modo de Operação | Normalmente ECB (sem modos reais) | Suporta CBC, CTR, OFB, entre outros |

Na tentativa de incrementar ainda mais a versão simplificada do AES, foi implementado o modo de operação Electronic Codebook (ECB) para blocos múltiplos de 16 bits. Durante o desenvolvimento da primeira etapa, as funções já foram incluídas no loop principal para lidar com mensagens maiores que 16 bits, portanto a função encrypt\_saes\_ecb(texto, chave) foi implementada indiretamente.

De modo complementar, foi implementado uma versão simplificada para lidar com entradas não múltiplas de 16 bits. Como a entrada são apenas caracteres ASCII, a única situação adversa seria a entrada de um número ímpar de caracteres e, para contornar isso, é informado no terminal que foi incluído o valor 0 em ASCII ao final da mensagem para manter a simetria.

Evidenciando a principal vulnerabilidade do ECB, por trabalhar com cifra por bloco individual e propagar as mesmas chaves, vamos analisar a entrada ‘oioi’, com uma repetição evidente:

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Para compreender melhor o AES real, foram utilizadas bibliotecas de criptografia para visualizar alguns dos diferentes modos de operação do AES:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Modo | Segurança | Paralelismo | Aleatoriedade | Tempo de Execução | Observações |
| ECB | Fraca | Simples | Baixa | Rápido | Não protege padrões |
| CBC | Boa | Não | Alta | Mais lento | Depende de IV |
| CFB | Boa | Não | Alta | Intermediário | Sem padding |
| OFB | Boa | Sim | Alta | Intermediário | Sensível a IV |
| CTR | Forte | Total | Alta | Muito rápido | Requer nonce seguro |