Universidade de Brasília – UnB

Departamento de Ciência da Computação - CIC

Disciplina: Segurança Computacional – 2025/1

Professora: Lorena Borges

# Trabalho Prático 02

## Roteiro de Programação: S-AES e AES/Modos de Operação

### Parte 1 – Implementação do S-AES

O **S-AES (Simplified Advanced Encryption Standard)** é uma versão didática e altamente simplificada do algoritmo AES (Advanced Encryption Standard), criada especificamente para fins educacionais. Assim como o S-DES (Simplified DES) é uma versão simplificada do DES, o S-AES mantém a estrutura geral do AES, mas com parâmetros reduzidos para facilitar o aprendizado.

**Objetivo:**

Implementar o Simplified AES (S-AES) com blocos de 16 bits e 2 rodadas, seguindo os princípios básicos do AES original.

**Tarefas:**

1. Implementar as operações básicas do S-AES:
    - AddRoundKey
    - SubNibbles (com S-Box fixa)
    - ShiftRows
    - MixColumns (em $GF(2^4)$)
    - KeyExpansion
2. Representar blocos como matriz 2x2 de nibbles (4 bits).
3. Receber como entrada uma mensagem simples (ex: string curta), converter para binário e aplicar a cifra.
4. Exibir o texto cifrado em hexadecimal e em base64 (para visualização amigável).

**Entregas:**

- Código-fonte bem comentado do S-AES

- Entrada/saída no terminal
- Codificação base64
- Saídas intermediárias para cada função e saídas de cada rodada.
- Comparativo entre o S-AES e o AES oficial (NIST.FIPS.197)

**Parte 2 – Implementação do Modo de Operação ECB com o S-AES**

**Objetivo:**

Utilizar o código desenvolvido na Parte 1 para aplicar o modo de operação ECB (Electronic Codebook) sobre textos com múltiplos blocos de 16 bits.

**Entregas:**

- Função *encrypt_saes_ecb(texto, chave*) usando o S-AES
- Texto de saída visualizados em base64
- Mostrar como blocos idênticos geram cifras idênticas no modo ECB, destacando a fraqueza desse modo. (blocos iguais x saídas iguais)

**Parte 3 – Simulação com AES Real usando Bibliotecas Criptográficas**

**Objetivo:**

Usar uma biblioteca de criptografia para simular o AES real com vários modos de operação.

**Tarefas:**

1. Implementar a cifragem AES real nos modos:
    - ECB
    - CBC
    - CFB
    - OFB
    - CTR
2. Para cada modo:
    - Código-fonte bem comentado
    - Cifrar a mesma mensagem

- Usar chaves e vetores de inicialização (IV)
- Medir o tempo de execução para analisar a eficiência
- Apresentar a saída em base64
- Mostrar grau de aleatoriedade e segurança

**Entregas:**

- O trabalho poderá ser feito individual ou em dupla.
- Códigos executáveis e comentados.
- Relatório do trabalho organizado em tópicos: objetivo, introdução, desenvolvimento, análise e conclusão.
- Para parte III: incluir análises de desempenho entre os modos de operação, abordando vários aspectos de segurança, sendo necessariamente, segurança computacional, aleatoriedade, tempo de execução, eficiência e possíveis vulnerabilidades.