**FACULDADE VANGUARDA**

LUIZ GUSTAVO FRANCISCO DE SOUZA

**ATIVIDADES PRÁTICAS SUPERVISIONADAS - APR**

Desenvolvimento de aplicação utilizando técnicas criptográficas

CRIPTOGRAFIA SIMÉTRICA COM PERMUTAÇÃO DE BYTES INSPIRADO NO AES

São José dos Campos

2025

LUIZ GUSTAVO FRANCISCO DE SOUZA

**ATIVIDADES PRÁTICAS SUPERVISIONADAS - APR**

Desenvolvimento de aplicação utilizando técnicas criptográficas

CRIPTOGRAFIA SIMÉTRICA COM PERMUTAÇÃO DE BYTES INSPIRADO NO AES

Atividades Práticas Supervisionadas do curso de ENGENHARIA DA COMPUTAÇÃO da FACULDADE VANGUARDA, sob orientação de:

Profa. Dra. Ivana Yoshie Sumida – Prof. Responsável:

Prof. MSc. André Yoshimi Kusumoto – Coordenador:

São José dos Campos

2025

**SUMÁRIO**

Sumário automático gerado pelo Word após inserção dos títulos com estilo de cabeçalho.

# INTRODUÇÃO

A Atividade Prática Supervisionada (APS) tem como objetivo colocar em prática os conhecimentos adquiridos na disciplina de Algoritmos e Programação Estruturada, através do desenvolvimento de uma aplicação criptográfica utilizando a linguagem Python.

O trabalho busca proporcionar não apenas a aplicação dos conteúdos teóricos aprendidos em sala de aula, mas também o desenvolvimento de habilidades importantes para a formação em Engenharia da Computação.

A escolha do tema criptografia está relacionada à sua importância no contexto atual da tecnologia, onde a proteção de dados e a privacidade são cada vez mais necessárias. Assim, o desafio de implementar um algoritmo próprio de criptografia, sem utilizar bibliotecas prontas, permitiu aprofundar o entendimento sobre como funcionam técnicas como a permutação de bytes, a geração de chaves seguras e a utilização de elementos como o vetor de inicialização (IV).

Portanto, este relatório apresenta desde os fundamentos teóricos da criptografia até a descrição da técnica escolhida, finalizando com a solução desenvolvida em Python, demonstrando sua aplicação prática.

Particularmente, uma experiência pessoal que reforçou meu interesse pelo tema foi assistir ao filme O Jogo da Imitação (The Imitation Game, 2014), que retrata a quebra da Máquina Enigma durante a Segunda Guerra Mundial. A Enigma era uma avançada máquina de criptografia utilizada pelos alemães para proteger comunicações militares. O desafio de decifrar seus códigos exigiu um esforço significativo da inteligência britânica, liderada por Alan Turing, que desenvolveu uma máquina capaz de automatizar a criptoanálise. Esse episódio histórico não só mostra a importância da criptografia, mas também como sua aplicação pode ter impactos profundos na sociedade. Essa conexão histórica trouxe ainda mais motivação para me aprofundar no estudo e desenvolvimento de técnicas criptográficas.

EXPLIQUE QUAL É O OBJETIVO DA APS.

# FUNDAMENTOS DE CRIPTOGRAFIA

A criptografia é uma área da ciência da computação e da matemática aplicada que estuda técnicas para proteger a informação contra acessos não autorizados. Seu principal objetivo é garantir a **confidencialidade**, **integridade**, **autenticidade** e, em alguns casos, a **irrestrutibilidade** dos dados durante a comunicação ou armazenamento.

Existem dois principais tipos de criptografia: **simétrica** e **assimétrica**.

Na **criptografia simétrica**, o mesmo segredo (ou chave) é usado tanto para cifrar quanto para decifrar a informação. É um modelo eficiente em termos de desempenho, mas que exige um método seguro de compartilhamento da chave entre as partes. Algoritmos clássicos desse tipo incluem o AES (Advanced Encryption Standard) e o DES (Data Encryption Standard).

Já na **criptografia assimétrica**, são utilizadas duas chaves distintas: uma pública, que pode ser divulgada, e uma privada, que deve ser mantida em sigilo. O que é cifrado com uma chave só pode ser decifrado com a outra. Esse modelo é amplamente utilizado em sistemas de assinatura digital, autenticação e troca segura de chaves. Exemplos conhecidos incluem o RSA, o ECC (Criptografia de Curvas Elípticas) e o algoritmo ElGamal.

Além das técnicas de cifra, a criptografia moderna envolve outros conceitos essenciais, como a **função hash**, usada para garantir integridade dos dados, e os **vetores de inicialização (IVs)**, que garantem aleatoriedade mesmo quando a mesma chave é usada em múltiplas operações.

A segurança criptográfica não depende apenas do sigilo do algoritmo, mas da robustez matemática contra ataques, como força bruta, análise estatística ou ataques de criptoanálise. Por isso, é comum utilizar algoritmos públicos, amplamente testados pela comunidade científica, com segredos limitados apenas às chaves utilizadas.

EXPLIQUE OS CONCEITOS BÁSICOS, TIPOS, APLICAÇÕES, ETC SOBRE CRIPTOGRAFIA

# TÉCNICA CRIPTOGRÁFICA ESCOLHIDA

A técnica criptográfica escolhida para este trabalho é uma combinação de cifra por permutação baseada na operação lógica XOR e derivação segura de chave utilizando PBKDF2-HMAC com SHA-256. Essa técnica utiliza princípios fundamentais da criptografia para transformar dados legíveis em um formato cifrado de forma reversível.

O processo inicia com a entrada de uma frase em texto claro e uma senha fornecida pelo usuário. Para aumentar a segurança, é gerado um salt aleatório, que serve para tornar cada chave única mesmo quando a mesma senha é utilizada, dificultando ataques de dicionário e força bruta. A senha e o salt são usados na função de derivação de chave PBKDF2-HMAC, que realiza múltiplas iterações do algoritmo para criar uma chave criptográfica robusta de 256 bits.

Em seguida, a operação XOR é aplicada byte a byte entre os dados da frase e os bytes da chave gerada, promovendo a cifragem da mensagem. Esta operação é simples e reversível, ou seja, aplicando XOR novamente com a mesma chave, é possível recuperar o texto original. O resultado, junto com o salt e o vetor de inicialização (IV), que neste projeto é incluído para simular estruturas reais de criptografia, é codificado em Base64 para facilitar o armazenamento e transmissão.

Entre as vantagens desta técnica estão a simplicidade de implementação, a utilização apenas de bibliotecas padrão do Python, e a eficiência no processamento de textos de qualquer tamanho. No entanto, ela possui limitações, como a falta de resistência contra ataques mais avançados devido à simplicidade do XOR, a não utilização do vetor de inicialização para cifragem, e a ausência de mecanismos para garantir a integridade e autenticação dos dados.

Essa abordagem é especialmente útil para quem está começando a estudar criptografia, pois permite compreender os conceitos básicos de forma prática e acessível. Ela é indicada para projetos simples e protótipos onde a segurança máxima não é o foco principal, oferecendo uma base sólida para aprendizado.

DESCREVA QUAL A TÉCNICA CRIPTOGRÁFICA ESCOLHIDA. COMO É REALIZADO A CRIPTOGRAFIA E DESCRIPTOGRAFIA. VANTAGENS E DESVANTAGENS. APLICAÇÕES DE USO DA TÉCNICA. COMPLEXIDADE.

# SOLUÇÃO DESENVOLVIDA

DESCREVA COMO O ALUNO OU GRUPO DESENVOLVEU A APLICAÇÃO. QUAIS SÃO AS FUNCIONALIDADES. POSSUI INTERFACE GRÁFICA, BANCO DE DADOS, ETC. INSIRA IMAGENS DAS TELAS DA APLICAÇÃO.

# CÓDIGO-FONTE

# REFERÊNCIAS

Exemplo: SOBRENOME, Nome. Título do livro. Edição. Local: Editora, ano.