Requisitos do Trabalho: Curvas Elípticas e Criptografia

24 de junho de 2025

Requisitos do Trabalho

1. Introdução Teórica

- Explicação do conceito de **curvas elípticas** sobre corpos finitos $\mathbb{F}_p$
- Definição da **equação de Weierstrass** ($y^2 = x^3 + ax + b$) e condição de não-singularidade ($4a^3 + 27b^2 \neq 0$)
- Descrição do **grupo aditivo** dos pontos da curva (incluindo o ponto no infinito $\mathcal{O}$)

2. Fundamentos Matemáticos

- Explicação do **Problema do Logaritmo Discreto (ECDLP)** em curvas elípticas
- Comparação entre curvas sobre $\mathbb{R}$ e $\mathbb{F}_p$
- Menção às curvas sobre $\mathbb{F}_{2^n}$ (opcional)

3. Criptografia de Curva Elíptica (ECC)

- Descrição do protocolo **ECDH** (Elliptic Curve Diffie-Hellman)
- Explicação do esquema de assinatura **ECDSA**
- Comparação entre ECC e RSA (tamanhos de chave equivalentes)

4. Implementação em Python

- **Requisitos técnicos**:
  - Uso de bibliotecas como `sympy`, `ecdsa` ou implementação manual
- **Funcionalidades obrigatórias**:

1. Implementação da **adição de pontos** em $\mathbb{F}_p$
2. Implementação da **multiplicação escalar** (algoritmo *double-and-add*)
3. Simulação do protocolo **ECDH**
4. Implementação do **ECDSA** (opcional)

- **Entradas/Saídas**:
  - Parâmetros de entrada: (p, a, b), ponto base G, chave privada n
  - Saídas esperadas: pontos resultantes, chave compartilhada ou assinatura digital

5. Análise e Discussão

- Discussão sobre **complexidade computacional** das operações
- Análise de **vulnerabilidades** e ataques conhecidos
- Comparação entre diferentes curvas elípticas (e.g., NIST P-256 vs. Curve25519)

6. Conclusão e Reflexão

- Síntese dos desafios encontrados na implementação
- Reflexão sobre a importância das curvas elípticas na criptografia moderna

7. Apresentação e Formato

- **Relatório**:
  - Estrutura clara (introdução, desenvolvimento, resultados, conclusão)
  - Código bem documentado e explicado
- **Apresentação oral** (opcional):
  - Slides com pontos-chave
  - Demonstração prática