1 INTRODUÇÃO

As curvas elípticas, do seu primeiro uso em criptografia, no trabalho intitulado *Factoring integers with elliptic curves*, do matemático neerlandês Lenstra, H. W, e posterior formulação em corpos de Galois feita de maneira independente por Koblitz, N e Mille, V., até tempos atuais, mostraram-se uma alternativa segura e condizente com a crescente demanda por sintemas com alto grau de segurança. Uma de suas características é prover um elevado nível de criptografia através de chaves privadas relativamente pequenas, o que as tornam atrativas quando considera-se sua utilização em dispositivos embarcados.

Neste trabalho, estudaremos curvas elípticas definidas sobre um corpo finito $\mathbb{F}_p$, com $p > 3$ e primo, de equação $y^2 = x^3 + ax + b$ no qual $a, b \in \mathbb{F}_p$ e $4a^3 + 27b^2 \neq 0$. Curvas que atendem a estas características mostram-se viáveis para uso em criptosistemas por proporcionarem criptografia assimétrica cuja segurança é garantida pelo Problema de Logaritmo Discreto. Investigaremos aqui algumas propriedades destas curvas e aprenderemos as utiliza-las na criptografia e troca de mensagens entre duas pessoas, modelando esta interface de comunicação com a linguagem de programação $Python$.

2 REVISÃO DA LITERATURA

3 METODOLOGIA

Este estudo é de natureza exploratória, busca-se por meio dele, uma maior familiaridade com o objeto de estudo; para sua realização, inicialmente, realizou-se um levantamento bibliográfico de livros e periódicos que abordavam total ou parcialmente o tema; em seguida, realizou-se uma discussão teórica acerca dos resultados encontrados que, de maneira sequencial, corroboram com o entendimento das curvas elípticas; por fim, utilizou-se a linguagem de programação $Python$ para criar um aplicativo para envio e recebimento de mensagens, no qual as mensagens são criptografadas na curva elíptica secp256k1.