Abertura

Bom [dia/tarde/noite] a todos, obrigado pela presença.

Meu nome é Isak Paulo de Andrade Ruas, e hoje vou compartilhar com vocês o trabalho que desenvolvi sobre a "Criptografia de Curvas Elípticas: Propriedades, Métodos e Implementação".

Este trabalho marca um ponto importante na minha formação em Matemática no Instituto Federal do Norte de Minas Gerais, campus Januária; foi desenvolvido sob a orientação da Profa. Me. Celimar Reijane Alves Damasceno Paiva e a coorientação do Prof. Me. Fernando Marcos Souza Silva.

Introdução: Motivação, Metodologia e Objetivos

Vivemos em uma era digital, um período histórico caracterizado pela velocidade e pelo volume com que as informações são compartilhadas online.

Nestes tempos modernos, dados pessoais, comunicações privadas e informações confidenciais de negócios fluem continuamente através de redes globais.

Essa constante troca de dados levanta uma questão crucial: Como garantimos a segurança dessa informação durante a sua transmissão? Como podemos ter certeza de que nossos dados estão protegidos?

Foi essa curiosidade que serviu como catalisador para o desenvolvimento deste estudo.

A solução para esta problemática encontra-se em um método sofisticado conhecido como criptografia de ponta a ponta, com um destaque especial para uma técnica especificamente engenhosa – a criptografia de curvas elípticas.

Para embasar teoricamente nossa pesquisa, mergulhamos em uma vasta revisão bibliográfica, culminando na análise aprofundada dos algoritmos de criptografia ponta a ponta, com um foco particular nas curvas elípticas.

O projeto prático desta investigação veio na forma de desenvolver uma biblioteca na linguagem de programação Python, escolhida por sua versatilidade, eficiência e facilidade de implementação.

Esta biblioteca não apenas reforçou nossa compreensão teórica, mas também viabilizou a execução prática e a validação dos conceitos estudados;

Deste o seu lançamento publicamente no PyPI em 17 de abril de 2022, já soma mais de 5 mil downloads.

- PyPI - The Python Package Index

Panorama Histórico da Criptografia

A criptografia tem raízes profundas na antiguidade remota, usada nas mais variadas civilizações para a proteção de suas informações.

Conforme relatos de Heródoto (484-425 a.C.), ela foi empregada principalmente em situações complexas envolvendo guerras e diplomacia, fundamentais para o sucesso militar e para salvaguardar privacidade das comunicações (Pabón Cadavid, 2010, p. 59).

- Heródoto (484-425 a.C.) importante historiador grego da antiguidade

Através de figuras históricas como Júlio César (100-44 a.C.) que ela realmente ganhou destaque.

- Júlio César (100-44 a.C.) - importante militar, político e estadista romano que desempenhou um papel crucial na transformação da República Romana em um Império Romano

César, ao usar técnicas esteganográficas e criptográficas, garantiu uma comunicação segura entre ele e seus generais, passando mensagens que eram praticamente indecifráveis para quem não estava familiarizado com o método. (Pabón Cadavid, 2010, p. 61).

- Esteganografia é uma técnica que consiste em ocultar informações dentro de outra mensagem ou objeto físico para evitar a detecção

Foi um enorme passo de avanço na utilização da criptografia como um instrumento de segurança para a transmissão de informações.

No século XVIII começaram a surgir ideias para aproveitar os sistemas elétricos na transmissão de mensagens, foi somente em 1839, com o sistema Wheatstone-Cooke, que o telégrafo foi desenvolvido, e este feito foi realizado (Pabón Cadavid, 2010, p. 63).

- Permitindo a comunicação entre duas estações de trem localizadas a 29 km de distância

Com o advento dos sistemas elétricos de transmissão de informações, a criptografia tomou um novo rumo e se tornou precursora do que encontramos hoje em dia (Pabón Cadavid, 2010, p. 63).

A era moderna, especialmente após a Segunda Guerra Mundial, trouxe avanços tecnológicos notáveis na criptografia.

Durante esse período, houve uma expansão significativa na pesquisa e desenvolvimento em criptografia, o que despertou não apenas o interesse das forças armadas e dos governos, mas também do público em geral

A criptografia moderna, embora mantenha a essência de sua prática histórica, se tornou amplamente complexa devido ao avanço tecnológico.

Sua execução não se limita mais à simples reorganização do alfabeto, mas incorpora algoritmos matemáticos complicados para cifrar mensagens.

A demanda por sistemas seguros e confiáveis está em progressivo crescimento. Ao atender essas demandas, a criptografia emerge como uma protagonista estratégica. Ela atua como uma poderosa ferramenta na salvaguarda de dados, assegurando que as informações transmitidas permaneçam inacessíveis a olhares indesejados (Viana et al, 2022, p. 231-232).

Fundamentos e Características da Criptografia

A essência primordial da criptografia reside na asseguração de que uma mensagem, originada por um remetente, seja decifrável apenas pelo destinatário desejado, bloqueando assim qualquer tentativa de acesso não autorizado ao conteúdo da transmissão.

Neste cenário, destacam-se duas abordagens de amplo uso: a criptografia simétrica e a criptografia assimétrica.

Vamos analisar características de cada uma dessas estratégias, para compreender seu funcionamento e aplicabilidade em diferentes contextos.

A Criptografia Simétrica é um método de codificação de dados em que uma única chave é utilizada para criptografar e descriptografar as informações.

Este modelo permite a transformação eficiente e rápida da mensagem original em um formato não legível, garantindo assim a proteção dos dados durante o processo de transmissão. (Viana et al, 2022, p. 226)

- Imagem

No entanto, a criptografia simétrica acarreta um desafio crítico: o compartilhamento seguro da chave entre o remetente e o destinatário (Viana et al, 2022, p. 236).

Este procedimento de compartilhamento da chave precisa ser seguro para evitar que terceiros mal-intencionados interceptem a chave e, consequentemente, tenham acesso aos dados transmitidos.

Já a criptografia assimétrica opera de forma diferentemente (Viana et al, 2022, p. 238).

Em vez de uma única chave, este sistema usa um par de chaves: uma pública, a qual pode ser abertamente compartilhada, e uma privada, que deve ser mantida em sigilo exclusivo pelo receptor da mensagem.

- Imagem

Vale ressaltar que, na criptografia assimétrica, a mensagem criptografada só pode ser decodificada pelo destinatário que possui a chave privada correspondente, aumentando assim a segurança do processo de transmissão da informação (Viana et al, 2022, p. 240).

Apesar de ambos os sistemas de criptografia terem suas vantagens e desvantagens, suas diferenças essenciais orientam suas aplicações ideais.

A criptografia simétrica, sendo eficiente e rápida, é ideal para a codificação de conteúdos de mensagens. Entretanto, o gerenciamento e a distribuição segura das chaves usadas para criptografia é um desafio (Oliveira, 2012, p. 8).

Por outro lado, a criptografia assimétrica supera os problemas de gerenciamento das chaves que são inerentes à criptografia simétrica.

Embora seja um pouco mais lenta devido à sua complexidade, fornece maior segurança ao dividir as chaves em públicas e privadas (Oliveira, 2012, p. 8).

Este tipo de criptografia é ideal para a distribuição de chaves e assinatura digital, assegurando não só a confidencialidade, mas também a autenticidade das mensagens.

A decisão entre usar criptografia simétrica ou assimétrica deverá levar em consideração as necessidades específicas de cada situação. Não existe uma receita de bolo, vai depender do tipo de aplicação a ser desenvolvido.

Criptografia com Curvas Elípticas: Conceitos preliminares

___Definição de Curvas Elípticas___

Vamos iniciar nossa jornada nos fundamentos das curvas elípticas explorando a equação de Weierstrass simplificada.

Uma curva elíptica E sobre um corpo $\K$ é o conjunto de pontos que satisfazem a relação $y^2 = x^3 + Ax + B$.

- Imagem

É essencial que $4A^3 +27B^2 \neq 0$ e $\K$ não sejam 2 ou 3 para garantir a diferenciabilidade de cada ponto, o que simplifica as operações matemáticas.

Na aplicação prática de criptografia, é recomendado, trabalhar com a estrutura de um corpo de inteiros módulo p, assim nossa curva se redefine como $E(\Z_p)$ (Gonzaga e Pesco, 2021, p. 43).

- Imagem

Desta forma, E formará um grupo abeliano finito (Brady; Davis; Tracy, 2010, p. 6-7), o que é crucial para as operações na criptografia.

__Catálogo de curvas elípticas__

__Protocolo Diffie-Hellman__

Para assegurar que dois usuários, como Alice e Bob, possam estabelecer uma comunicação segura em uma rede insegura, sem a necessidade de um intercâmbio prévio de chaves secretas, faz-se uso do protocolo de Diffie-Hellman.

- Imagem

Este protocolo aproveita a dificuldade inerente à resolução do problema do logaritmo discreto em curvas elípticas.

Através da geração e compartilhamento de chaves públicas derivadas de seus segredos privados, Alice e Bob conseguem calcular um segredo compartilhado que será usado para cifrar e decifrar mensagens.

Este segredo compartilhado nunca é transmitido através da rede, e, portanto, mesmo que um adversário observe a comunicação, ele não poderá determinar o segredo.

__Protocolo Massey-Omura__

Outro protocolo existente para realização do compartilhamento de chaves e comunicação é o Massey-Omura, ele funciona de forma semelhante ao Diffie-Hellman, porém o seu

funcionamento é mais direcionado a troca de informações em um canal inseguro, e requer mais etapas para efetivação do seu funcionameto.

- Imagem

__Algoritmo de Koblitz__

Para transformar uma mensagem como sendo um ponto de uma curva elíptica, utilizamos o algoritmo de Koblitz, ele possibilita transformar uma sequência de caracteres, seja Unicode ou ASCII em um ponto da curva elíptica utilizada.

- Imagem

__Algoritmo de Assinatura Digital de Curva Elíptica__

A integridade e autenticação da mensagem são garantidas por meio do Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA, sigla em inglês).

- Imagem

O ECDSA utiliza um conjunto de operações matemáticas para gerar uma assinatura digital única. Esta assinatura, atrelada à mensagem original, permite confirmar não apenas que a mensagem não foi alterada durante a transmissão, mas também a identidade da pessoa que a assinou.

A verificação da assinatura é feita utilizando a chave pública do remetente, garantindo a qualquer receptor a legitimidade da mensagem.

Implementação Prática

Nos cenários simulados a seguir, iremos detalhar passo a passo a aplicação desses conceitos. Abordaremos a geração de chaves, a segura troca de chaves via protocolos como Diffie-Hellman e Massey-Omura, e o intricado processo de assinatura digital e verificação de mensagens utilizando o ECDSA.

Cada exemplo se propõe a ser uma representação prática, destilando mesmo os conceitos mais abstratos em procedimentos concretos. Revelaremos como mensagens podem ser codificadas, transmitidas e a integridade verificada, proporcionando uma compreensão mais tangível dessas práticas criptográficas.

- Exemplo com ECDSA, Diffie-Hellman e Koblitz
- Exemplo com ECDSA, Massey-Omura e Koblitz

Considerações Finais

À medida que exploramos a intrincada complexidade da criptografia de curvas elípticas, um ponto se destaca nitidamente: apesar de sua presença difundida em nossas interações digitais, a criptografia permanece uma arte distante e enigmática para muitos.

Este trabalho se propôs a revelar seus contornos, ilustrando não apenas seus fundamentos teóricos, mas também como ela se manifesta na prática, tornando-se uma ferramenta integral na construção do tecido da segurança digital.

Apesar de sua abrangência, este estudo não pretende ser uma exposição exaustiva da criptografia de ponta a ponta. Em vez disso, oferece um panorama que pinta com tons gerais a paisagem dessa disciplina complexa e profunda.

Esperando fornecer uma base sólida que não apenas auxilie no entendimento, mas também inspire futuras investigações sobre o tema.

Ao olharmos para frente, fica evidente que a criptografia continuará sendo um componente vital de nossa infraestrutura digital. Com o avanço das tecnologias da informação, novas necessidades de segurança e privacidade emergem, e a criptografia está na vanguarda desses desafios, pronta para evoluir e inovar.

Neste contexto, a criptografia de curvas elípticas vislumbra um terreno fértil para crescimento e refinamento, permanecendo firmemente entrelaçada ao nosso mundo conectado.