Desvendando a Criptografia de Curvas Elípticas

Propriedades, Métodos e Implementação

Isak Paulo de Andrade Ruas

Sob orientação

Me. Celimar Reijane Alves Damasceno Paiva

Me. Fernando Marcos Souza Silva

Instituto Federal do Norte de Minas Gerais
Campus Januária
Curso de Licenciatura em Matemática

8 de Março de 2024

Agenda

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Introdução: Motivação, Metodologia e Objetivos

- Motivação para estudar a criptografia e sua importância na era digital.
- Metodologia adotada: revisão bibliográfica e criação de uma biblioteca Python.
- Objetivos do estudo: compreender e aplicar criptografia de curvas elípticas.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Panorama Histórico da Criptografia

- O uso da criptografia desde Júlio César até os tempos modernos.
- A evolução da criptografia com novas tecnologias e o surgimento do telégrafo.
- Papel atual da criptografia na segurança de dados em um contexto digital crescente.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Fundamentos e Características da Criptografia

- Conceitos de criptografia simétrica e assimétrica.
- Importância de chaves seguras e a diferença entre chave pública e privada.
- Escolha entre criptografia simétrica e assimétrica com base em necessidades específicas.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Entendendo a criptografia simétrica

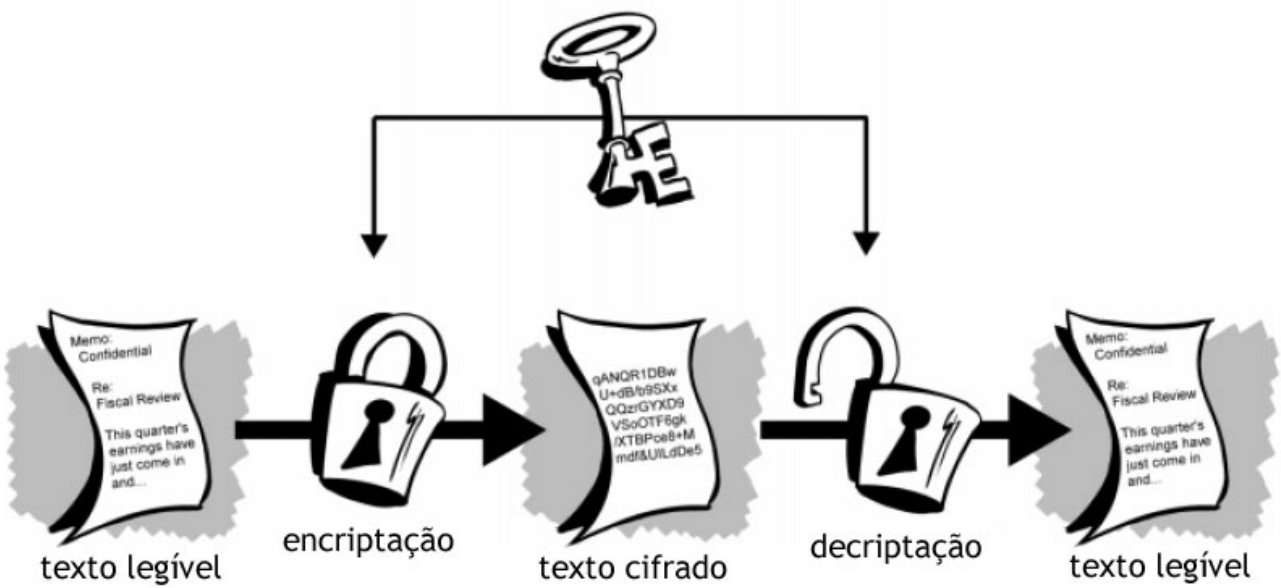

Figura: Ilustração do processo de criptografia Simétrico

Fonte: Seragiotto, 2023, p. ?

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Entendendo a criptografia assimétrica

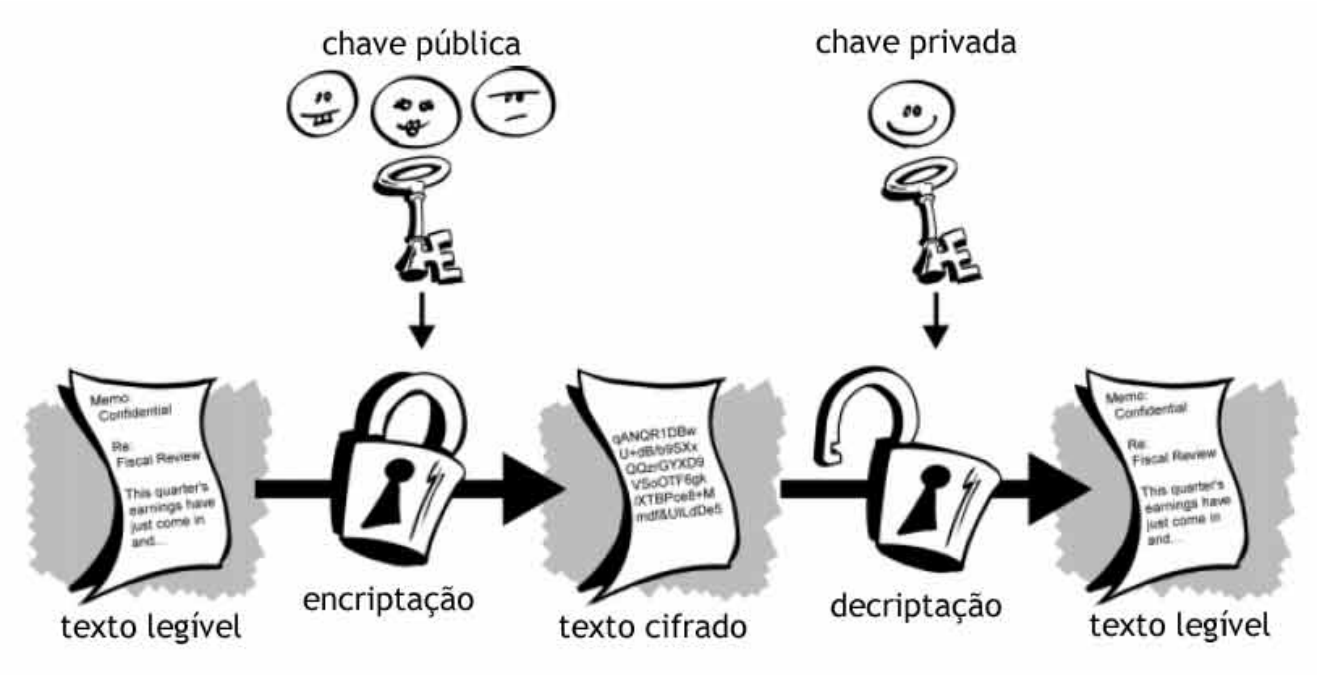

Figura: Ilustração do processo de criptografia Assimétrico

Fonte: Seragiotto, 2023, p. ?

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Criptografia com Curvas Elípticas

- Definição e propriedades das curvas elípticas em criptografia.
- Protocolos de Diffie-Hellman e Massey-Omura para troca de chaves.
- Uso do algoritmo de Koblitz para codificar mensagens em curvas elípticas.
- Implementação do ECDSA para assinatura digital de mensagens.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Definição de Curvas Elípticas

Definição

Uma curva elíptica $E = \{(x, y) \in \mathbb{K} | (y^2 = x^3 + Ax + B)\}$ no qual $(car(\mathbb{K}) \notin \{2, 3\})$ e $(4A^3 + 27B^2 \neq 0)$.

Definição

$E(\mathbb{Z}_p) : y^2 \equiv x^3 + Ax + B \pmod{p}$, donde $4A^3 + 27B^2 \neq 0 \pmod{p}$

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Catálogo de curvas elípticas

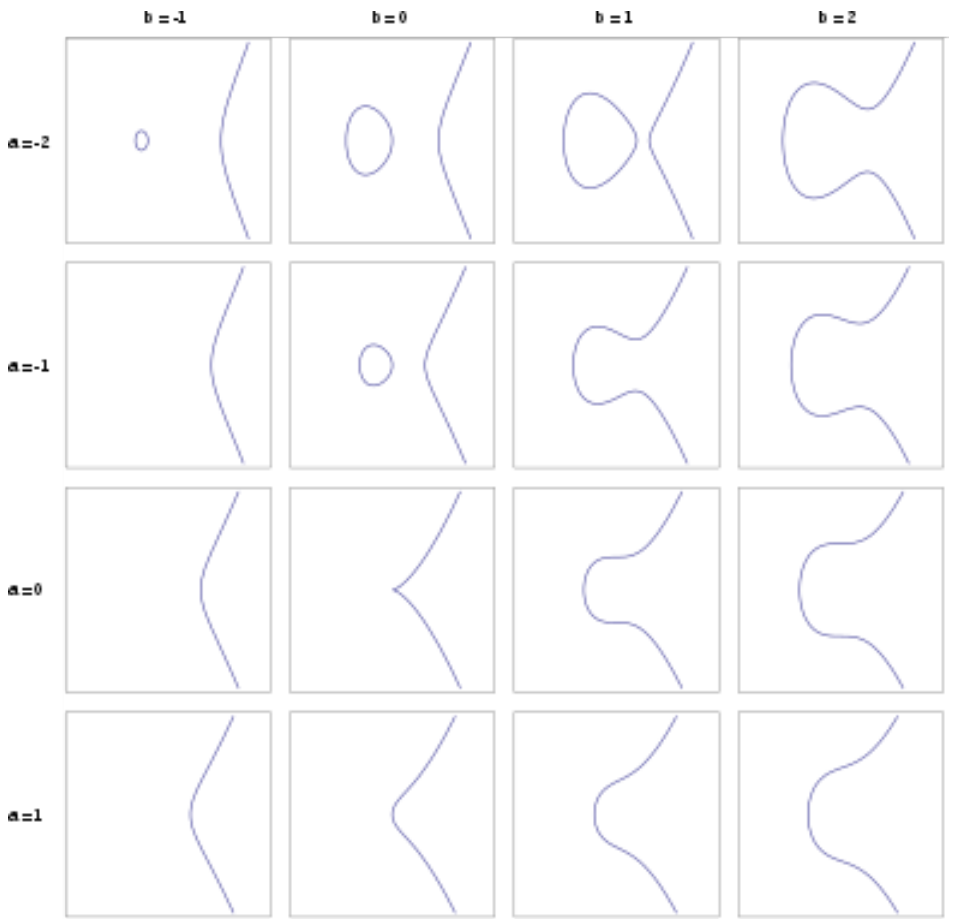

Figura: Catálogo de curvas elípticas

Fonte: Domínio Público

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Protocolo Diffie-Hellman

Tabela: Fluxo de passos do protocolo Diffie-Hellman

Alice	**Canal Público**	**Bob**
Gera aleatoriamente $d_A \in \{1, \ldots, n\}$		Gera aleatoriamente $d_B \in \{1, \ldots, n\}$
Define $H_A = d_A \cdot G$	$H_A \Rightarrow$	Define $H_B = d_B \cdot G$
Calcula $S = d_A \cdot H_B$	$\Leftarrow H_B$	
		Calcula $S = d_B \cdot H_A$

Fonte: Maimon, 2018, p. 5

Em que n é a ordem do gerador da curva $i.e\ \forall P \in E : n \cdot P = \mathcal{O}$.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Protocolo Massey-Omura

Tabela: Fluxo de passos do protocolo Massey-Omura

Alice	**Canal Público**	**Bob**
Representa m como um ponto $M_A \in E$		
Gera aleatoriamente $d_A \in \{1, \ldots, n\}$, $mdc(d_A, n) = 1$		Gera aleatoriamente $d_B \in \{1, \ldots, n\}$, $mdc(d_B, n) = 1$
Define $H_A = d_A \cdot M_A$	$H_A \Rightarrow$	Define $H_B = d_B \cdot H_A$
$S_A = (d_A^{-1} \pmod n) \cdot H_B$	$\Leftarrow H_B$	
	$S_A \Rightarrow$	$M_A = (d_B^{-1} \pmod n) \cdot S_A$

Fonte: Autoria própria.

Em que n é a ordem do gerador da curva $i.e\ \forall P \in E : n \cdot P = \mathcal{O}$.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Algoritmo de Koblitz

Definição

$\mathcal{M}$ é a representação de uma mensagem na forma de uma sequência de caracteres, denotada como $\{m_1, m_2, \ldots, m_n\}$, onde n é o tamanho da mensagem. $\mathcal{A}$ é uma sequência numérica, representada como $\{a_1, a_2, \ldots, a_n\}$, que corresponde ao decimal de cada caractere de $\mathcal{M}$ obtido nas tabelas Unicode ou ASCII. Considerando $b = 2^{16}$ para Unicode e $b = 2^8$ para ASCII, a mensagem cifrada m será obtida por: $m = \sum_{k=1}^{n} a_k \cdot b^{k-1}$ e cada elemento $\{a_1, a_2, \ldots, a_n\}$ poderá ser obtido novamente pela relação a seguir: $a_n = m \div b^{n-1} \pmod{b}$

Nota: $\div$ neste contexto representa divisão na qual o resultado é o quociente inteiro, sem considerar a parte fracionária.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Algoritmo de Assinatura Digital de Curva Elíptica

Definição

Seja $E(\mathbb{Z}_p) : y^2 \equiv x^3 + Ax + B \pmod{p}$ curva elíptica, um ponto base G, um natural n, primo, tal que $\forall P \in E : n \cdot P = \mathcal{O}$, onde $\mathcal{O}$ é o ponto no infinito, m um numero natural representando uma mensagem e $d \in \{1, \ldots, n-1\}$ representando uma chave privada e $Q = d \cdot G$ representando uma chave publica.

Para Q assinar a mensagem m em E, siga os seguintes passos:

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Algoritmo de Assinatura Digital de Curva Elíptica

Para Q assinar a mensagem m em E, siga os seguintes passos:

1. Escolha um $k \in \mathbb{N} \mid 1 \leq k \leq n-1$ e $mdc(k, n) = 1$.
2. Calcule $P = k \cdot G$.
3. Calcule $r = P_x \pmod{n}$. Se $r = 0$ volte ao passo 1.
4. Calcule $s = (m + r \cdot d) \cdot (k^{-1} \pmod{n}) \pmod{n}$. Se $s = 0$ volte ao passo 1.
5. A assinatura da mensagem m, por Q é o par r e s.

Para verificação da assinatura de m em E, dados r e s, siga os seguintes passos:

1. Verifique se r e s estão no intervalo $\{1, \ldots, n-1\}$
2. Calcule $w = s^{-1} \pmod{n}$
3. Calcule $u_1 = m \cdot w \pmod{n}$ e $u_2 = r \cdot w \pmod{n}$
4. Calcule $P = u_1 \cdot G \oplus u_2 \cdot Q$. Se $P = \mathcal{O}$ a assinatura é invalida.
5. Calcule $v = P_x \pmod{n}$. Se $v = r$ a assinatura é valida.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Implementação Prática

- Demonstração da implementação dos conceitos com a linguagem Python.
- Exemplo de geração e troca de chaves usando Diffie-Hellman e Massey-Omura.
- Exemplo de assinatura digital e verificação com o ECDSA.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Considerações Finais

- Resumo da contribuição do trabalho para o entendimento da criptografia de curvas elípticas.
- Importância da criptografia para a segurança de informações na era digital.
- Perspectivas futuras para criptografia em resposta a novos desafios de segurança.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Perguntas?

Obrigado pela atenção!
Perguntas?

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária