Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 5** 1 (2021): 35–48. ©JEEPEMA–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Exemplo de cálculo com chaves criptografadas com curvas elípticas

Ana Carolina Sakurai Ferreira – Email: carolynasf@msn.com

Resumo: Este artigo é um fragmento da dissertação de mestrado apresentado no Programa de Mestrado Profissional em Rede Nacional - Profmat e nele mostramos as curvas elípticas a partir de uma adaptação do Problema do Logaritmo Discreto. São apresentados alguns embasamentos teóricos de aritmética e apresentamos um exemplo de uma mensagem/palavra criptografada utilizando o método estudado.
Palavras-chave: Criptografia, Curvas Elípticas, ElGamal.

1. Introdução

Falaremos sobre a criptografia com uso de curvas elípticas. Essa técnica foi, inicialmente, introduzida em 1985 por Victor Miller e Neal Koblitz e foi abordada no uso de curvas elípticas como uma nova forma de implementação a um sistema de chave pública em algumas das aplicações já existentes.

Esse método criptográfico tem tido uma relevância nas últimas décadas pois está associado a crescente necessidade de segurança nos modernos meios de comunicação, fundamentado em computadores onde a eficiência de processamento tem evoluído a cada instante.

Apresentamos os conceitos matemáticos usados no sistema de criptografia desenvolvido a partir das curvas elípticas definidas sobre corpos finitos. Para tal, assumiremos que o leitor tenha conhecimento de alguns conceitos apresentados em disciplinas do curso de graduação em matemática tais como grupos, anéis, corpos, etc. O referencial teórico empregado neste texto pode ser averiguado nas obras de (OLIVEIRA, 2009), (ANDRADE, 2016), (CORREIA, 2013) e (F. B. LARA, 2010).

2. Curvas Elípticas

Curvas elípticas são definidas a partir da Equação de Weierstrass sobre um corpo $\mathbf{K}$:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

com $a, b, c, d, e \in \mathbf{K}$ mais, um ponto chamado de ponto no infinito (representaremos esse ponto por ∞). Neste trabalho, trabalharemos com curvas elípticas simétricas em relação ao

eixo das abcissas e sem singularidades. Assim, trabalharemos com uma versão simplificada da Equação de Weierstrass.

Definição 2.1 *Seja* $\mathbf{K}$ *um corpo. Uma curva elíptica* E *sobre* $\mathbf{K}$*, denotada por* $E(\mathbf{K})$*, é o lugar geométrico dos pontos* $(x, y) \in \mathbf{K} \times \mathbf{K}$ *tais que* x *e* y *são soluções da equação*

$$y^2 = x^3 + Ax + B$$

com $A, B \in \mathbf{K}$ *e* $4A^3 + 27B^2 \neq 0$.

Esta curva não possui raízes múltiplas, ou seja, deve ser uma curva não-singular, por isso devemos ter $\Delta = 4A^3 + 27B^2 \neq 0$.

Abaixo estão alguns gráficos de curvas elípticas.

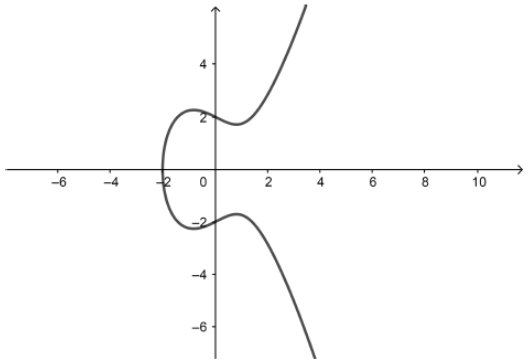

Figura 1: Gráfico da curva $y^2 = x^3 - 2x + 4$

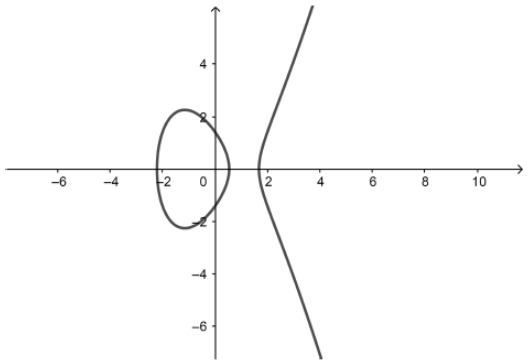

Figura 2: Gráfico da curva $y^2 = x^3 - 4x + 2$

Esses gráficos são de curvas definidas para os reais, ou seja, os valores das variáveis x e y na equação são reais e os valores dos parâmetros A e B são números reais. Porém uma curva

elíptica pode ser definida em qualquer corpo. Aqui, estamos interessados no caso onde elas estão definidas sobre corpos finitos.

Queremos definir uma estrutura de grupo no conjunto das curvas elípticas, para isso vamos definir a "soma"entre dois pontos. Essa soma pode ser tratada tanto de forma geométrica ou algébrica, iremos, inicialmente, analisar a forma geométrica.

O ponto infinito ∞ será o nosso elemento neutro da operação. Assim, se Ω é uma curva elíptica sobre um corpo K, e temos $P \in \Omega$, então:

$$P + \infty = P = \infty + P.$$

Consideremos o simétrico de um ponto $P = (x, y)$ sendo o ponto $-P = (x, -y)$, se somarmos um ponto $P \in \Omega$ com o ponto simétrico $-P$, obtemos o ponto infinito, logo:

$$P + (-P) = \infty = (-P) + P.$$

Tome dois pontos P e Q distintos de uma curva elíptica sobre o corpo $\mathbb{R}$ dos números reais, seja PQ o segmento de reta que interceptará a curva em um terceiro ponto que chamaremos de R' (estamos considerando o caso em que a reta não seja vertical). Assim, o reflexo do ponto R' em relação ao eixo horizontal, que é dado por R, será a soma de P e Q. Logo:

$$R = P + Q.$$

O gráfico abaixo, representa graficamente a soma entre dois pontos distintos $P, Q \in \Omega$ em uma curva elíptica sobre o corpo $\mathbb{R}$.

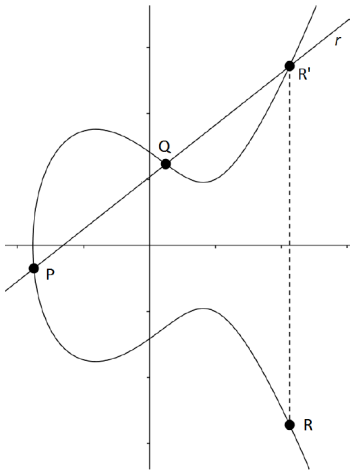

Figura 3: Soma de dois pontos em uma curva $E(\mathbb{R}) : R = P + Q$.

Agora vamos definir a soma $P + P$, para isso trassemos a reta tangente ao ponto P, de tal modo que a reta tangente em P intersecta a curva em um segundo ponto R' e tomamos

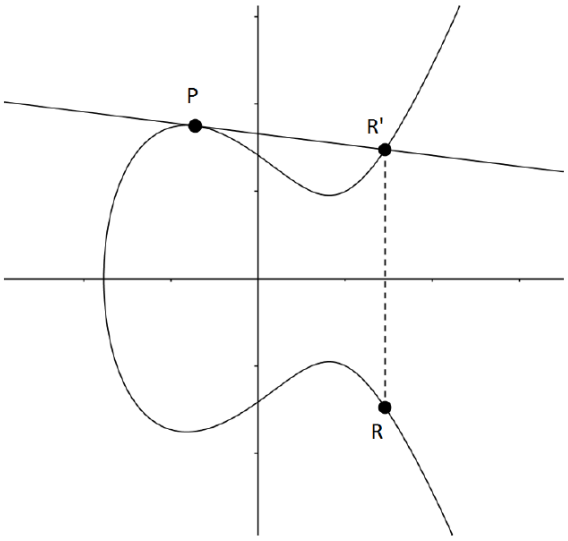

Figura 4: $R = P + P$ ou $R = 2P$.

a reflexão R em relação ao eixo horizontal, ou seja $P + P = R$. Podemos representar a soma de $P + P$ por $2P$.

Um caso particular é disposto se tivermos $P = (x, 0)$, pois, neste caso, a reta tangente à curva no ponto P será vertical e não interceptará a curva em um outro ponto. Neste caso teremos:

$$P + P = 2P = \infty.$$

Veremos agora a soma de dois pontos utilizando a soma algébrica. Para tal iremos trabalhar com as coordenadas dos pontos em uma curva elíptica.

Sejam $P = (x_p, y_p)$ e $Q = (x_q, y_q)$ dois pontos em uma curva elíptica Ω de equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$ e $P \neq \infty$ e $Q \neq \infty$, vamos analisar o caso $P \neq Q$. Seja r a reta que passa pelos pontos P e Q, que intersecta a curva Ω em um terceiro ponto que chamaremos de $R' = (x'_r, y'_r)$ e agora chamaremos de R a reflexão de R'. Assim, pela fórmula da inclinação da reta, conclui-se que a inclinação da reta r é:

$$m = \frac{y_q - y_p}{x_q - x_p},$$

com $x_p \neq x_q$.

Logo a equação da reta r é:

$$y = m(x - x_p) + y_p$$

pois r passa pelo ponto P. Para obter as intersecções entre a reta r e a curva Ω iremos substituir a equação da reta na equação da curva, ou seja,

$$(m(x - x_p) + y_p)^2 = x^3 + ax + b$$

o que nos dá,

$$x^3 + ax + b = m^2x^2 - 2m^2x_px + m^2x_p^2 + 2my_px - 2mx_py_p + y_p^2.$$

Portanto,

$$x^3 - m^2x^2 + (a + 2m^2x_p - 2my_p)x + (b - m^2x_p^2 + 2mx_py_p - y_p^2) = 0.$$

$$\text{Tomando } a' = -m^2, b' = a + 2m^2x_p - 2my_p \text{ e } c' = -m^2x_p^2 + 2mx_py_p - y_p^2$$

teremos:

$$x^3 + a'x^2 + b'x + c' = 0.$$

Sabemos que P, Q e $R^{'}$ são as intersecções da reta r com a curva Ω, então x_p, x_q e $x_r^{'}$ são as raízes da equação. Aplicando as Relações de Girard, temos que a soma das raízes é:

$$-a' = x_p + x_q + x_r^{'}.$$

Como $a = -m^2$ temos que :

$$m^2 = x_p + x_q + x_r^{'};$$

$$x_r^{'} = m^2 - x_p - x_q. \tag{1}$$

Como $R^{'} \in r$, podemos substituir suas coordenadas na equação da reta r, assim:

$$y_r^{'} = m(x_r^{'} - x_p) + y_p. \tag{2}$$

Como $R = P+Q$, $R = (x_r, y_r)$ é a reflexão de $R^{'}$ em relação ao eixo horizontal, assim $x_r = x_r^{'}$ e $y_r = -y_r^{'}$. Substituindo nas equações (1) e (2) temos :

$$x_r = m^2 - x_p - x_q$$

e

$$y_r = m(x_p - x_r) - y_p.$$

Vamos analisar o caso que em $P = Q$, nesse caso temos que a reta r é tangente à curva no ponto P. Assim, a inclinação da reta será a derivada no ponto P em relação a x. Logo,

podemos concluir que:

$$m = \frac{3x_p^2 + a}{2y_p},$$

com $y_p \neq 0$, pois caso contrario a reta seria vertical e teríamos $P + P = \infty$. Logo, a reta r que passa por P com inclinação m tem a mesma forma da equação $y = m(x - x_p) + y_p$. Observe que se realizarmos a interseção desta reta com a curva Ω, obteremos a equação $x^3 + ax^2 + bx + c = 0$, porem agora as raízes não são todas distintas, pois x_p é uma raiz dupla. Assim, aplicando as Relações de Girard, temos que:

$$m^2 = x_p + x_p + x_r^{'};$$

$$x_r = x_r^{'} = m^2 - 2x_p.$$

Agora, para determinar y_r seguimos o mesmo procedimento para o caso $P \neq Q$ e temos

$$y_r = m(x_p - x_r) - y_p.$$

O caso em que $P = \infty$, teremos $x_r = x_p$ e $y_r = y_p$ e no caso $Q = \infty$, teremos $x_r x_q$ e $y_r = y_q$, pois ∞ é o elemento neutro da operação.

Podemos, agora, padronizar a definição de soma entre dois pontos de uma curva elíptica em termos algébricos.

Definição 2.2 *(Soma de dois pontos de uma curva elíptica em termos algébricos) Seja Ω uma curva elíptica de equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$ e sejam $P = (x_p, y_p), Q = (x_q, y_q)$ e $R = (x_r, y_r)$ pontos da curva Ω tais que $R = P + Q$.*

- *Se $P = \infty$, então $R = Q$;*
- *Se $Q = \infty$, então $R = P$;*
- *Se $P = -Q$ então $R = \infty$;*

Nos demais casos, defina

$$m = \begin{cases} \dfrac{y_q - y_p}{x_q - x_p}, & \text{se } P \neq Q; \\ \\ \dfrac{3x_p^2 + a}{2y_p}, & \text{se } P = Q. \end{cases}$$

Em termos de coordenadas, temos:

$$x_r = \begin{cases} m^2 - x_p - x_q, & se\ P \neq Q; \\ \\ m^2 - 2x_p, & se\ P = Q; \end{cases}$$

e

$$y_r = m(x_p - x_r) - y_p$$

Proposição 2.3 $(E(\mathbf{K}), +)$[1]*, onde* $+$ *é a operação de soma entre dois pontos de* $\mathbf{K}$*, é um grupo abeliano.*

A demonstração pode ser encontrada em (WASHINGTON, 2008), página 20.

A operação de soma é válida para qualquer corpo K, assim podemos trabalhar com curvas sobre corpos finitos. Neste trabalho, trabalharemos com curvas sobre o corpo $\mathbb{Z}_p$.

3. Curvas elípticas sobre o corpo $\mathbb{Z}_p$

Definição 3.1 *Uma curva elíptica sobre o corpo* $\mathbb{Z}_p$*, é o conjunto de pontos* (x, y) *com* $x, y \in \mathbb{Z}_p$*, tais que* $y^2 = x^3 + ax + b$*, com* $a, b \in \mathbb{Z}_p$ *e* $4a^3 + 27b^2 \neq 0$ *mod p incluindo o ponto no infinito* ∞*.*

A curva $\mathbb{Z}_p$ possui um número finito de pontos, pois existem p possibilidades para a coordenada x e, para cada valor de x, existem dois valores possíveis para y. Assim, acrescentando o ponto infinito, uma curva no ponto $\mathbb{Z}_p$, terá, no máximo, $2p + 1$ pontos.

A curva E($\mathbf{K}$) é um conjunto finito de pontos. No exemplo abaixo iremos determinar todos os pontos de uma equação cúbica.

Exemplo 3.2 *Determine todos os pontos da curva* $E(\mathbb{Z}_{11})$ *de equação* $y^2 = x^3 - x + 3$*.*

Solução:

Para descobrirmos se um ponto pertence à curva, pegamos cada valor de x*, substituímos em* $(x^3 - x + 3)$ *mod* 11 *e averiguamos se este resultado é o quadrado módulo* 11 *de algum* y*. A tabela abaixo apresenta todos os valores possíveis de* x *e* y*.*

[1]Um grupo $(G, *)$ é um conjunto G com uma operação binária $*$ definida sobre G, de tal forma que as seguintes propriedades sejam válidas:

- A operação * é associativa, isto é, $\forall a, b, c \in G$ temos $a * (b * c) = (a * b) * c$.
- Existe um elemento $e \in G$, chamado elemento neutro, tal que $\forall a \in G$ temos $a * e = e * a = a$.
- Para cada elemento $a \in G$ existe um elemento $a^{-1} \in G$, chamado elemento inverso, tal que $a * a^{-1} = a^{-1} * a = e$.

Se a operação $*$ for comutativa, o grupo é chamado grupo comutativo ou grupo abeliano.

y	y^2 *mod 11*	x	$x^3 - x + 3$ *mod 11*
0	*0*	*0*	*3*
1	*1*	*1*	*3*
2	*4*	*2*	*9*
3	*9*	*3*	*5*
4	*5*	*4*	*8*
5	*3*	*5*	*2*
6	*3*	*6*	*4*
7	*5*	*7*	*9*
8	*9*	*8*	*1*
9	*4*	*9*	*8*
10	*1*	*10*	*3*

Na tabela podemos observar, por exemplo, que para $x = 3$*, temos* $x^3 - x + 3 \equiv 5$ *mod* 11*, que por sua vez é quadrado módulo* 11 *de* $y = 4$ *e* $y = 7$*. Assim, os pontos* $(3, 4)$ *e* $(3, 7)$ *pertencem a curva. Note que para* $x = 5$ *temos* $x^3 - x + 3 \equiv 2$ *mod* 11*, mas não há nenhum valor de* y *cujo quadrado seja congruente a* 2 *módulo* 11*, ou seja, nenhum ponto da curva tem coordenada* $x = 5$*.*

Logo, os pontos da curva são:

$$(0,5), (0,6), (1,5), (1,6), (2,3), (2,8), (3,3), (3,7), (6,2), (6,9), (7,3), (7,8), (8,1), (8,10), (10,5)$$

$$e\ (10,6).$$

Podemos observar que quanto maior o número primo p, mais inacessível se torna determinar todos os pontos de $E(\mathbb{Z}_p)$.

Na curva $E(\mathbb{Z}_p)$, queremos calcular a soma entre dois pontos na forma algébrica. Vejamos o exemplo abaixo:

Exemplo 3.3 *Seja a curva* $E(\mathbb{Z}_{11})$ *de equação* $y^2 = x^3 - x + 3$ *e os pontos* $P = (1, 5)$ *e* $Q = (2, 8)$ *pertencentes a curva. Calcule as coordenadas do ponto* $R = P + Q$*.*

Solução:

Como $P \neq Q$ *e* $x_p \neq x_q$*, então*

$$m = \frac{y_q - y_p}{x_q - x_p} = 3.$$

Estamos trabalhando em $\mathbb{Z}_{11}$*, isto significa que* m *é o inteiro tal que* $1m \equiv 3$ *mod* 11*, logo,* $m = 3$*, pois* $1.3 = 3 \equiv 3$ *mod* 11*.*

Calculando a coordenada x_r:

$$x_r = (m^2 - x_p - x_q) \ mod \ 11$$

$$x_r = ((3)^2 - 1 - 2) \ mod \ 11$$

$$x_r = 6 \ mod \ 11.$$

Para y_r:

$$y_r = (m(x_p - x_r) - y_p) \ mod \ 11$$

$$y_r = (3(1 - 6) - 5) \ mod \ 11$$

$$y_r = -20 \equiv -9 \equiv 2 \ mod \ 11.$$

Logo, $R = (6, 2)$ e, pelo exemplo anterior, $R \in \mathbb{Z}_{11}$.

4. Logaritmo discreto elíptico

Já vimos que se realizarmos a soma $P + P$ temos como resultado $2P$, que é múltiplo de P. Realizando o mesmo procedimento e somando P novamente, teremos $2P + P$ e o seu resultado será $3P$, fazendo esse procedimento n vezes, com $n \in \mathbb{N}$, temos:

$$P + P + P + \cdots + P = nP.$$

Assim, dado um ponto $P \in E(\mathbb{Z}_p)$, podemos determinar os múltiplos $2P, 3P, \cdots, nP$ deste ponto P.

Exemplo 4.1 *Considere a curva $E(\mathbb{Z}_{13})$ de equação $y^2 = x^3 + 2x - 1$. Verifique se o ponto $P = (5, 2)$ pertence à curva e, em caso positivo, determine seus múltiplos.*

Solução: Encontrando os pontos da curva, que são: $(0, 5), (0, 8), (5, 2), (5, 11), (11, 0)$, $(12, 3)$ e $(12, 10)$. Temos que $P \in E(\mathbb{Z}_{13})$.

Iremos, agora, determinar os múltiplos de P pela definição da soma algébrica.

$$2P = P + P = (5; 2) + (5; 2) = (12, 3);$$

$$3P = 2P + P = (12; 3) + (5; 2) = (0, 8);$$

$$4P = 3P + P = (0; 8) + (5; 2) = (11, 0);$$

$$5P = 4P + P = (11; 0) + (5; 2) = (0, 5);$$

$$6P = 5P + P = (0; 5) + (5; 2) = (12, 10);$$

$$7P = 6P + P = (12; 10) + (5; 2) = (5, 11);$$

$$8P = 7P + P = (5; 11) + (5; 2) = \infty.$$

Observe que estes são os únicos múltiplos de P, pois como $8P = \infty$, a partir de $9P$ os resultados seriam repetidos.

Observe que, no exemplo anterior, todos os pontos da curva são múltiplos de $P = (5, 2)$, como $E(\mathbb{Z}_{13})$ com a operação de adição entre dois pontos é um grupo abeliano, dizemos que P é um gerador do grupo.

Podemos reescrever o Problema do Logaritmo Discreto em relação à operação de soma entre dois pontos de uma curva sobre $\mathbb{Z}_p$. Considere um ponto $P \in E(\mathbb{Z}_p)$ tal que P seja um gerador de $E(\mathbb{Z}_p)$. Assim, para cada $Q \in E(\mathbb{Z}_p)$, existe $n \in (\mathbb{Z}_p)$ tal que

$$Q = nP,$$

onde n é o Logaritmo Discreto Elíptico de Q em relação a P, representado por $n = \log_p(Q)$. O Problema do Logaritmo Discreto Elíptico baseia-se em determinar n para cada ponto Q.

5. Criptografia com Curvas Elípticas

O referencial teórico empregado nesta seção é averiguado na obra de (R.C.COMPUTADOR, 2019), (NO, 2019) e (F. B. LARA, 2010).

5.1. Protocolo Diffie-Hellman aplicado a curvas elípticas sobre $\mathbb{Z}_p$

Vamos supor que duas pessoas, Maria e João desejam criar e compartilhar uma chave de codificação segura. Neste protocolo, além do número primo p e do gerador P, a equação da curva $E(\mathbb{Z}_p)$ é pública, pois Maria e João precisam calcular os pontos usando a mesma curva. Abaixo está descrito a metodologia do Protocolo Diffie-Hellman :

- Maria e João escolhem um primo p, uma curva $E(\mathbb{Z}_p)$ de equação $y^2 = x^3 + Ax + B$ com $\Delta = 4A^3 + 27B^2 \neq 0$, e um ponto $P \in E(\mathbb{Z}_p)$ gerador do grupo.
- Maria escolhe um inteiro $n_A \in \mathbb{Z}_p$, mantem secreto, e calcula $Q_A = n_A P$ e envia Q_A para João.
- João escolhe um inteiro n_B, mantem secreto, calcula $Q_B = n_B P$ e envia Q_B para Maria.
- Maria calcula $R_A = n_A Q_B$, que equivale a

$$R_A = n_A(n_B P) = (n_A n_B)P.$$

- João calcula $R_B = n_B Q_A$, que equivale a

$$R_B = n_B(n_A P) = (n_A n_B)P.$$

- Logo a chave secreta é $R_{AB} = R_A = R_B$.

Podemos observar que o método para criar e compartilhar a chave secreta é o mesmo. Logo, a comunicação pode ser realizada por um criptossistema qualquer. Caso um terceiro consiga capturar a comunicação, deverá calcular o Logaritmo Discreto Elíptico de Q_A e Q_B para alcançar os dados iniciais.

Vejamos um exemplo:

Exemplo 5.1 *Considere a curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$ e o ponto $P = (1, 5)$ seu gerador.*

- *Suponhamos que Maria escolha $n_A = 3$, e calcule $Q_A = n_A P$, ou seja,*

$$P = (1, 5),$$

$$2P = (2, 8),$$

$$3P = (6, 2) = Q_A$$

e envia Q_A para João.

- *Suponhamos que João escolha $n_B = 2$, e calcule $Q_B = n_B P$, ou seja,*

$$P = (1, 5),$$

$$2P = (2, 8)$$

e envia Q_B para Maria.

- *Maria então calcula $R_A = n_A Q_B$, ou seja,*

$$R_A = 3.(2, 8) = (3, 4).$$

- *João calcula $R_B = n_B Q_A$. Temos:*

$$R_B = 2.(6, 2) = (3, 4).$$

Logo a chave secreta é $R_{AB} = R_A = R_B = (3, 4)$.

5.2. Criptossistema ElGamal

Iremos exemplificar o criptossistema de chave pública ElGamal utilizando, novamente, o caso Maria e João.

Mais uma vez, o primo p, a curva $E(\mathbb{Z}_p)$ da equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$, e o ponto $p \in E(\mathbb{Z}_p)$, gerador do grupo, são abertos para o público. Para iniciar o processo de encriptação João, que irá enviar uma mensagem a Maria, deve transformar a mensagem, que chamaremos de M, em um ponto $P_M \in E(\mathbb{Z}_p)$. Essa transformação pode ser realizada de várias maneiras, por exemplo, converter a mensagem por um inteiro utilizando a Tabela 1, onde cada letra do alfabeto, a partir de A recebe um valor numérico iniciado em 1.

Tabela 1: Tabela de conversão ElGamal

Letra	Valor	Letra	Valor	Letra	Valor
A	01	J	10	S	19
B	02	K	11	T	20
C	03	L	12	U	21
D	04	M	13	V	22
E	05	N	14	W	23
F	06	O	15	X	24
G	07	P	16	Y	25
H	08	Q	17	Z	26
I	09	R	18		

Fonte: A autora.

Feito isso, separamos esse inteiro em duas coordenadas de um ponto, de maneira que este ponto pertença à curva $E(\mathbb{Z}_p)$. Caso o ponto gerado não pertença à curva, habitualmente acrescenta-se zero, ou outro algarismo ajustado entre as partes, no caso João e Maria, até que as coordenadas encontradas formem um ponto de $E(\mathbb{Z}_p)$.

Realizada esta transformação podemos iniciar a codificação.

Abaixo está descrito a metodologia do Criptossistema ElGgamal:

1. Maria escolhe um inteiro secreto $n_A \in \mathbb{Z}_p$, calcula $Q_A = n_A P$ e envia Q_A para João.

2. João escolhe um inteiro aleatório k e calcula

$$R = kP \text{ e } S = P_M + kQ_A$$

3. João envia para Maria o par de pontos (R, S).

Para Maria decifrar a mensagem, basta calcular $S - n_A R$:

$$S - n_A R = P_M + kQ_A - n_A.kP = P_M + k.n_A P - k.n_A P = P_M.$$

Vejamos um exemplo:

Exemplo 5.2 *Considere a curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$ e o ponto $P = (1, 5)$ gerador de $E(\mathbb{Z}_{11})$ com a operação de soma entre dois pontos. Transforme a mensagem M em um ponto P_M da curva.*

Solução:

Utilizando a tabela de conversão ELGamal temos que a mensagem M = FI, em termos numéricos, corresponde ao inteiro 0609*, pois F*=06 *e I*=09*. Desmembrando este inteiro em duas coordenadas, encontramos o ponto $(06, 09) = (6, 9)$, vamos verificar se este ponto pertence a curva:*

$$y^2 = 9^2 = 81 \equiv 4 \ mod\ 11$$

$$x^3 - x + 3 = (6)^3 - 6 + 3 \equiv 216 - 6 + 3 = 213 \equiv 4 \ mod\ 11$$

Logo, a mensagem M é transformada no ponto $P_M = (6, 9)$.

Exemplo 5.3 *Agora, vamos supor, que João deseja enviar a mensagem M para Maria empregando o primo, a curva e o ponto gerador do exemplo anterior. Faça a codificação e decodificação da mensagem M utilizando o criptossistema ElGamal.*

Solução:

Usando os dados do exemplo anterior temos que $P_M = (6, 9)$. Vejamos os passos do ElGamal:

1. *Suponhamos que Maria escolha $nA = 3$. Temos:*

$$P = (1, 5)$$

$$2P = (2, 8)$$

$$3P = (6, 2) = Q_A$$

e envia para João.

2. *Suponhamos que João escolha $k = 2$, temos:*

$$R = kP = 2(1, 5) = (2, 8)$$

e

$$S = P_M = (6, 9) + KQ_A = (6, 9) + 2(6, 2) = (6, 9) + (3, 4) = (6, 2).$$

3. *João envia para Maria p par de pontos* (R, S)

   Para decodificar a mensagem, basta Maria calcular

$$S - n_A R = (6,2) - 3(2,8) = (6,2) - (3,4) = (6,2) + (3,4 = (6,2) + (3,7) = (6,9) = P_M.$$

Assim, Maria consegue ler a mensagem.

Referências

1 ANDRADE, E. G. **Criptografia com curvas elipticas**. 2016. f. 78. Mestrado Profissional em Matemática - PROFMAT – Universidade Federal do Pará Instituto de Ciências Exatas e Naturais, Belém/AM.

2 CONHECIMENTO COMPUTADOR, Rede de. **Quais são as vantagens e desvantagens de Elliptic Curve Cryptography para segurança sem fio**. edicao. Internet, 2019. p. 1. Disponível em: ¡ptcomputador.com/Networking/wireless-networking/81737.html¿.

3 CORREIA, S. S. J. **Criptografia via curvas elípticas**. 2013. f. 87. Mestrado Profissional em Matemática - PROFMAT – Universidade Federal do Estado do Rio de Janeiro - UNIRIO, Rio de Janeiro/RJ.

4 DESCONHECIDO. **Segurança Lógica de Software**. edicao. Internet, 2019. p. 1. Disponível em: ¡segurancalogica01.blogspot.com/2008/04/criptografia-com-o-usode-%20curvas.html¿.

5 F. B. LARA, P. C. S; Oliveira. **Curvas Elípticas: Aplicação em Criptografia Assimétrica.** Petrópolis/RJ: [s.n.], 2010.

6 OLIVEIRA, J. G. Curvas Elípticas sobre Corpos Finitos e Criptografia de Chave. In: COLÓQUIO DE MATEMÁTICA DA REGIÃO CENTRO-OESTE, I., 2009, Universidade Federal do Mato Grosso do Sul. CADERNO do Minicurso. Campo Grande/MS: SBM, 2009. p. 1–12.

7 WASHINGTON, L. C. **Elliptic Curves: number theory and criptography**. 2nd edition. Boca Raton: Chapman e Hall, 2008. p. 531.