# As Fórmulas de Cardano e um Criptossistema do tipo RSA

# The Cardano formulas and an RSA-type cryptosystem

**Antônio de Andrade e Silva**
Departamento de Matemática
Universidade Federal da Paraíba - UFPB, João Pessoa, PB
*andrade@mat.ufpb.br*

**João Bosco Batista Lacerda**
Departamento de Matemática
Universidade Federal da Paraíba - UFPB, João Pessoa, PB
*boscolacerda@mat.ufpb.br*

**Resumo:** Nestas notas caracterizaremos as raízes de uma cúbica, via fórmulas de Cardano, sobre um corpo de Galois $\mathbb{F}_p$ tendo uma característica positiva $p$. Como aplicação, apresentaremos um criptossistema com chave pública do tipo RSA baseado nas propriedades de uma par sequência recursiva linear homogênea de ordem três sobre um anel finito $\mathbb{Z}_p$.

**Palavras-chave:** campo de extensão cúbico finito; chave pública do tipo RSA; fórmulas de Cardano; sequência característica.

**Abstract:** In these notes we will characterize the cubic roots, via Cardano formulas, on a body of Galois $\mathbb{F}$ with a positive characteristic $p$. As application, we will present a cryptosystem with public-key of the RSA-type based on the properties of third-order linear feedback shift-register sequences over a finite ring $\mathbb{Z}_p$.

**Keywords:** characteristic sequence; cubic finite field extension; public-key of the RSA-type; The Cardano formulas.

Recebido em 07/04/2014 - Aceito em 28/08/2014.

# 1 Introdução

A *Criptografia* é a arte ou ciência de escrever mensagens em cifra ou códigos e é tão antiga quanto a própria escrita, já estava presente no sistema de escrita hieroglífico dos egípcios. O imperador romano Júlio César utilizava o criptossistema denominado de *Cifra de César* para codificar suas mensagens de planos de batalhas. Durante a Segunda Guerra Mundial, os ingleses ficaram conhecidos por seus esforços para a decifração de mensagens. Com a invenção do computador, a área floresceu incorporando complexos algoritmos matemáticos e esse trabalho criptográfico formou a base para a ciência da computação moderna.

O primeiro sistema de criptografia com chave pública foi desenvolvido por W. Diffie e M. Hellman em 1976. Este sistema criptográfico funciona da seguinte maneira. Dado um grupo cíclico finito $G$ (alfabeto) e $g$ o seu gerador (públicos). Assim, dois usuários $A$ e $B$ segue os seguintes passos.

1. O usuário $A$ gera aleatoriamente um inteiro $a$ (chave secreta) e calcula $g^a$ em $G$; em seguida envia $g^a$ (chave pública) para o usuário $B$.

2. O usuário $B$ gera aleatoriamente um inteiro $b$ (chave secreta) e calcula $g^b$ em $G$; em seguida envia $g^b$ (chave pública) para o usuário $A$.

3. O usuário $A$ recebe $g^b$ e calcula $(g^b)^a$.

4. O usuário $B$ recebe $g^a$ e calcula $(g^a)^b$.

Portanto, os usuários $A$ e $B$ compartilham o mesmo elemento $g^{ab}$ em $G$. Neste caso, o problema é produzir um algoritmo eficiente para computar $g^{ab}$ de $g^a$ e $g^b$.

O criptossistema com chave pública *RSA* foi desenvolvido por R. L. Rivest, A. Shamir e L. Adleman em 1978. Este sistema criptográfico funciona semelhante ao anterior. São criadas duas chaves, uma chave de codificação que será pública e uma chave de decodificação que será privada. Assim, se um usuário $A$ deseja enviar uma mensagem para um usuário $B$, então $A$ usa a chave de codificação de $B$ para codificar a mensagem e envia essa mensagem codificada para $B$, quando $B$ recebe a mensagem

codificada usa sua chave de decodificação, que apenas ele conhece, e decodifica a mensagem codificada, obtendo assim a mensagem original.

## 2 Cúbicas

Nesta seção, faremos um estudo da equação cúbica

$$f(x) = x^3 + ax^2 + bx + c = 0,$$

sobre um corpo finito $\mathbb{F}$. O leitor interessado em mais detalhes sobre corpos finitos e equações polinomiais sobre corpos finitos pode consultar [1, 2].

Qualquer corpo finito $\mathbb{F}$ é de característica um número primo $p$, de ordem $|\mathbb{F}| = q = p^k$, para algum $k \in \mathbb{N}$. Neste caso, o grau $[\mathbb{F} : \mathbb{Z}_p] = k$, em que $\mathbb{Z}_p$ é o *corpo primo* de $\mathbb{F}$ e

$$\mathbb{Z}_p \simeq \mathbb{F}_p = GF(p) = \{0, 1, \ldots, p-1\}$$

é o *corpo de Galois* de ordem $p$. Vamos denotar por $\mathbb{F}^*$ o grupo multiplicativo (cíclico) de $\mathbb{F}$. Então, $|\mathbb{F}^*| = q-1$ e $\alpha^{q-1} = 1$, para todo $\alpha \in \mathbb{F}^*$. Assim, $\alpha^q = \alpha$, para todo $\alpha \in \mathbb{F}$. Portanto,

$$x^q - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha) \in \mathbb{F}[x].$$

Consequentemente, $\mathbb{F}_q = Gal(x^q - x, \mathbb{Z}_p)$ é o *corpo de Galois* de $x^q - x$ sobre $\mathbb{Z}_p$, ou seja, $\mathbb{F}_q$ é a menor extensão de $\mathbb{Z}_p$ que contém todas as raízes de $x^q - x \in \mathbb{Z}_p[x]$, e $\mathbb{F}_q$ é uma extensão Galoisiana de $\mathbb{Z}_p$. Em particular, seja $f(x)$ um polinômio irredutível de grau $m$ sobre $\mathbb{Z}_p$. Então, $f(x)$ divide $x^q - x$ em $\mathbb{Z}_p[x]$ se, e somente se, $m$ divide $k$. Neste caso, se $\alpha \in \mathbb{F}_q$ é uma raiz de $f(x)$, então:

$$\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}} \in \mathbb{F}_q$$

são todas as outras raízes de $f(x)$, chamadas de *conjugadas* de $\alpha$. Se $f(0) \neq 0$, diremos que o menor $t \in \mathbb{N}$ tal que $f(x)$ divide $x^t - 1$ é a *ordem* de $f(x)$ e denotaremos por $t = ord(f)$. Portanto, $t \leq q - 1$.

**Teorema 1:** *Seja $f(x) \in \mathbb{Z}_p[x]$, com grau $m$ e $f(0) \neq 0$.*

1. *Se $f(x)$ é irredutível sobre $\mathbb{Z}_p$, então $ord(f)$ é igual a ordem de qualquer raiz $\alpha$ de $f(x)$ em $\mathbb{F}_q^*$. Em particular, $ord(f)$ divide $q-1=p^m-1$.*

2. *$f(x)$ divide $x^n-1$ se, e somente se, $ord(f)$ divide $n$, para todo $n\in\mathbb{N}$.*

3. *Se $f(x)=f_1(x)\cdots f_l(x)$ é a fatoração de $f(x)$ em fatores irredutíveis distintos, então $ord(f)$ é igual ao mínimo múltiplo comum de $ord(f_1)$,..., $ord(f_l)$.*

Por exemplo, se $p=5$, $q=5^3$ e

$$f(x)=x^3-3x^2+2x-1=(x-3)(x^2+0x+2)\in\mathbb{Z}_5[x]$$

então $ord(f)=mmc(4,8)=8$. Observe que $ord(x-3)$ divide $p-1$ e $ord(x^2+2)$ divide $p^2-1$.

Seja $\mathbb{L}$ qualquer extensão $\mathbb{F}_q$ tal que $|\mathbb{L}|=q^l$, para algum $l\in\mathbb{N}$. Então, a função $\sigma:\mathbb{L}\to\mathbb{L}$ definida como $\sigma(x)=x^q$ é bijetora e satisfaz as condições

$$\sigma(x+y)=\sigma(x)+\sigma(x) \text{ e } \sigma(xy)=\sigma(x)\sigma(y), \ \forall \ x,y\in\mathbb{L}.$$

Em particular, $\sigma(\alpha)=\alpha$, para todo $\alpha\in\mathbb{F}_q$. Portanto, $\sigma\in G=Gal(\mathbb{L}/\mathbb{F}_q)$ o *grupo de Galois* de $\mathbb{L}$ sobre $\mathbb{F}_q$, que é um subgrupo do grupo dos automorfismo de $Aut(\mathbb{L})$ que fixam os elementos de $\mathbb{F}_q$. Observe que:

$$G=\{I,\sigma,\ldots,\sigma^{l-1}\}=\langle\sigma\rangle$$

é um grupo cíclico gerado por $\sigma$. Pode ser provado que se $f(x)$ é um polinômio mônico irredutível de grau $m$ sobre $\mathbb{F}_q$, então:

$$\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}=\{a_0+a_1\alpha+\cdots+a_{m-1}\alpha^{m-1}:a_0,a_1,\ldots,a_{m-1}\in\mathbb{F}_q\}=\mathbb{F}_q[\alpha]\simeq\mathbb{F}_q^m,$$

em que

$$\langle f(x)\rangle=\{f(x)g(x):g(x)\in\mathbb{F}_q[x]\}$$

e $\alpha=x+\langle f(x)\rangle$ é a classe de equivalência de $x$, é um corpo. Em particular, um espaço

vetorial sobre $\mathbb{F}_q$, com uma base

$$\mathscr{B} = \{1, \alpha, \ldots, \alpha^{m-1}\}.$$

Neste caso, $f$ possui todas as suas raízes em $\mathbb{F}_q[\alpha]$ e $f(x)$ chama-se o *polinômio minimal* de $\alpha$ sobre $\mathbb{F}_q$.

Em tudo que segue $\mathbb{F} = \mathbb{F}_q$ significa um corpo finito de característica $p$ diferente de 2, 3 e $|\mathbb{F}| = q = p^k$, para algum $k \in \mathbb{N}$. Seja :

$$f(x) = x^3 + ax^2 + bx + c \in \mathbb{F}[x].$$

Então, fazendo a mudança $y = x + 3^{-1}a$, obtemos:

$$g(y) = y^3 + Ay + B,$$

em que

$$A = \frac{1}{3}(3b - a^2), B = \frac{1}{27}(2a^3 - 9ab + 27c) \in \mathbb{F}.$$

Como $3^{-1}a \in \mathbb{F}$ temos que $\mathbb{L} = Gal(f, \mathbb{F}) = Gal(g, \mathbb{F})$. Sejam $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{L}$ as raízes de $g(y)$. Então $\mathbb{L} = \mathbb{F}[\alpha_1, \alpha_2, \alpha_3]$ e

$$y^3 + Ay + B = (y - \alpha_1)(y - \alpha_2)(y - \alpha_3).$$

Assim, teremos as relações:

$$\begin{aligned} p_1 &= \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ p_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = A \\ p_3 &= \alpha_1\alpha_2\alpha_3 = -B \\ p_j &= 0, \ \forall \ j \geq 4, \end{aligned}$$

e o sistema

$$\alpha_j^3 = -(A\alpha_j + B), \quad j = 1, 2, 3.$$

Portanto, usando as relações e o sistema, obtemos as fórmulas de Newton em termos de $A$ e $B$ a partir de:

$$s_0 = 3 \text{ e } s_k = \alpha_1^k + \alpha_2^k + \alpha_3^k, \ \forall \ k \in \mathbb{N},$$

a saber,

$$s_k = \begin{cases} \sum_{i=1}^{k-1} (-1)^{i+1} p_i s_{k-i} + (-1)^{k+1} k p_k, & \text{se } k \leq 3 \\ \sum_{i=1}^{3} (-1)^{i+1} p_i s_{k-i}, & \text{se } k > 3. \end{cases}$$

Por exemplo,

$$\begin{aligned} s_1 &= p_1 = 0 \\ s_2 &= p_1^2 - 2p_2 = -2A \\ s_3 &= p_1^3 - 3p_1 p_2 + 3p_3 = -3B \\ s_4 &= p_1^3 - 4p_1^2 p_2 + 4p_1 p_3 + 2p_2^2 = 2A^2. \end{aligned}$$

Consideremos o determinante de Vandermonde

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \det \begin{bmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{bmatrix}.$$

O *discriminante* de $g(y)$ é definido como $\Delta = \delta^2$. Neste caso,

$$\Delta = \det \begin{bmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{bmatrix} = -(4A^3 + 27B^2).$$

É fácil verificar que o discriminante de $f(x)$ e $g(y)$ são iguais. Expressando $\Delta$ em termos de $a$, $b$ e $c$:

$$\Delta = a^2 b^2 - 4b^3 - 4a^3 c - 27c^2 + 18abc \in \mathbb{F}.$$

Note que, se $g(y)$ é redutível sobre $\mathbb{F}$, então:

$$g(y) = (y-\alpha_1)(y-\alpha_2)(y-\alpha_3) \text{ ou } g(y) = (y-\alpha)h(y),$$

onde $\alpha, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$ e $h(y)$ é irredutível sobre $\mathbb{F}$. Portanto, $|G| = |Gal(\mathbb{L}/\mathbb{F})| = 1$ ou 2. Suponhamos que $g(y)$ seja irredutível sobre $\mathbb{F}$ e $\sigma \in G$. Então,

$$g(\sigma(\alpha_1)) = B + A\sigma(\alpha_1) + \sigma(\alpha_1)^3 = \sigma(B + A\alpha_1 + \alpha_1^3) = \sigma(0) = 0.$$

Logo, $\sigma(\alpha_1) \in \mathbb{L}$ é uma raiz de $g$, isto é, as raízes de $g$ são permutadas por qualquer $\sigma \in G$. Assim, se $S = \{\alpha_1, \alpha_2, \alpha_3\} \subseteq \mathbb{L}$, então a função $\varphi_\sigma : S \to S$ definida como $\varphi_\sigma(\alpha_j) = \sigma(\alpha_j)$ é bijetora. Portanto, $\varphi_\sigma \in P(\mathscr{S})$, para todo $\sigma \in G$. Consequentemente, a função $\varphi : G \to P(\mathscr{S})$ definida como $\varphi(\sigma) = \varphi_\sigma$ é um monomorfismo de grupos. Assim, $G$ é isomorfo a um subgrupo do grupo de permutações $P(\mathscr{S}) \simeq S_3$. Neste caso, $G \simeq A_3$ o grupo das permutações pares ou $G \simeq S_3$. Note que

$$\sigma(\delta) = (\alpha_{\sigma(1)} - \alpha_{\sigma(2)})(\alpha_{\sigma(1)} - \alpha_{\sigma(3)})(\alpha_{\sigma(2)} - \alpha_{\sigma(3)}) = \pm\delta, \quad \forall \ \sigma \in G.$$

Então, $\sigma(\delta^2) = \delta^2$ e $\Delta = \delta^2 \in \mathbb{F}$. Logo, $\delta$ é uma raiz do polinômio $h(x) = x^2 - \delta^2 \in \mathbb{F}[x]$. Assim, se $h(x)$ é redutível sobre $\mathbb{F}$, então $\delta \in \mathbb{F}$. Neste caso, $G \simeq A_3$, $[\mathbb{L} : \mathbb{F}] = 3$ ($\mathbb{L} = \mathbb{F}[\alpha_1]$) e $\Delta$ é o quadrado de um elemento de $\mathbb{F}$. Se $h(x)$ é irredutível sobre $\mathbb{F}$, então $\delta \notin \mathbb{F}$. Neste caso, $G \simeq S_3$, $[\mathbb{L} : \mathbb{F}] = 6$ e $\Delta$ não é o quadrado de um elemento de $\mathbb{F}$. Observe que $G = \langle \sigma, \tau \rangle$, onde $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$, $\sigma(\alpha_3) = \alpha_1$ e $\sigma(\delta) = \delta$; $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$ e $\tau(\alpha_j) = \alpha_j$, $j = 1, 2, 3$. Portanto, $[\mathbb{L} : \mathbb{F}[\sqrt{\Delta}]] = 3$ é uma extensão cíclica de grau 3 e $G = \langle \sigma \rangle \simeq A_3$ é um grupo cíclico. Resumiremos isto no seguinte teorema:

**Teorema 2:** *Sejam* $g(y) = y^3 + Ay + B \in \mathbb{F}[y]$, *com discriminante* $\Delta \neq 0$ *e* $\mathbb{L} = Gal(g, \mathbb{F})$ *Então*:

1. $g(y)$ *é redutível sobre* $\mathbb{F}$ *se, e somente se,*

$$g(y) = (y-\alpha_1)(y-\alpha_2)(y-\alpha_3) \text{ ou } g(y) = (y-\alpha)h(y),$$

*onde* $\alpha, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$ *e* $h(y)$ *é irredutível sobre* $\mathbb{F}$. *No último caso, se, e somente se,* $\Delta$ *não é um quadrado em* $\mathbb{F}$.

2. $g(y)$ *é irredutível sobre* $\mathbb{F}$ *se, e somente se,* $g(y)$ *não possui raízes em* $\mathbb{F}$.

3. *Se* $g(y)$ *é irredutível sobre* $\mathbb{F}$, *então* $G = Gal(\mathbb{L}/\mathbb{F}) \simeq A_3$ *se, e somente se,* $\Delta$ *é um quadrado em* $\mathbb{F}$.

4. *Se* $g(y)$ *é irredutível sobre* $\mathbb{F}$, *então* $G = Gal(\mathbb{L}/\mathbb{F}) \simeq S_3$ *se, e somente se,* $\Delta$ *não é um quadrado em* $\mathbb{F}$.

Para obtermos mais informações sobre $g(y)$, vamos determinar explicitamente as raízes de $g(y)$. Para isto, adjuntamos a $\mathbb{L}$ as raízes cúbicas da unidade

$$1, \ \ \omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2} \ \text{ e } \ \omega^2 = -\frac{1}{2} - \frac{\sqrt{-3}}{2} = \omega^{-1}.$$

Então,

$$\omega^3 = 1 \ \text{ e } \ 1 + \omega + \omega^2 = 0.$$

Pondo

$$\mathbb{K} = \mathbb{F}[\sqrt{\Delta}, \omega] = \mathbb{F}[\sqrt{\Delta}, \sqrt{-3}] \ \text{ e } \ \mathbb{M} = \mathbb{L}[\omega] = \mathbb{L}[\sqrt{-3}]$$

temos, em geral, que $\mathbb{K} \neq \mathbb{F}[\sqrt{\Delta}]$ e $\mathbb{M} \neq \mathbb{L}$. Então, $\mathbb{M}$ é uma extensão cíclica de $\mathbb{K}$ e $G = Gal(\mathbb{M}/\mathbb{K}) = \langle \sigma \rangle \simeq A_3$ é um grupo cíclico. Assim, podemos considerar a *resolvente de Lagrange* $Lag : \mathbb{M} \to \mathbb{M}$ definida como

$$Lag(\rho, \beta) = \beta + \rho\sigma(\beta) + \rho^2\sigma^2(\beta), \ \ \forall \ \ \beta \in \mathbb{M} \ \text{ e } \ \rho^3 = 1.$$

Em particular,

$$\begin{aligned} t &= Lag(1, \alpha_1) = \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ u &= Lag(\omega, \alpha_1) = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \\ v &= Lag(\omega^2, \alpha_1) = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3. \end{aligned}$$

Observe que:

$$\sigma(u) = \alpha_2 + \omega\alpha_3 + \omega^2\alpha_1 \Rightarrow \omega\sigma(u) = u.$$

Assim, $u^3 = \sigma(u^3)$ e $u^3, v^3 \in \mathbb{K}$. Além disso, como $t = 0$ temos que

$$\begin{aligned} t + u + v &= u + v = 3\alpha_1 \\ t + \omega^2 u + \omega v &= \omega^2 u + \omega v = 3\alpha_2 \\ t + \omega u + \omega^2 v &= \omega u + \omega^2 v = 3\alpha_3. \end{aligned}$$

Primeiro temos que

$$u^3 + v^3 = (u + v)(u + \omega v)(u + \omega^2 v) = 27\alpha_1\alpha_2\alpha_3 = -27B$$

e com alguns cálculos $uv = -3A$ ou $u^3v^3 = -27A^3$. Assim, $u^3$ e $v^3$ são as raízes da equação

$$z^2 + 27Bz - 27A^3 = 0,$$

ou seja,

$$u^3 = -\frac{27}{2}B + \frac{1}{2}\sqrt{-27\Delta} \text{ e } v^3 = -\frac{27}{2}B - \frac{1}{2}\sqrt{-27\Delta}.$$

Note que $u$ é uma raiz do polinômio irredutível $h(x) = x^3 - u^3 \in \mathbb{K}[x]$. Então, $\mathbb{M} = Gal(h, \mathbb{K})$. Portanto,

$$u, \omega u, \omega^2 u \in \mathbb{M}$$

são as raízes de $h(x)$. De modo análogo,

$$v, \omega v, \omega^2 v \in \mathbb{M}.$$

Como $uv = -3A$ devemos ter

$$\begin{aligned} \alpha_1 &= \frac{1}{3}(u + v) \\ \alpha_2 &= \frac{1}{3}(\omega^2 u + \omega v) \\ \alpha_3 &= \frac{1}{3}(\omega u + \omega^2 v) \end{aligned}$$

as raízes de $g(y)$ em $\mathbb{M}$, com

$$u = \sqrt[3]{-\frac{27}{2}B + \frac{1}{2}\sqrt{-27\Delta}} \text{ e } v = \sqrt[3]{-\frac{27}{2}B - \frac{1}{2}\sqrt{-27\Delta}}.$$

As fórmulas obtidas acima são chamadas de *fórmulas de Cardano*.

**Teorema 3:** *Seja* $g(y) = y^3 + Ay + B \in \mathbb{F}[y]$, *com* $A \neq 0$ *e* $\Delta = -(4A^3 + 27B^2) \neq 0$. *Então*:

1. $g(y)$ *possui três raízes em* $\mathbb{F}$ *se, e somente se,* $\Delta$ *é quadrado em* $\mathbb{F}$ *e*

$$\left(\frac{-27B + \sqrt{-27\Delta}}{-27B - \sqrt{-27\Delta}}\right)^{2m} = 1, \text{ onde } m \in \left\{\frac{q-1}{6}, \frac{q+1}{6}\right\}.$$

2. $g(y)$ *não possui raízes em* $\mathbb{F}$ *se, e somente se,*

$$\left(\frac{-27B + \sqrt{-27\Delta}}{-27B - \sqrt{-27\Delta}}\right)^{2m} \neq 1, \text{ onde } m \in \left\{\frac{q-1}{6}, \frac{q+1}{6}\right\}.$$

**Prova**. Sejam $\mathbb{F}_6$ uma extensão de $\mathbb{F}$ tal que $|\mathbb{F}_6| = q^6$ e $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_6$ as raízes de $g(y)$. Já vimos que $\omega$ é uma raiz do polinômio $\phi_3(x) = x^2 + x + 1 \in \mathbb{F}[x]$ e que $\omega \in \mathbb{F}_2 = \mathbb{F}[\sqrt{-3}] = \mathbb{F}[\omega]$ é um subcorpo de $\mathbb{F}_6$. Então, $[\mathbb{F}_2 : \mathbb{F}] \leq 2$. Como $\omega^{q^2-1} = 1$ e $\omega^3 = 1$ temos que 3 divide $q^2 - 1$. Neste caso, 3 divide $q-1$ ou 3 divide $q+1$. Se 3 divide $q-1$, então $\omega \in \mathbb{F}$ e $[\mathbb{F}_2 : \mathbb{F}] = 1$. Se 3 divide $q+1$, então $\omega \notin \mathbb{F}$ e $[\mathbb{F}_2 : \mathbb{F}] = 2$. Portanto,

$$q = 6m \pm 1 \text{ ou } m \in \left\{\frac{q-1}{6}, \frac{q+1}{6}\right\},$$

pois $mdc(6, q) = 1$ e $q$ é um número ímpar. Neste caso, $\omega^q = \omega$ ou $\omega^q = \omega^2$.

(1) $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$ se, e somente se, $\Delta = \delta^2 \in \mathbb{F}$ e $\Delta$ é um quadrado em $\mathbb{F}$. Para provar a segunda afirmação consideremos as resolventes de Lagrange

$$u = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \text{ e } v = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.$$

Então,

$$u^q = \alpha_1 + \omega^q \alpha_2 + \omega^{2q} \alpha_3 \text{ e } v^q = \alpha_1 + \omega^{2q} \alpha_2 + \omega^q \alpha_3.$$

Assim,

$$\begin{aligned} u^q &= u \text{ ou } u^q = v \\ v^q &= v \text{ ou } v^q = u, \end{aligned}$$

pois $\omega^q = \omega$ ou $\omega^q = \omega^2$. Logo, dividindo, teremos

$$\left(\frac{u}{v}\right)^{q-1} = 1 \text{ ou } \left(\frac{u}{v}\right)^{q+1} = 1 \Leftrightarrow \left(\frac{u}{v}\right)^{2m} = 1,$$

ou seja,

$$\left(\frac{-27B + \sqrt{-27\Delta}}{-27B - \sqrt{-27\Delta}}\right)^{2m} = 1.$$

Portanto, $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$ se, e somente se, $\Delta$ é um quadrado em $\mathbb{F}$ e $(uv^{-1})^{2m} = 1$.

(2) Suponhamos que $g(y)$ não possua raízes em $\mathbb{F}$. Então $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_3$, em que $\mathbb{F}_3$ é um subcorpo de $\mathbb{F}_6$ tal que $|\mathbb{F}_3| = q^3$. Assim, podemos escolher $\sigma \in Gal(\mathbb{F}_6/\mathbb{F})$ tal que

$$\alpha_2 = \sigma(\alpha_1) = \alpha_1^q, \ \alpha_3 = \sigma(\alpha_2) = \alpha_2^q \text{ e } \alpha_1 = \sigma(\alpha_3) = \alpha_3^q.$$

Então:

$$\begin{aligned} u^q &= \alpha_2 + \omega^q \alpha_3 + \omega^{2q} \alpha_1 = \omega^{2q}(\alpha_1 + \omega^q \alpha_2 + \omega^{2q} \alpha_3) \\ v^q &= \alpha_2 + \omega^{2q} \alpha_3 + \omega^q \alpha_1 = \omega^q(\alpha_1 + \omega^{2q} \alpha_2 + \omega^q \alpha_3). \end{aligned}$$

Assim,

$$\begin{aligned} u^q &= \omega^2 u \text{ ou } u^q = \omega v \\ v^q &= \omega v \text{ ou } v^q = \omega^2 u, \end{aligned}$$

pois $\omega^q = \omega$ ou $\omega^q = \omega^2$. Logo, dividindo, teremos

$$\left(\frac{u}{v}\right)^{q-1} = \omega \text{ ou } \left(\frac{u}{v}\right)^{q+1} = \omega^{-1},$$

ou seja,

$$\left(\frac{-27B + \sqrt{-27\Delta}}{-27B - \sqrt{-27\Delta}}\right)^{2m} \neq 1.$$

Portanto, $g(y)$ não possui raízes em $\mathbb{F}$ se, e somente se,

$$\left(\frac{-27B + \sqrt{-27\Delta}}{-27B - \sqrt{-27\Delta}}\right)^{2m} \neq 1,$$

que é o resultado desejado. ■

Observe que a condição

$$\left(\frac{-27B + \sqrt{-27\Delta}}{-27B - \sqrt{-27\Delta}}\right)^{2m} = 1$$

é equivalente a $h(-27B^2\Delta^{-1}) = 0$, com

$$h(x) = \binom{2m}{1} + \binom{2m}{3}x + \cdots + \binom{2m}{2m-1}x^{m-1} \in \mathbb{F}[x],$$

pois

$$\left(\frac{-27B + \sqrt{-27\Delta}}{-27B - \sqrt{-27\Delta}}\right)^{2m} = 1$$

é equivalente a:

$$\left(1 + \sqrt{-27B^2\Delta^{-1}}\right)^{2m} - \left(1 - \sqrt{-27B^2\Delta^{-1}}\right)^{2m} = 0.$$

Assim, aplicando o Teorema Binomial e dividindo por $2\sqrt{-27B^2\Delta^{-1}}$, obtemos

$$h(-27B^2\Delta^{-1}) = 0.$$

## 3 Sequências recorrentes

Nesta seção, faremos um estudo de sequência recorrente linear gerada pelo polinômio cúbico

$$f(x) = x^3 - ax^2 + bx - 1 \in \mathbb{F}[x]$$

sobre o corpo finito $\mathbb{F} = \mathbb{Z}_p$. O leitor interessado em mais detalhes sobre sequências recorrentes lineares sobre corpos finitos gerais pode consultar [1, 3].

Já vimos que:

$$\frac{\mathbb{F}[x]}{\langle f(x)\rangle} = \{a_0 + a_1\alpha + a_2\alpha^2 : a_0, a_1, a_2 \in \mathbb{F}\} = \mathbb{F}[\alpha] \simeq \mathbb{F}^3,$$

em que $\alpha = x + \langle f(x)\rangle$ é a classe de equivalência de $x$, é uma álgebra sobre $\mathbb{F}$, ou seja, é um anel que possui uma estrutura de espaço vetorial sobre $\mathbb{F}$, com uma base

$$\mathscr{B} = \{1, \alpha, \alpha^2\}.$$

Neste caso, $f$ possui todas as suas raízes em $\mathbb{L} = \mathbb{F}[\alpha]$. É claro que a função $\phi_\alpha : \mathbb{L} \to \mathbb{L}$ definida como $\phi_\alpha(\beta) = \alpha\beta$ é um operador $\mathbb{F}$-linear. Se $End_{\mathbb{F}}(\mathbb{L})$ é o conjunto de todos os operadores $\mathbb{F}$-lineares, então a função $\varphi : \mathbb{L} \to End_{\mathbb{F}}(\mathbb{L})$ definida como $\varphi(\alpha) = \phi_\alpha$ é um $\mathbb{F}$-homomorfismo de álgebras injetor. Portanto, podemos identificar $\mathbb{L}$ com a sub-álgebra $\mathbb{M} = \varphi(\mathbb{L})$ de $End_{\mathbb{F}}(\mathbb{L})$. Neste caso,

$$\varphi(\mathscr{B}) = \{\phi_1, \phi_\alpha, \phi_\alpha^2\} = \{I, \phi_\alpha, \phi_\alpha^2\}$$

é uma base de $\mathbb{M}$. A representação matricial de $\phi_\alpha$ em relação à base $\mathscr{B}$ é dada por

$$A = A_f = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -b \\ 0 & 1 & a \end{bmatrix}$$

a qual chama-se *matriz companheira* de $f(x)$. Note que

$$f(x) = \det(x\boldsymbol{I}_3 - \boldsymbol{A})$$

é o *polinômio característico* de $\boldsymbol{A}$. Como $I$, $\phi_\alpha$ e $\phi_\alpha^2$ são $LI$ temos que $\boldsymbol{I}$, $\boldsymbol{A}$ e $\boldsymbol{A}^2$ também o são. Mas, $f(\alpha) = 0$ implica que $f(\boldsymbol{A}) = \boldsymbol{O}$. Portanto, $f(x)$ é o *polinômio minimal* de $\boldsymbol{A}$, pois o grau de $f(x)$ é igual a 3. Consequentemente, $f(x)$ é o polinômio característico e minimal de $\boldsymbol{A}$.

Sejam $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{L}$ as raízes distintas de $f(x)$. Então, de modo semelhante à Seção anterior, obtemos as relações:

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= a \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= b \\ \alpha_1\alpha_2\alpha_3 &= 1 \end{aligned}$$

e o sistema

$$\alpha_j^3 = a\alpha_j^2 - b\alpha_j + 1, \quad j = 1,2,3. \tag{3.1}$$

Portanto,

$$s_k = s_k(a,b) = \alpha_1^k + \alpha_2^k + \alpha_3^k, \quad \forall \ \ k \in \mathbb{Z}_+. \tag{3.2}$$

Observe que $s_0 = 3$, $s_1 = a$, $s_2 = a^2 - 2b$ e

$$s_3 = as_2 - bs_1 + s_0.$$

Em geral, temos a sequência recorrente linear em $\mathbb{F}$:

$$s_{k+3} = s_{k+3}(a,b) = as_{k+2} - bs_{k+1} + s_k, \quad \forall \ \ k \in \mathbb{Z}_+. \tag{3.3}$$

Os termos $s_0$, $s_1$ e $s_2$ chamam-se *valores iniciais*. A sequência $s = (s_k)_{k\in\mathbb{Z}_+}$ chama-se *sequência característica gerada* por $f(x)$. É importante lembrar que os termos da sequência

$$s = (s_0, s_1, s_2, \ldots, s_k, \ldots)$$

são lidos módulo $p$. Além disso, é fácil verificar que o conjunto das sequências que satisfazem a equação de recorrência (3.3) é um espaço vetorial sobre $\mathbb{F}$ de dimensão 3.

Note que a equação de recorrência (3.3) pode ser posta na forma matricial

$$\begin{aligned} S_{k+1} &= \begin{bmatrix} s_{k+1} & s_{k+2} & s_{k+3} \end{bmatrix} \\ &= \begin{bmatrix} 0s_k + s_{k+1} + 0s_{k+2} & 0s_k + 0s_{k+1} + s_{k+2} & s_k - bs_{k+1} + as_{k+2} \end{bmatrix} \\ &= \begin{bmatrix} s_k & s_{k+1} & s_{k+2} \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -b \\ 0 & 1 & a \end{bmatrix} \\ &= S_k A, \end{aligned}$$

para todo $k \in \mathbb{Z}_+$, com valor inicial

$$S_0 = \begin{bmatrix} s_0 & s_1 & s_2 \end{bmatrix} = \begin{bmatrix} 3 & a & a^2 - 3b \end{bmatrix}.$$

Portanto, indutivamente, obtemos

$$S_{k+1} = S_0 A^k, \ \ \forall \ \ k \in \mathbb{Z}_+.$$

Como $\det(A) = 1$, temos que $A$ é um elemento do *grupo linear geral*

$$GL(3, \mathbb{F}) = \{A \in M(3, \mathbb{F}) : \det(A) \neq 0\}$$

de ordem

$$p^3(p-1)(p^2-1)(p^3-1).$$

Neste caso,

$$A^{-1} = \begin{bmatrix} b & 1 & 0 \\ -a & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \in GL(3, \mathbb{F})$$

é a matriz companheira do polinômio

$$f^{\perp}(x) = -x^3 f\left(\frac{1}{x}\right) = x^3 - bx^2 + ax - 1$$

(recíproco de $f(x)$). Observe que se $\alpha \in \mathbb{L}$ é uma raiz de $f(x)$, então

$$\alpha^3 - a\alpha^2 + b\alpha - 1 = 0 \Leftrightarrow -\alpha^3\left(\left(\frac{1}{\alpha}\right)^3 - b\left(\frac{1}{\alpha}\right)^2 + a\left(\frac{1}{\alpha}\right) - 1\right) = 0.$$

Assim, $\alpha^{-1}$ é uma raiz de $f^{\perp}(x)$. Como $\alpha_1\alpha_2 = \alpha_3^{-1}$, $\alpha_1\alpha_3 = \alpha_2^{-1}$ e $\alpha_2\alpha_3 = \alpha_1^{-1}$, temos:

$$\begin{aligned} s_{-1} &= b \\ s_{-2} &= b^2 - 2a \\ s_{-3} &= bs_{-2} - as_{-1} + s_0. \end{aligned}$$

De modo análogo acima, obtemos:

$$s_{-k} = s_{-k}(a,b) = \alpha_1^{-k} + \alpha_2^{-k} + \alpha_3^{-k}, \ \forall \ k \in \mathbb{Z}_+.$$

Em geral, temos a sequência recorrente linear em $\mathbb{F}$:

$$s_{-(k+3)} = s_{-(k+3)}(b,a) = bs_{-(k+2)} - as_{-(k+1)} + s_{-k}, \ \forall \ k \in \mathbb{Z}_+.$$

Seja $\boldsymbol{s} = (s_k)_{k\in\mathbb{Z}_+}$ uma sequencia recorrente linear em $\mathbb{F}$. Diremos que $\boldsymbol{s}$ é *periódica* se existir um inteiro $r > 0$ tal que

$$s_{k+r} = s_k, \ \forall \ k \in \mathbb{Z}_+.$$

O menor inteiro que satisfaz esta condição chama-se o *período* e será denotado por $per(\boldsymbol{s})$.

Por exemplo, se $p = 5$ e $\boldsymbol{s} = (s_k)_{k\in\mathbb{Z}_+}$ é uma sequência recorrente linear em $\mathbb{F}$ que satisfaz a equação de recorrência

$$s_{k+3} = 3s_{k+2} - 2s_{k+1} + s_k, \ \forall \ k \in \mathbb{Z}_+,$$

com polinômio característico

$$f(x) = x^3 - 3x^2 + 2x - 1 \in \mathbb{Z}_5[x],$$

então:

$$\boldsymbol{s} = (s_k)_{k\in\mathbb{Z}_+} = (3,3,0,2,4,3,3,2,3,3,0,2,4,3,3,2,\ldots).$$

Portanto, $\boldsymbol{s} = (s_k)_{k\in\mathbb{Z}_+}$ é periódica de $per(\boldsymbol{s}) = 8$. Note que $per(\boldsymbol{s}) = ord(f)$.

**Teorema 4:** *Sejam $\boldsymbol{s} = (s_k)_{k\in\mathbb{Z}_+}$ uma sequência recorrente linear em $\mathbb{F}$ que satisfaz a equação de recorrência* (3.3)*, $f(x)$ seu polinômio característico e $\boldsymbol{A}$ a matriz companheira de $f(x)$.*

1. *$ord(f)$ é igual a ordem de $\boldsymbol{A}$ no grupo $GL(3,\mathbb{F})$. Em particular, $ord(f) = ord(f^{\perp})$.*
2. *$\boldsymbol{s}$ é uma sequência periódica. Em particular, $per(\boldsymbol{s}) \leq p^3 - 1$.*
3. *O período $per(\boldsymbol{s})$ divide $ord(f)$.*
4. *Se $f(x)$ é irredutível sobre sobre $\mathbb{F}$, então $ord(f) = per(\boldsymbol{s})$. Em particular, $ord(f)$ divide $p^3 - 1$.*

Sejam $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{L}$ as raízes distintas de $f(x)$ e

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -b \\ 0 & 1 & a \end{bmatrix}.$$

sua matriz companheira. Então é fácil verificar que $A^k$ é a matriz companheira do polinômio

$$f_k(x) = (x - \alpha_1^k)(x - \alpha_2^k)(x - \alpha_3^k)$$

Como

$$(x - \alpha_1^k)(x - \alpha_2^k)(x - \alpha_3^k) = x^3 - \sum_{i=1} \alpha_i^k x^2 + \sum_{1\leq i<j\leq 3} (\alpha_i \alpha_j)^k x - (\alpha_1\alpha_2\alpha_3)^k,$$

$\alpha_1\alpha_2\alpha_3 = 1$, $\alpha_1\alpha_2 = \alpha_3^{-1}$, $\alpha_1\alpha_3 = \alpha_2^{-1}$ e $\alpha_2\alpha_3 = \alpha_1^{-1}$ temos que

$$f_k(x) = x^3 - s_k(a,b)\,x^2 + s_{-k}(a,b)\,x - 1.$$

**Lema 1:** *Sejam $s = (s_k)_{k\in\mathbb{Z}_+}$ uma sequência recorrente linear em $\mathbb{F}$ que satisfaz a equação de recorrência* (3.3)*, $f(x)$ seu polinômio característico e $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{L}$ as raízes distintas de $f(x)$. Então*:

1. *$t = ord(f) = ord(f_k)$ se, e somente se, $mdc(t,k) = 1$.*

2. *Se $mdc(t,k) = 1$, então $f(x)$ é irredutível sobre $\mathbb{F}$ se, e somente se, $f_k(x)$ é irredutível sobre $\mathbb{F}$.*

**Prova**. Basta provar o item (1). A ordem de $A$ e $A^k$ são iguais a $t$ no grupo $GL(3,\mathbb{F})$ se, e somente se, $mdc(t,k) = 1$. ■

**Teorema 5:** *Sejam $s = (s_k)_{k\in\mathbb{Z}_+}$ uma sequência recorrente linear em $\mathbb{F}$ que satisfaz a equação de recorrência* (3.3)*, $f(x)$ seu polinômio característico e $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{L}$ as raízes distintas de $f(x)$. Então*

$$s_k\big(s_l(a,b), s_{-l}(a,b)\big) = s_{kl}(a,b), \quad \forall \ \ k,l \in \mathbb{Z}_+.$$

**Prova**. Como

$$\begin{aligned} f_l(x) &= \left(x-\alpha_1^l\right)\left(x-\alpha_2^l\right)\left(x-\alpha_3^l\right) \\ &= x^3 - s_l(a,b)\,x^2 + s_{-l}(a,b)\,x - 1 \end{aligned}$$

temos que

$$\begin{aligned} s_k(s_l(a,b), s_{-l}(a,b)) &= \left(\alpha_1^l\right)^k + \left(\alpha_2^l\right)^k + \left(\alpha_3^l\right)^k \\ &= \alpha_1^{lk} + \alpha_2^{lk} + \alpha_3^{lk} \\ &= s_{kl}(a,b), \end{aligned}$$

que é o resultado desejado. ■

Note que para cada $k$ fixado e quaisquer $u, v \in \mathbb{F}$, pode ser provado (cf. [1, Theorem 7.46]) que o sistema

$$\begin{cases} s_k(a,b) = u \\ s_{-k}(a,b) = v \end{cases} \tag{3.4}$$

possui uma única solução $(a,b) \in \mathbb{F} \times \mathbb{F}$ se, e somente se,

$$mdc(k, p^i - 1) = 1, \quad i = 1,2,3,$$

ou seja, $s_k(a,b)$ e $s_{-k}(a,b)$ são ortogonais.

O próximo resultado, devido a Gong e Harn (cf. [4,Lemma 3]), fornece um algoritmo para calcular o $k$-ésimo termo de uma sequência recorrente em $\mathbb{F}$ que satisfaz a equação de recorrência (3.3).

**Teorema 6:** *Sejam $\mathbf{s} = (s_k)_{k \in \mathbb{Z}_+}$ uma sequência recorrente linear em $\mathbb{F}$ que satisfaz a equação de recorrência* (3.3)*, $f(x)$ seu polinômio característico e $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{L}$ as raízes distintas de $f(x)$. Então*:

1. $s_{2k} = s_k^2 - 2s_{-k}$, *para todo* $k \in \mathbb{Z}_+$.
2. $s_m s_k - s_{m-k} s_{-k} = s_{m+k} - s_{m-2k}$, *para todos* $k, m \in \mathbb{Z}_+$, *com* $m \neq k$.

Vamos finalizar esta seção com relações explícitas entre o período e a ordem da sequência característica $\mathbf{s} = (s_k)_{k \in \mathbb{Z}_+}$ gerada pelo polinômio

$$f(x) = x^3 - ax^2 + bx - 1 \in \mathbb{F}[x].$$

Então, pelo Teorema 2, há três casos a serem considerados:

1.º **Caso**. $f$ é redutível sobre $\mathbb{F}$ se, e somente se,

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

em que $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$. Como $x - \alpha$ é irredutível sobre $\mathbb{F}$ temos, pelo item (1) do Teorema 1, que $ord(x - \alpha)$ é igual a ordem de $\alpha$ em $\mathbb{F}^*$, ou seja, $ord(x - \alpha)$ divide

$p-1$. Assim, pelo item (3) do Teorema 1, $ord(f)$ divide $p-1$. Portanto, pelo item (3) do Teorema 4, $f$ é redutível sobre $\mathbb{F}$ se, e somente se,

$$per(s) \mid p-1.$$

2.º **Caso**. $f$ é redutível sobre $\mathbb{F}$ se, e somente se,

$$f(x) = (x-\alpha)g(x),$$

em que $\alpha \in \mathbb{F}$ e $g(x)$ é irredutível sobre $\mathbb{F}$. Como $g(x)$ é irredutível sobre $\mathbb{F}$ temos, pelo item (1) do Teorema 1, que $ord(g)$ é igual a ordem de qualquer raiz em $\mathbb{F}^*_{p^2}$, ou seja, $ord(g)$ divide $p^2-1$, mas não divide $p-1$. Assim, pelo item (3) do Teorema 1, $ord(f)$ divide $p^2-1$. Portanto, pelo item (3) do Teorema 4, $f$ é redutível sobre $\mathbb{F}$ se, e somente se,

$$per(s) \mid p^2-1 \text{ e } per(s) \nmid p-1.$$

3.º **Caso**. Se $f$ é irredutível sobre $\mathbb{F}$, então, pelo item (1) do Teorema 1, $ord(g)$ é igual a ordem de qualquer raiz em $\mathbb{F}^*_{p^3}$, ou seja, $ord(g)$ divide $p^3-1$, mas não divide $p-1$. Portanto, pelo item (3) do Teorema 4, $f$ é irredutível sobre $\mathbb{F}$ se, e somente se,

$$per(s) \mid p^2+p+1.$$

## 4 Sistema de codificação do tipo RSA

Nesta seção apresentaremos um criptossistema com chave pública do tipo *RSA* baseado em um par de sequências recorrentes de ordem 3 sobre o anel finito $\mathbb{Z}_n$, em que $n = pq$ é um produto de número primos distintos:

$$s_{k+3} = as_{k+2} - bs_{k+1} + s_k, \ \ \forall \ \ k \in \mathbb{Z}_+,$$

com polinômio característico

$$f(x) = x^3 - ax^2 + bx - 1.$$

O leitor interessado em mais detalhes sobre outros sistemas de criptografias com chave pública pode consultar [4, 5].

Os criptossistemas com chave pública são projetados como segue. Dados um conjunto de *chaves* $\mathscr{K}$, um conjunto de *transformações de codificações* ou *cifragens* $\{f_e : e \in \mathscr{K}\}$ e um conjunto de *transformações de decodificações* ou *decifragens* $\{f_d : d \in \mathscr{K}\}$. Então qualquer par $(f_e, f_d)$ possui a seguinte propriedade: dado aleatoriamente um texto cifrado $\boldsymbol{c} \in \mathscr{C}$ é possível calcular a mensagem ou texto original $\boldsymbol{u} \in \mathscr{M}$ tal que $f_e(\boldsymbol{u}) = c$. Neste caso,

$$f_e : \mathscr{M} \to \mathscr{C} \text{ tal que } f_e(\boldsymbol{u}) = \boldsymbol{c}$$

é o processo de codificação e

$$f_d : \mathscr{C} \to \mathscr{M} \text{ tal que } f_d(\boldsymbol{c}) = \boldsymbol{u}$$

é o processo de decodificação. Um *cripossistema* é qualquer bijeção de $\mathscr{M}$ sobre $\mathscr{C}$. Com estas hipóteses, consideremos a comunicação entre dois usuários $A$ (Alice) e $B$ (Bob). Bob seleciona um par de chaves $(e, d)$ e envia a chave de codificação $e$ para Alice através de qualquer canal de comunicação (por exemplo, internet), mas mantém secreto a chave de decodificação $d$. Alice pode enviar uma mensagem $\boldsymbol{u}$ para Bob aplicando o processo de codificação determinado pela chave pública de Bob para obter $f_e(\boldsymbol{u}) = \boldsymbol{c}$. Bob decodifica o texto cifrado $\boldsymbol{c}$ aplicando o processo de decodificação $f_d$ unicamente determinado por $d$.

Vamos descrever com mais detalhes o processo acima. Os elementos de $\mathscr{M}$ são chamados de *textos originais* e os elementos de $\mathscr{C}$ são chamados de *textos cifrados*, ambos são escritos em algum alfabeto $\mathbb{A}$, consistindo de um certo número $N$ de símbolos. Assim, é útil substituir os símbolos do alfabeto $\mathbb{A}$ por números inteiros $0, 1, 2, \ldots$, para tornar mais fácil a construção do criptossistema $f$. Uma correspondência natural entre o alfabeto

$$\mathbb{A} = \{A, B, C, \ldots, K, \ldots, X, Y, Z, \text{ espaço} = \sqcup\}$$

e o conjunto de números inteiros

$$\mathbb{Z}_{27} = \{0, 1, 2, \ldots, 10, \ldots, 23, 24, 25, 26\}$$

é dada pela tabela:

$$\begin{array}{cccccccccc} A & B & C & \cdots & K & \cdots & X & Y & Z & \sqcup \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \cdots & 10 & \cdots & 23 & 24 & 25 & 26. \end{array} \tag{4.5}$$

Em geral, podemos rotular mensagens unitárias, com blocos de $k$ símbolos, de um alfabeto $\mathbb{A}$ de $N$ símbolos, por inteiros do conjunto

$$\mathbb{Z}_{N^k} = \{0, 1, \ldots, N^k - 1\}$$

do seguinte modo:

$$(x_{k-1}, \ldots, x_1, x_0) \in \mathbb{Z}_N^k \leftrightarrow x_{k-1}N^{k-1} + \cdots + x_1 N + x_0 N^0 \in \mathbb{Z}_{N^k},$$

em que cada $x_i$ corresponde a um símbolo do alfabeto $\mathbb{A}$. Por exemplo, a mensagem unitária com bloco de cinco símbolos

$$RECEN$$

corresponde ao inteiro

$$17 \cdot 27^4 + 4 \cdot 27^3 + 2 \cdot 27^2 + 4 \cdot 27 + 13 \cdot 27^0 = 9.114.808 \in \mathbb{Z}_{27^5}.$$

Descrição do método de criptografar: Cada usuário segue os seguintes passos:

1.$^o$ **Passo**. Escolhe aleatoriamente dois números primos grandes $p$, $q$ e aleatoriamente um número $e$ tal que

$$mdc(e, p^i - 1) = mdc(e, q^i - 1) = 1, \quad i = 1, 2, 3.$$

2.º **Passo**. Torna público a chave de codificação

$$k_e = (n, e)$$

e mantém secreta a chave de decodificação

$$k_d = (n, d_j), \quad j \in \{1,2,3,4,5,6,7,9\},$$

em que $n = pq$ e os $d_j$ são dados na tabela 1, devido a Gong e Harn (cf. [4, Table I]).

**Processos de codificação e decodificação**:

Cada usuário poderá enviar uma mensagem para outro usuário via o processo de codificação

$$f_e : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$$

definido como

$$f_e(\boldsymbol{u}) = f_e(u_1, u_2) = (s_e(u_1, u_2), s_{-e}(u_1, u_2)) = (c_1, c_2) = c.$$

Note, pelo sistema 3.4 e o Teorema Chinês dos Restos, que $f_e$ é uma função bijetora.

O processo de decodificação é composto de algumas etapas.

1.º **Etapa**. Cada usuário calcula (módulo $m \in \{p, q\}$)

$$\begin{aligned} C(c_1, c_2) &= 3^{-1}c_1^2 + c_2 \\ D(c_1, c_2) &= -2 \cdot 3^{-3}c_1^3 + 3^{-1}c_1c_2 - 1 \\ \Delta(c_1, c_2) &= -4C^3(c_1, c_2) - 27D^2(c_1, c_2) \end{aligned}$$

2.º **Etapa**. Calcula

$$\gamma(c_1, c_2) = \left( \frac{-27D(c_1, c_2) + \sqrt{-27\Delta(c_1, c_2)}}{-27D(c_1, c_2) - \sqrt{-27\Delta(c_1, c_2)}} \right)^{2k},$$

em que

$$k \in \left\{ \frac{m-1}{6}, \frac{m+1}{6} \right\} \quad \text{e} \quad m \in \{p, q\}.$$

3.$^o$ **Etapa**. Cada usuário escolhe a chave de decodificação apropriada

$$k_{d,i} = (n, d_j), \quad j \in \{1,2,3,4,5,6,7,9\},$$

em que os $d_j$ são dados na tabela 1 e calcula (módulo $n$)

$$u_1 = s_{d_j}(c_1, c_2) \text{ e } u_2 = s_{-d_j}(c_1, c_2).$$

Para as etapas acima precisamos das seguintes informações:

Primeiro como os polinômios

$$x^3 - u_1 x^2 + u_2 x - 1 \text{ e } x^3 - c_1 x^2 + c_2 x - 1$$

possuem a mesma ordem temos que cada usuário poderá selecionar uma chave de decodificação

$$k_{d_j} = (n, d_j)$$

apropriada, de acordo com o polinômio construído pelo texto cifrado

$$\boldsymbol{c} = (c_1, c_2).$$

Segundo vamos definir a função lógica

$$\Gamma(j, m), \text{ onde } j \in \{1,2,3\} \text{ e } m \in \{p, q\}.$$

Neste caso, precisamos do *símbolo de Legendre*

$$\left(\frac{a}{m}\right) = \begin{cases} 1, & \text{se } a \text{ é resíduo quadrado módulo } m \\ -1, & \text{caso contrário} \end{cases}$$

(a) $\Gamma(1, m)$ é verdade se, e somente se,

$$\Delta(c_1, c_2) \equiv 0 \ (mod\, m)$$

| Condição | Multiplicador do Período | Chave de Decodificação |
|---|---|---|
| $\Gamma(1,p)\wedge\Gamma(1,q)$ | $\delta_1 = R_{1,p}\cdot R_{1,q}$ | $d_1 e \equiv 1\ (mod\,\delta_1)$ |
| $\Gamma(1,p)\wedge\Gamma(2,q)$ | $\delta_2 = R_{1,p}\cdot R_{2,q}$ | $d_2 e \equiv 1\ (mod\,\delta_2)$ |
| $\Gamma(1,p)\wedge\Gamma(3,q)$ | $\delta_3 = R_{1,p}\cdot R_{3,q}$ | $d_3 e \equiv 1\ (mod\,\delta_3)$ |
| $\Gamma(2,p)\wedge\Gamma(1,q)$ | $\delta_4 = R_{2,p}\cdot R_{1,q}$ | $d_4 e \equiv 1\ (mod\,\delta_4)$ |
| $\Gamma(2,p)\wedge\Gamma(2,q)$ | $\delta_5 = R_{2,p}\cdot R_{2,q}$ | $d_5 e \equiv 1\ (mod\,\delta_5)$ |
| $\Gamma(2,p)\wedge\Gamma(3,q)$ | $\delta_6 = R_{2,p}\cdot R_{3,q}$ | $d_6 e \equiv 1\ (mod\,\delta_6)$ |
| $\Gamma(3,p)\wedge\Gamma(1,q)$ | $\delta_7 = R_{3,p}\cdot R_{1,q}$ | $d_7 e \equiv 1\ (mod\,\delta_7)$ |
| $\Gamma(3,p)\wedge\Gamma(2,q)$ | $\delta_8 = R_{3,p}\cdot R_{2,q}$ | $d_8 e \equiv 1\ (mod\,\delta_8)$ |
| $\Gamma(3,p)\wedge\Gamma(3,q)$ | $\delta_9 = R_{3,p}\cdot R_{3,q}$ | $d_9 e \equiv 1\ (mod\,\delta_9)$ |

*Tabela 1. Chaves de Decodificação*

ou

$$\Delta(c_1,c_2)\not\equiv 0\ (mod\,m),\ \left(\frac{\Delta(c_1,c_2)}{m}\right)=1\ \text{ e }\ \gamma(c_1,c_2)\equiv 1\ (mod\,m)$$

se, e somente se, $f$ é redutível sobre $\mathbb{Z}_m$ (1.º **Caso**).

(b) $\Gamma(2,m)$ é verdade se, e somente se,

$$\Delta(c_1,c_2)\not\equiv 0\ (mod\,m)\ \text{ e }\ \left(\frac{\Delta(c_1,c_2)}{m}\right)=-1$$

se, e somente se, $f$ é redutível sobre $\mathbb{Z}_m$ (2.º **Caso**).

(c) $\Gamma(3,m)$ é verdade se, e somente se,

$$\Delta(c_1,c_2)\not\equiv 0\ (mod\,m),\left(\frac{\Delta(c_1,c_2)}{m}\right)=1\ \text{ e }\ \gamma(c_1,c_2)\not\equiv 1\ (mod\,m)$$

se, e somente se, $f$ é irredutível sobre $\mathbb{Z}_m$ (3.º **Caso**).

Vamos denotar os períodos de cada caso por

$$R_{1,m}=m-1,\ \ R_{2,m}=m^2-1\ \text{ e }\ R_{3,m}=m^2+m+1.$$

Então, obtemos a tabela 1.

Vamos finalizar esta seção com um exemplo simples. Sejam $p = 5$, $q = 7$, $n = pq = 35$ e $e = 5$ escolhido convenientemente. Então para codificar o texto original **AMOR**, dividimos em blocos de dois símbolos, com correspondência numérica

$$\begin{array}{cc} AM & OR \\ \updownarrow & \updownarrow \\ 12 & 395 \end{array}$$

Logo,

$$\boldsymbol{u} = (u_1, u_2) = (12, 10),$$

onde

$$\begin{aligned} u_1 &= 12 \equiv 0 \cdot 27 + 12 \ (mod 35) \\ u_2 &= 10 \equiv 14 \cdot 27 + 17 \ (mod 35). \end{aligned}$$

O usuário $A$, com chave de codificação

$$k_e = (n, e) = (35, 5),$$

calcula

$$\begin{aligned} s_0(12,10) &= 3, \ \ s_1(12,10) = 12, \ \ s_2(12,10) = 19 \\ s_3(12,10) &= 6, \ \ s_4(12,10) = 34, \ \ s_5(12,10) = 17 \end{aligned}$$

e

$$\begin{aligned} s_0(12,10) &= 3, \ \ s_{-1}(12,10) = 10, \ \ s_{-2}(12,10) = 6 \\ s_{-3}(12,10) &= 13, \ \ s_{-4}(12,10) = 33, \ \ s_{-5}(12,10) = 5. \end{aligned}$$

Assim,

$$c_1 = s_5(12,10) = 17 \ \text{ e } \ c_2 = s_{-5}(12,10) = 5.$$

Logo, o texto cifrado é o par

$$\boldsymbol{c} = (c_1, c_2) = (17, 5)$$

onde

$$\begin{aligned} c_1 &= 17 \equiv 0 \cdot 27 + 17 \ (mod 35) \\ c_2 &= 5 \equiv 0 \cdot 27 + 5 \ (mod 35). \end{aligned}$$

Portanto, o usuário $A$ envia para o usuário $B$, o texto cifrado **ARAF**.

Após recuperar $\boldsymbol{c} = (17, 5)$, como obter a chave de decodificação? Para $p = 5$ e

$$\begin{aligned} f(x) &= x^3 - 17x^2 + 5x - 1 \\ &\equiv x^3 - 2x^2 + 0x - 1 \in \mathbb{Z}_5[x], \end{aligned}$$

o usuário $B$ calcula

$$C(2,0) = 3, \ \ D(2,0) = 1 \ \text{ e } \ \Delta(2,0) = 0.$$

Como $\Delta(2,0) = 0$ temos a função lógica $\Gamma(1,5)$. Do mesmo modo, para $q = 7$ e

$$\begin{aligned} f(x) &= x^3 - 17x^2 + 5x - 1 \\ &\equiv x^3 - 3x^2 + 5x - 1 \in \mathbb{Z}_7[x], \end{aligned}$$

o usuário $B$ calcula

$$C(3,5) = 1, \ \ D(3,5) = 2 \ \text{ e } \ \Delta(3,5) = 0.$$

Como $\Delta(3,5) = 0$ temos a função lógica $\Gamma(1,7)$. Assim, de acordo com a tabela 1, obtemos a condição

$$\Gamma(1,5) \wedge \Gamma(1,7)$$

e o multiplicador do período

$$\delta_1 = R_{1,5} \cdot R_{1,7} = 4 \cdot 6 = 24.$$

Finalmente, como

$$d_1 \cdot 5 \equiv 1 \ (mod 24)$$

temos que $d_1 = 5$.

Agora, com a chave de decodificação

$$k_{d_1} = (35, 5),$$

o usuário $B$ calcula

$$u_1 = s_5(17,5) = 12 \ \text{ e } \ u_2 = s_{-5}(17,5) = 10$$

e recupera a mensagem original

$$\boldsymbol{u} = (u_1, u_2) = (12, 10).$$

Portanto, o texto original é **AMOR**.

Obseve que a segurança deste sistema está baseado na dificuldade de fatorar um número inteiro composto muito grande, estima-se que para fatorar um número de 500 dígitos exige aproximadamente $10^{25}$ anos.

## Referências

[1] LIDL, R.; NIEDERREITER, H., Finite Fields. in Encyclopedia of Mathematics and Its Applications, vol. 20, 1983

[2] RÉDEI, L., Algebra. U.K.: Pergamon, London, 1967.

[3] CAVALCANTI, A. C. F., Cripto-Sistemas com Chave Pública Baseado em Extensões Cúbicas. Dissertação de Mestrado, UFPB, 2002.

[4] GONG, G.; HARN, L. Public-Key Cryptosystems Based on Cubic Finite Field Extentions, *IEEE Trans Infor Theory*, vol IT-45, pp 2601 — 2605, 1999.

[5] KOBLITZ, N., A Course in Number Theory and Cryptography. Springer, New York, 1994.