José Laudelino de Menezes Neto

PRIMEIROS PASSOS EM CRIPTOGRAFIA

Editora UFPB

PRIMEIROS PASSOS EM CRIPTOGRAFIA

José Laudelino de Menezes Neto

PRIMEIROS PASSOS EM CRIPTOGRAFIA

Editora UFPB
João Pessoa
2021

Projeto Gráfico Editora UFPB
Revisão Gráfica Alice Brito
Editoração Eletrônica Alexandre Câmara
Design de Capa Alexandre Câmara

Catalogação na fonte:
Biblioteca Central da Universidade Federal da Paraíba

M543p Menezes Neto, José Laudelino de.
Primeiros passos em criptografia [recurso eletrônico] / José Laudelino de Menezes Neto. - João Pessoa : Editora UFPB, 2021.

E-book
Modo de acesso: http://www.editora.ufpb.br/sistema/press/
ISBN 978-65-5942-143-5

1. Criptografia. 2. Função afim. 3. Matemática. I. Título.

UFPB/BC CDU 003.26

Livro aprovado para publicação através do Edital Nº 01/2020/Editora Universitária/ UFPB – Programa de Publicação de E-books.

EDITORA UFPB
Cidade Universitária, Campus I
Prédio da Editora Universitária, s/n
João Pessoa – PB
CEP 58.051-970
http://www.editora.ufpb.br
E-mail: editora@ufpb.br
Fone: (83) 3216.7147

SUMÁRIO

APRESENTAÇÃO

Este livro tem como objetivo iniciar o leitor nos seus primeiros passos rumo ao caminho da criptografia, ensinando um método simples para criptografar utilizando uma função afim.

José Laudelino de Menezes Neto

INTRODUÇÃO

A criptografia é a arte de cifrar, codificar, mensagens de forma que o texto fique incompreensível para leitores não autorizados. Apenas leitores autorizados terão acesso ao teor original da mensagem.

Desde tempos remotos a criptografia é utilizada. O imperador Júlio César utilizou um tipo de criptografia, conhecida por cifra de César, para proteger suas mensagens de leitores não autorizados [3].

Durante a segunda guerra mundial, de 1939 a 1945, os alemães utilizaram a Máquina Enigma [3] para cifrar suas mensagens e esconder suas táticas de guerra. A luta para quebrar este método criptográfico é retratada no filme *O jogo da imitação* [5], que conta a história de Alan Turing, um dos responsáveis por decifrar a Máquina Enigma.

Nos dias atuais, a criptografia se encontra em evidência, pois está presente para proteger as transações bancárias; na proteção de banco de dados online que armazenam senhas, fotos etc; os aplicativos de mensagens como *WhatsApp*, *Telegram* e *Wickr Me* utilizam métodos criptográficos para codificar a comunicação dos seus usuários, evitando que terceiros tenham acesso ao conteúdo das mensagens.

Vale ressaltar que a criptografia também é importante para proteger a segurança nacional de um país, na transmissão de mensagens sensíveis e que não devem se tornar públicas. Faz-se notar também que produzir um método criptográfico próprio é de suma importância, dado que comprar criptografia de terceiros pode ser um fator não confiável, como foi o caso descoberto de que a CIA vendia métodos criptográficos para terceiros com o intuito de decifrar estas informações, pois o método criptográfico fornecido era de baixa segurança [4].

Existem vários livros teóricos sobre criptografia [1-3,6], entretanto neste livro, temos por objetivo deixar o material accessível, sem nos aprofundar muito nas teorias matemáticas, e apresentar um método clássico de criptografia simples, utilizando uma função afim, de grau um, de forma que o leitor entenda o básico de como criptografar e descriptografar uma mensagem. Ao término do livro, esperamos ter aberto um caminho para que o leitor entenda métodos mais elaborados de criptografia, como a criptografia RSA [1-3,6], ou a criptografia de curvas elípticas [2], e também se interesse em estudar mais a fundo as teorias matemáticas envolvidas.

Os pré-requisitos para compreender os conteúdos abordados são assuntos vistos em cursos iniciais da graduação nas ciências exatas, ou nas áreas de tecnologia e

engenharias. Faz-se necessário um conhecimento das operações básicas de soma, subtração, multiplicação e divisão; estar familiarizado com Teoria dos Conjuntos, conhecer os conjuntos numéricos dos inteiros, $\mathbb{Z}$, e reais, $\mathbb{R}$; saber lidar com uma função afim, também chamada de função de grau um, do tipo $f(x) = ax + b$; compreender os conceitos de função inversa, comumente denotada por $f^{-1}(x)$; e ter estudado Máximo Divisor Comum (MDC).

O livro está estruturado do seguinte modo:

1. explicação da escolha de um alfabeto, conjunto de caracteres utilizados para escrever as mensagens;
2. método de criptografia utilizando uma função afim definida em $\mathbb{R}$;
3. para incrementar a criptografia, apresentamos um tipo de conjunto essencial, o conjunto $\mathbb{Z}_n$;
4. lidamos com operações de soma e multiplicação em $\mathbb{Z}_n$;
5. estudamos um método de cálculo de Máximo Divisor Comum (MDC);
6. apresentamos uma metodologia para calcular o inverso multiplicativo de um número em $\mathbb{Z}_n$;

7. exibimos o conteúdo principal do livro, um método de criptografia utilizando uma função afim definida em $\mathbb{Z}_n$.

ALFABETO (CONJUNTO DE CARACTERES)

Para iniciar na criptografia, definimos o alfabeto, conjunto de caracteres que utilizaremos. Em princípio, utilizaremos apenas as letras maiúsculas

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z

Estamos utilizando um conjunto composto de 26 caracteres.

No último tópico deste livro, veremos como adicionar mais caracteres, por exemplo, espaço em branco, caracteres de pontuação (! ? . , ; : etc.), números (0 1 2 3 4 5 6 7 8 9), letras minúsculas (a b c d e ... x y z) e caracteres especiais ($ & = # % + - etc.).

Devemos associar cada letra, caractere, com um número. Como temos 26 caracteres, A, B, C, ..., Z, iremos associar com os números de 0 a 25

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25

A associação de um caractere com um número pode ser feita de qualquer maneira. Aqui, optamos por associar de modo

crescente. Caractere A se associa com o 0, em símbolos, A↔0; caractere B se associa com o 1, B↔1; caractere C se associa com o 2, B↔2; e assim sucessivamente.

A↔0; B↔1; C↔2; D↔3; E↔4; F↔5; G↔6; H↔7; I↔8; J↔9; K↔10; L↔11; M↔12; N↔13; O↔14; P↔15; Q↔16; R↔17; S↔18; T↔19; U↔20; V↔21; W↔22; X↔23; Y↔24; Z↔25.

CRIPTOGRAFANDO COM UMA FUNÇÃO AFIM REAL

Definido nosso conjunto de caracteres, devemos escolher o método de criptografia de mensagem. O essencial é que este método de criptografia, tenha um caminho de ida, criptografa a mensagem num texto incompreensível (cifrado), e volta, descriptografa a mensagem cifrada, recuperando o texto original, compreensível.

Mensagem	$\rightarrow$	Mensagem
original	$\leftarrow$	cifrada

O método criptográfico que utilizaremos será através de uma função afim real, de grau 1, da forma

$$f:\mathbb{R}\rightarrow\mathbb{R}, f(x) = ax + b, a \neq 0.$$

A função $f(x) = ax + b$ é a responsável por fazer esta ponte entre mensagem original e mensagem cifrada, portanto esta função deverá ser inversível, ou seja, possuir uma função inversa $f^{-1}(x) = cx + d$.

Como escolhemos uma função definida nos números reais, $\mathbb{R}$, $f(x) = ax + b$, com $a \neq 0$, para determinar a função inversa, $f^{-1}(x) = cx + d$, utilizamos

$$c = \frac{x}{a},\ d = -\frac{b}{a}.$$

o que nos leva a

$$f^{-1}(x) = \frac{x}{a} - \frac{b}{a}.$$

CRIPTOGRAFANDO NOSSA PRIMEIRA MENSAGEM

Vamos criptografar a mensagem **BOLA**, utilizando a função $f(x) = 2x + 6$. Fazemos a associação de cada letra (caractere) com o seu respectivo número

B↔1, O↔14, L↔11, A↔0

Aplicamos a função $f(x) = 2x + 6$ em cada valor numérico.

$$f(1) = 2 \cdot 1 + 6 = 8,$$

$$f(14) = 2 \cdot 14 + 6 = 34,$$

$$f(11) = 2 \cdot 11 + 6 = 28,$$

$$f(0) = 2 \cdot 0 + 6 = 6.$$

A partir da mensagem original **BOLA**, utilizando a função $f(x) = 2x + 6$ para criptografar e obtemos o texto cifrado, criptografado,

$$8 \;\; 34 \;\; 28 \;\; 6.$$

Para recuperar o texto original da mensagem cifrada, sabendo que foi criptografado com a função $f(x) = 2x + 6$, basta utilizarmos a função inversa, obtida através da fórmula mencionada previamente, dada por

$$f^{-1}(x) = \frac{x}{2} - \frac{6}{2} \Longrightarrow f^{-1}(x) = \frac{x}{2} - 3.$$

Aplicamos a mensagem cifrada $8 \;\; 34 \;\; 28 \;\; 6$ na função inversa

$$f^{-1}(8) = \frac{8}{2} - 3 = 4 - 3 = 1,$$

$$f^{-1}(34) = \frac{34}{2} - 3 = 17 - 3 = 14,$$

$$f^{-1}(28) = \frac{28}{2} - 3 = 14 - 3 = 11,$$

$$f^{-1}(6) = \frac{6}{2} - 3 = 3 - 3 = 0.$$

Observamos que $f^{-1}(8) = 1$ e 1↔B; $f^{-1}(34) = 14$ e 14↔O; $f^{-1}(28) = 11$ e 11↔L; $f^{-1}(6) = 0$ e 0↔A.

Logo, recuperamos a mensagem original **BOLA**.

DESCRIPTOGRAFANDO UMA MENSAGEM CIFRADA

Sabendo que a mensagem cifrada $60\ 5\ 126\ 203\ 159$ foi criptografada usando a função afim real $f(x) = 11x + 5$, vamos recuperar a mensagem original.

Sabemos que a mensagem cifrada foi criptografada com a função $f(x) = 11x + 5$, então para recuperar a mensagem original, basta utilizarmos a função inversa, dada por

$$f^{-1}(x) = \frac{x}{11} - \frac{5}{11}.$$

Aplicamos a mensagem cifrada $60\ 5\ 126\ 203\ 159$ na função inversa

$$f^{-1}(60) = \frac{60}{11} - \frac{5}{11} = \frac{55}{11} = 5,$$

$$f^{-1}(5) = \frac{5}{11} - \frac{5}{11} = \frac{0}{11} = 0,$$

$$f^{-1}(126) = \frac{126}{11} - \frac{5}{11} = \frac{121}{11} = 11,$$

$$f^{-1}(203) = \frac{203}{11} - \frac{5}{11} = \frac{198}{11} = 18,$$

$$f^{-1}(159) = \frac{159}{11} - \frac{5}{11} = \frac{154}{11} = 14.$$

Observamos que $f^{-1}(60) = 5$ e 5↔F; $f^{-1}(5) = 0$ e 0↔A; $f^{-1}(126) = 11$ e 11↔L; $f^{-1}(203) = 18$ e 18↔S; $f^{-1}(159) = 14$ e 14↔O. Logo, recuperamos a mensagem original **FALSO**.

CONJUNTO $\mathbb{Z}_n$

Utilizando uma função afim real, nossa mensagem original com as letras de A a Z, é cifrada em uma mensagem com números, o ideal seria que nossa mensagem original fosse cifrada também utilizando as letras de A a Z. Para tanto, deixaremos de usar uma função afim real e passaremos a utilizar uma função afim em um subconjunto dos números inteiros, $\mathbb{Z}$, com certas propriedades específicas, o conjunto $\mathbb{Z}_n$.

Nosso conjunto de caracteres, letras de A a Z, possui 26 elementos, e associamos com os números de 0 a 25, portanto, utilizaremos o subconjunto

$$\{0,1,2,3,4,5,6,7,8,9,10,11,12,\ldots,18,20,21,22,23,24,25\}.$$

Este conjunto possui 26 elementos, denotaremos por

$$\mathbb{Z}_{26}.$$

Este conjunto, $\mathbb{Z}_{26}$, é um conjunto fechado para as operações de soma e multiplicação. Funciona da seguinte maneira, por exemplo,

$$18 + 25 = 43$$

observamos que 43 não pertence ao conjunto $\mathbb{Z}_{26}$, assim, fazemos o seguinte procedimento, dividimos 43 por 26

$$43 = 1 \cdot 26 + 17,$$

ou seja, o resto da divisão de 43 por 26 é 17, utilizaremos este 17 para representar o 43 no conjunto $\mathbb{Z}_{26}$, e escrevemos $43 \equiv 17(mod\ 26)$, que significa "43 é côngruo a 17 módulo 26" – o leitor que deseja se aprofundar mais sobre o assunto, pode pesquisar sobre congruência de números inteiros. Por simplicidade, de agora em diante, escreveremos $43 = 17$ em $\mathbb{Z}_{26}$, para representar $43 \equiv 17(mod\ 26)$.

Outro exemplo, o número 532 não pertence a $\mathbb{Z}_{26}$. Procedemos do mesmo modo, dividimos 532 por 26

$$532 = 20{\cdot}26 + 12,$$

obtemos que o resto da divisão de 532 por 26 é 12, então utilizaremos o 12 para representar o 532 no conjunto $\mathbb{Z}_{26}$; neste caso, escrevemos $532 = 12$ em $\mathbb{Z}_{26}$, para representar $532 \equiv 12(mod\ 26)$.

Antes de procedermos e chegarmos a utilizar uma função afim no conjunto $\mathbb{Z}_{26}$, vamos nos acostumar a utilizar soma e multiplicação neste tipo de conjunto

$$\mathbb{Z}_n = \{0,1,2,3,4,5,\ldots,n-1,n\}.$$

Devemos também aprender a lidar com Máximo Divisor Comum e saber como calcular o inverso multiplicativo de um número em $\mathbb{Z}_n$.

Observamos que, em casos onde não houver dúvidas com qual conjunto $\mathbb{Z}_n$ lidamos, escreveremos apenas $x = y$ para representar $x \equiv y(mod\ n)$.

SOMA E MULTIPLICAÇÃO EM $\mathbb{Z}_n$

O conjunto $\mathbb{Z}_{26}$ é muito grande para observarmos mais a fundo como funciona o ser fechado para soma e multiplicação. Vamos ver em um conjunto $\mathbb{Z}_n$ com n menor que 26, por exemplo, para $n = 6$, ou seja,

$$\mathbb{Z}_6 = \{0,1,2,3,4,5\}.$$

Faremos todas as operações possíveis de soma e multiplicação em $\mathbb{Z}_6$. Começaremos pela soma

$$\begin{aligned} &0+1=1, \quad 0+2=2, \quad 0+3=3,\\ &0+4=4, \quad 0+5=5, \quad 1+0=1,\\ &1+1=2, \quad 1+2=3, \quad 1+3=4,\\ &1+4=5, \quad 1+5=6, \end{aligned}$$

até então, todos os valores das somas estavam dentro do conjunto $\mathbb{Z}_6$, mas esta última operação, $1+5=6$, tem um resultado que está fora de $\mathbb{Z}_6$. Neste caso, procedemos como feito antes, dividimos o valor que excede, ou que seja igual, o 6 por 6 e usamos o resto da divisão para representar este valor excedente

$$6 = 1 \cdot 6 + 0,$$

obtemos que o resto da divisão de 6 por 6 é zero, então utilizaremos o zero para representar o 6 no conjunto $\mathbb{Z}_6, 6 = 0$ em $\mathbb{Z}_6$. Lembrando que, por simplicidade, escrevemos $6 = 0$ em $\mathbb{Z}_6$, para evitar usar $6 \equiv 0(mod\ 6)$.

Continuamos nossa tábua de operação da soma

$1 + 5 = 6 = 0,$ $2 + 0 = 2,$ $2 + 1 = 3,$
$2 + 2 = 4,$ $2 + 3 = 5,$ $2 + 4 = 6 = 0,$
$2 + 5 = 7 = 1,$ $3 + 0 = 3,$ $3 + 1 = 4,$
$3 + 2 = 5,$ $3 + 3 = 6 = 0,$ $3 + 4 = 7 = 1,$
$3 + 5 = 8 = 2,$ $4 + 0 = 4,$ $4 + 1 = 5,$
$4 + 2 = 6 = 0,$ $4 + 3 = 7 = 1,$ $4 + 4 = 8 = 2,$
$4 + 5 = 9 = 3,$ $5 + 0 = 5,$ $5 + 1 = 6 = 0,$
$5 + 2 = 7 = 1,$ $5 + 3 = 8 = 2,$ $5 + 3 = 8 = 2,$
$5 + 4 = 9 = 3,$ $5 + 5 = 10 = 4.$

Observamos que na nossa tabela utilizamos o procedimento para caso o valor exceda, ou seja igual, o 6, para representar o número no conjunto $\mathbb{Z}_6$. Por exemplo, $5 + 5 = 10$ e 10 excede 6, assim, usamos o resto da divisão de 10 por 6, que é 4, para representar o 10 no $\mathbb{Z}_6$; resumindo $10 = 4$ em $\mathbb{Z}_6$.

Na multiplicação, procedemos da mesma maneira, já utilizando a técnica de representar em $\mathbb{Z}_6$ um número maior ou igual que 6.

$$
\begin{aligned}
&0\cdot 0 = 0, && 0\cdot 1 = 0,\\
&0\cdot 2 = 0, && 0\cdot 3 = 0,\\
&0\cdot 4 = 0, && 0\cdot 5 = 0,\\
&1\cdot 0 = 0, && 1\cdot 1 = 1,\\
&1\cdot 2 = 2, && 1\cdot 3 = 3,\\
&1\cdot 4 = 4, && 1\cdot 5 = 5,\\
&2\cdot 0 = 0, && 2\cdot 1 = 2,\\
&2\cdot 2 = 4, && 2\cdot 3 = 6 = 0,\\
&2\cdot 4 = 8 = 2, && 2\cdot 5 = 10 = 4,\\
&3\cdot 0 = 0, && 3\cdot 1 = 3,\\
&3\cdot 2 = 6 = 0, && 3\cdot 3 = 9 = 3,\\
&3\cdot 4 = 12 = 0, && 3\cdot 5 = 15 = 3,\\
&4\cdot 0 = 0, && 4\cdot 1 = 4,\\
&4\cdot 2 = 8 = 2, && 4\cdot 3 = 12 = 0,\\
&4\cdot 4 = 16 = 4, && 4\cdot 5 = 20 = 2,\\
&5\cdot 0 = 0, && 5\cdot 1 = 5,\\
&5\cdot 2 = 10 = 4, && 5\cdot 3 = 15 = 3,\\
&5\cdot 4 = 20 = 2, && 5\cdot 5 = 25 = 1.
\end{aligned}
$$

Vimos o funcionamento da soma e multiplicação no conjunto $\mathbb{Z}_6$.

Para fixar melhor o conteúdo, veremos, a seguir, a tabela de soma e multiplicação em $\mathbb{Z}_8$.

SOMA E MULTIPLICAÇÃO EM $\mathbb{Z}_8$

Vamos fixar mais o procedimento de soma e multiplicação em um conjunto $\mathbb{Z}_n$, agora para o caso em que $n = 8$, ou seja, no conjunto

$$\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}.$$

Neste caso, como nosso $n = 8$, quando um número for maior ou igual a 8, devemos dividir este valor por 8 e utilizar o resto da divisão para representar este número. Por exemplo, 15 é maior que 8 e dividindo 15 por 8 obtemos

$$15 = 1 \cdot 8 + 7,$$

o que nos leva a dizer que 7 é o resto da divisão de 15 por 8, logo, $15 = 7$ em $\mathbb{Z}_8$.

Tabela da soma em $\mathbb{Z}_8$

$0+0=0$, $0+1=1$, $0+2=2$,
$0+3=3$, $0+4=4$, $0+5=5$,
$0+6=6$, $0+7=7$, $1+0=1$,
$1+1=2$, $1+2=3$, $1+3=4$,
$1+4=5$, $1+5=6$, $1+6=7$,
$1+7=8=0$, $2+0=2$, $2+1=3$,
$2+2=4$, $2+3=5$, $2+4=6$,
$2+5=7$, $2+6=8=0$, $2+7=9=1$,
$3+0=3$, $3+1=4$, $3+2=5$,
$3+3=6$, $3+4=7$, $3+5=8=0$,
$3+6=9=1$, $3+7=10=2$, $4+0=4$,
$4+1=5$, $4+2=6$, $4+3=7$,
$4+4=8=0$, $4+5=9=1$, $4+6=10=2$,
$4+7=11=3$, $5+0=5$, $5+1=6$,
$5+2=7$, $5+3=8=0$, $5+4=9=1$,
$5+5=10=2$, $5+6=11=3$, $5+7=12=4$,
$6+0=6$, $6+1=7$, $6+2=8=0$,
$6+3=9=1$, $6+4=10=2$, $6+5=11=3$,
$6+6=12=4$, $6+7=13=5$, $7+0=7$,
$7+1=8=0$, $7+2=9=1$, $7+3=10=2$,
$7+4=11=3$, $7+5=12=4$, $7+6=13=5$,
$7+7=14=6$.

Tabela da multiplicação em $\mathbb{Z}_8$

$0 \cdot 0 = 0,$ $0 \cdot 1 = 0,$ $0 \cdot 2 = 0,$
$0 \cdot 3 = 0,$ $0 \cdot 4 = 0,$ $0 \cdot 5 = 0,$
$0 \cdot 6 = 0,$ $0 \cdot 7 = 0,$ $1 \cdot 0 = 0,$
$1 \cdot 1 = 1,$ $1 \cdot 2 = 2,$ $1 \cdot 3 = 3,$
$1 \cdot 4 = 4,$ $1 \cdot 5 = 5,$ $1 \cdot 6 = 6,$
$1 \cdot 7 = 7,$ $2 \cdot 0 = 0,$ $2 \cdot 1 = 2,$
$2 \cdot 2 = 4,$ $2 \cdot 3 = 6,$ $2 \cdot 4 = 8 = 0,$
$2 \cdot 5 = 10 = 2,$ $2 \cdot 6 = 12 = 4,$ $2 \cdot 7 = 14 = 6,$
$3 \cdot 0 = 0,$ $3 \cdot 1 = 3,$ $3 \cdot 2 = 6,$
$3 \cdot 3 = 9 = 1,$ $3 \cdot 4 = 12 = 4,$ $3 \cdot 5 = 15 = 7,$
$3 \cdot 6 = 18 = 2,$ $3 \cdot 7 = 21 = 3,$ $4 \cdot 0 = 0,$
$4 \cdot 1 = 4,$ $4 \cdot 2 = 8 = 0,$ $4 \cdot 3 = 12 = 4,$
$4 \cdot 4 = 16 = 0,$ $4 \cdot 5 = 20 = 4,$ $4 \cdot 6 = 24 = 0,$
$4 \cdot 7 = 28 = 4,$ $5 \cdot 0 = 0,$ $5 \cdot 1 = 5,$
$5 \cdot 2 = 10 = 2,$ $5 \cdot 3 = 15 = 7,$ $5 \cdot 4 = 20 = 4,$
$5 \cdot 5 = 25 = 1,$ $5 \cdot 6 = 30 = 6,$ $5 \cdot 7 = 35 = 3,$
$6 \cdot 0 = 0,$ $6 \cdot 1 = 6,$ $6 \cdot 2 = 12 = 4,$
$6 \cdot 3 = 18 = 2,$ $6 \cdot 4 = 24 = 0,$ $6 \cdot 5 = 30 = 6,$
$6 \cdot 6 = 36 = 4,$ $6 \cdot 7 = 42 = 2,$ $7 \cdot 0 = 0,$
$7 \cdot 1 = 7,$ $7 \cdot 2 = 14 = 6,$ $7 \cdot 3 = 21 = 5,$
$7 \cdot 4 = 28 = 4,$ $7 \cdot 5 = 35 = 3,$ $7 \cdot 6 = 42 = 2,$
$7 \cdot 7 = 49 = 1.$

Ressaltamos que estamos usando uma força de expressão para simplificar na escrita, ao dizer, por exemplo, que

$$14 = 6, \qquad 35 = 3,$$
$$42 = 2, \qquad 49 = 1.$$

Estas igualdades só são válidas no conjunto $\mathbb{Z}_8$ e, respectivamente, representam as seguintes congruências

$$14 \equiv 6 (mod\ 8), \qquad 35 \equiv 3 (mod\ 8),$$
$$42 \equiv 2 (mod\ 8), \qquad 49 \equiv 1 (mod\ 8).$$

MÁXIMO DIVISOR COMUM (MDC)

Existe uma peculiaridade para identificar quando uma função afim, $f(x) = ax + b$, possui ou não função inversa em $\mathbb{Z}_n$. Basta verificar se o Máximo Divisor Comum (MDC) entre a e n é igual a 1, em símbolos,

$$MDC(a,n) = 1.$$

Mostraremos, através de exemplos, como calcular o MDC entre dois números inteiros, utilizando um método conhecido por *Algoritmo Euclidiano* [6].

Vamos calcular o MDC entre 4 e 26, em símbolos, $MDC(4,26)$. Fazemos a divisão de 26 por 4,

$$26 = 4 \cdot 6 + 2.$$

Observamos que na divisão de 26 por 4, obtemos o resto 2. Como este resto é diferente de zero, $2 \neq 0$, agora temos de dividir, o último divisor, 4, pelo último resto 2,

$$4 = 2 \cdot 2 + 0,$$

vemos que o resto da divisão de 4 por 2 é zero, portanto o MDC entre 4 e 26 é 2, $MDC(4,26) = 2$.

Resumindo, fazemos as devidas divisões, até chegar no resto zero, o penúltimo resto destas divisões, diferente de zero, é o MDC entre os dois números dados.

Vamos calcular $MDC(7,55)$. Fazemos a divisão de 55 por 7,

$$55 = 7 \cdot 7 + 6,$$

obtemos que o resto nesta divisão é $6 \neq 0$. Assim, devemos continuar e dividimos o último divisor, 7, pelo resto 6,

$$7 = 6 \cdot 1 + 1,$$

obtendo o resto desta divisão que é $1 \neq 0$. Portanto, temos de continuar e efetuamos a divisão do último divisor, 6, pelo último resto, 1,

$$6 = 1 \cdot 6 + 0,$$

chegando que o resto nesta divisão é zero e, concluímos que, $MDC(7,55) = 1$, pois 1 é o último resto das sequências de divisões, diferente de zero.

Calculando o $MDC(12,56)$. Dividimos 56 por 12,

$$56 = 12 \cdot 4 + 8,$$

obtemos resto $8 \neq 0$. Então, dividimos o último divisor, 12, pelo último resto, 8,

$$12 = 8 \cdot 1 + 4,$$

obtemos resto $4 \neq 0$. Assim, dividimos o último divisor, 8, pelo último resto, 4,

$$8 = 4 \cdot 2 + 0,$$

e chegamos no resto zero, portanto, o $MDC(12,56) = 4$, pois 4 é o último resto das divisões que é diferente de zero.

Calculando o $MDC(5,26)$. Dividimos 26 por 5,

$$26 = 5 \cdot 5 + 1,$$

obtemos resto $1 \neq 0$. Então, dividimos o último divisor, 5, pelo último resto, 1,

$$5 = 1 \cdot 5 + 0,$$

e chegamos no resto zero, portanto, o $MDC(5,26) = 1$.

Calculando o $MDC(13,26)$. Dividimos 26 por 13,

$$26 = 13 \cdot 2 + 0,$$

e chegamos no resto zero, portanto, o $MDC(13,26) = 13$.

De acordo com alguns dos exemplos que fizemos: temos, a título de ilustração, que a função $f(x) = 13x + 4$ não possui função inversa em $\mathbb{Z}_{26}$,, porque $MDC(13,26) = 13 \neq 1$. Em $\mathbb{Z}_{55}$ a função $f(x) = 7x + 43$ possui função inversa, porque $MDC(7,55) = 1$.

INVERSO MULTIPLICATIVO EM $\mathbb{Z}_n$

Nos números reais, sabemos que

$$2 \cdot \frac{1}{2} = 1,$$

então, dizemos que $\frac{1}{2}$ é o inverso multiplicativo de 2 em $\mathbb{R}$.

Em $\mathbb{Z}_n$, não possuímos esta facilidade de usar uma fração para encontrar um inverso multiplicativo de um número, porque não existe frações em $\mathbb{Z}_n$. Entretanto, um número $a \in \mathbb{Z}_n$ possui inverso multiplicativo, em $\mathbb{Z}_n$, se, e somente se, $MDC(a,n) = 1$. Neste caso, o inverso multiplicativo de um número $a \in \mathbb{Z}_n$, será um número

$$a^{-1} \in \mathbb{Z}_n, \text{ tal que } a \cdot a^{-1} = 1 \text{ em } \mathbb{Z}_n.$$

Para determinarmos o inverso multiplicativo de um número a em $\mathbb{Z}_n$, devemos chegar numa expressão do tipo

$$a \cdot a^{-1} + q \cdot n = 1, \text{ com } q \in \mathbb{Z}.$$

Assim, o número $a^{-1} \in \mathbb{Z}_n$ é o inverso multiplicativo de a em $\mathbb{Z}_n$. Vale ressaltar também que, a em $\mathbb{Z}_n$ é o inverso multiplicativo de a^{-1} em $\mathbb{Z}_n$, portanto, conclui-se que $MDC\left(a^{-1},n\right)$ também é 1.

Veremos como encontrar o inverso multiplicativo de 7 em $\mathbb{Z}_{55}$. Vimos que $MDC(7,55) = 1$, portanto, em $\mathbb{Z}_{55}$, 7 possui inverso multiplicativo. Procedemos como se fossemos calcular o MDC entre 7 e 55. Dividimos 55 por 7,

$$55 = 7 \cdot 7 + 6 \Longrightarrow 6 = 55 - 7 \cdot 7,$$

dividimos 7 por 6,

$$7 = 6 \cdot 1 + 1 \Longrightarrow 1 = 7 - 6 \cdot 1.$$

Chegamos que $1 = 7 - 6 \cdot 1$ e $6 = 55 - 7 \cdot 7$. Então, trocamos o 6 na primeira equação por $55 - 7 \cdot 7$, obtendo

$$1 = 7 - (55 - 7 \cdot 7) \cdot 1,$$

reorganizamos esta equação

$$1 = 7 - 55 + 7 \cdot 7 \Longrightarrow 1 = 7 \cdot 8 - 55.$$

Observamos que chegamos em uma expressão do tipo

$$a \cdot a^{-1} + q \cdot n = 1,$$

onde $a = 7, a^{-1} = 8, q = -1$ e $n = 55$, ou seja

$$7 \cdot 8 + (-1) \cdot 55 = 1.$$

Logo, 8 é o inverso multiplicativo de 7 em $\mathbb{Z}_{55}$. De fato,

$$7 \cdot 8 = 56,$$

e 56 é um número que excede o conjunto $\mathbb{Z}_{55} = \{0,1,2,...,52,53,54\}$, neste caso, devemos dividir 56 por 55 para encontrar seu representante em $\mathbb{Z}_{55}$,

$$56 = 55 \cdot 1 + 1,$$

portanto 56=1 em $\mathbb{Z}_{55}$ e, consequentemente, 8 é o inverso multiplicativo de 7 em $\mathbb{Z}_{55}$, pois $7 \cdot 8 = 56 = 1$ em $\mathbb{Z}_{55}$.

Observamos também que 7 é o inverso multiplicativo de 8 em $\mathbb{Z}_{55}$.

Outro exemplo, 4 não possui inverso multiplicativo em $\mathbb{Z}_{26}$, pois $MDC(4,26) = 2 \neq 1$.

Exemplo, 13 não possui inverso multiplicativo em $\mathbb{Z}_{26}$, pois $MDC(13,26) = 13 \neq 1$.

Vimos que o $MDC(5,26) = 1$, então 5 possui inverso multiplicativo em $\mathbb{Z}_{26}$. Vamos calcular o inverso multiplicativo de 5 em $\mathbb{Z}_{26}$. Dividimos 26 por 5

$$26 = 5 \cdot 5 + 1 \Longrightarrow 1 = 5 \cdot (-5) + 26,$$

Encontramos uma expressão do tipo $a \cdot a^{-1} + q \cdot n = 1$, ou seja, $a = 5, a^{-1} = -5, q = -1$ e $n = 26$. Logo o inverso multiplicativo de 5 em $\mathbb{Z}_{26}$ é -5. O problema é que -5 não está no conjunto $\mathbb{Z}_{26}$, logo devemos encontrar o seu representante em $\mathbb{Z}_{26}$. Quando é um número negativo, pelo fato

da divisão com números negativos não ser trivial, existe um procedimento mais simples que é ir somando 26 a este número negativo, até obter um número em $\mathbb{Z}_{26}$,

$$-5 + 26 = 21 \in \mathbb{Z}_{26}.$$

Portanto, $-5 = 21$ em $\mathbb{Z}_{26}$, e 21 é o inverso multiplicativo de 5 em $\mathbb{Z}_{26}$. De fato,

$$5 \cdot 21 = 105 = 4 \cdot 26 + 1,$$

ou seja, $5 \cdot 21 = 105 = 1$ em $\mathbb{Z}_{26}$. Ressaltamos também que 21 é o inverso multiplicativo de 5 em $\mathbb{Z}_{26}$.

Vamos verificar se 19 possui inverso multiplicativo em $\mathbb{Z}_{26}$, em caso afirmativo, calcularemos seu inverso multiplicativo. Primeiro, calculamos $MDC(19,26)$, começamos dividindo 26 por 19,

$$26 = 19 \cdot 1 + 7.$$

O resto da divisão é $7 \neq 0$, assim, dividimos o último divisor, 19, pelo último resto, 7,

$$19 = 7 \cdot 2 + 5.$$

O resto da divisão é $5 \neq 0$, então, continuamos e dividimos o último divisor, 7, pelo último resto, 5,

$$7 = 5 \cdot 1 + 2.$$

O resto da divisão é $2 \neq 0$, logo, continuamos e dividimos o último divisor, 5, pelo último resto, 2,

$$5 = 2 \cdot 2 + 1.$$

O resto da divisão é $1 \neq 0$, assim, continuamos e dividimos o último divisor, 2, pelo último resto, 1,

$$2 = 1 \cdot 2 + 0.$$

Obtemos que o resto desta última divisão é zero, portanto o $MDC(19{,}26) = 1$, que é o último resto, diferente de zero, de todas as divisões efetuadas.

Ora, como $MDC(19{,}26) = 1$, isto significa que 19 possui inverso multiplicativo em $\mathbb{Z}_{26}$. Nas divisões efetuadas para o cálculo do $MDC(19{,}26) = 1$, obtemos as seguintes equações

$$7 = 26 - 1 \cdot 19 = 26 - 19,$$

$$5 = 19 - 7 \cdot 2 \Longrightarrow 5 = 19 - (26 - 19) \cdot 2 \Longrightarrow$$

$$\Longrightarrow 5 = 3 \cdot 19 - 2 \cdot 26,$$

$$2 = 7 - 5 = (26 - 19) - (3 \cdot 19 - 2 \cdot 26)$$

$$\Longrightarrow 2 = 26 \cdot 3 - 4 \cdot 19,$$

$$1 = 5 - 2 \cdot 2 = (3 \cdot 19 - 2 \cdot 26) - 2(26 \cdot 3 - 4 \cdot 19)$$

$$\Longrightarrow 1 = 11 \cdot 19 - 8 \cdot 26.$$

Logo, desta última igualdade, chegamos em uma expressão do tipo $a \cdot a^{-1} + q \cdot n = 1$, pois

$$19 \cdot 11 + (-8) \cdot 26 = 1.$$

Assim, temos que $a = 19, a^{-1} = 11, q = -8$ e $n = 26$. Então, o inverso multiplicativo de 19 em $\mathbb{Z}_{26}$ é 11. De fato, $19 \cdot 11 = 209 = 1$ em $\mathbb{Z}_{26}$. Por outro lado, 19 é o inverso multiplicativo de 11 em $\mathbb{Z}_{26}$.

CRIPTOGRAFANDO EM $\mathbb{Z}_n$

Estamos aptos para criptografar mensagens em $\mathbb{Z}_n$, utilizando uma função afim do tipo $f(x) = ax + b$, com $a \neq 0, MDC(a,n) = 1$ e b pode ser qualquer número de $\mathbb{Z}_n$. Como $MDC(a,n) = 1$, então a possui inverso multiplicativo a^{-1} em $\mathbb{Z}_n$ e a função inversa, $f^{-1}(x)$, de $f(x) = ax + b$ é dada por

$$f^{-1}(x) = a^{-1}x - b \cdot a^{-1}.$$

Criptografaremos nossa primeira mensagem em $\mathbb{Z}_{26}$, utilizando a função

$$f(x) = 5x + 10, a = 5 \text{ e } b = 10.$$

Escolhemos esta função porque $a = 5$ e calculamos que $MDC(5,26) = 1$, logo existe função inversa. O valor $b = 10$ foi escolhido aleatoriamente, porque não tem restrição para $b \in \mathbb{Z}_{26}$. Criptografaremos a mensagem **BOLA**. Lembrando que associamos cada caractere, letra do alfabeto que utilizamos para escrever as mensagens, com um número de $\mathbb{Z}_{26} = \{0,1,2,...,23,24,25\}$,

A↔0; B↔1; C↔2; ... X↔23; Y↔24; Z↔25.

Associamos cada letra da palavra **BOLA**, com o seu respectivo número

B↔1, O↔14, L↔11, A↔0

Aplicamos a função $f(x) = 5x + 10$ em cada número.

$$f(1) = 5 \cdot 1 + 10 = 15 \in \mathbb{Z}_{26},$$

$$f(14) = 5 \cdot 14 + 10 = 80 = 2 \in \mathbb{Z}_{26},$$

$$f(11) = 5 \cdot 11 + 10 = 65 = 13 \in \mathbb{Z}_{26},$$

$$f(0) = 5 \cdot 0 + 10 = 10 \in \mathbb{Z}_{26}.$$

Aqui está a grande diferença da primeira criptografia que fizemos utilizando uma função em $\mathbb{R}$, pois agora podemos associar cada valor obtido com sua respectiva letra,

$$f(1) = 15 \leftrightarrow P,$$

$$f(14) = 2 \leftrightarrow C,$$

$$f(11) = 13 \leftrightarrow N,$$

$$f(0) = 10 \leftrightarrow K.$$

Portanto, a mensagem **BOLA** é cifrada para mensagem **PCNK**, quando criptografada com a função $f(x) = 5x + 10$ em $\mathbb{Z}_{26}$.

Vejamos como descriptografar a mensagem **PCNK**, sabendo que foi criptografada com a função $f(x) = 5x + 10$ em

$\mathbb{Z}_{26}$. Ora, devemos calcular a função inversa de $f(x) = 5x + 10$ em $\mathbb{Z}_{26}$, a qual é dada por

$$f^{-1}(x) = a^{-1}x - b \cdot a^{-1}.$$

Atentamos que, $a = 5$ e $b = 10$. Anteriormente, já calculamos o inverso multiplicativo de $a = 5$ em $\mathbb{Z}_{26}$, que é $a^{-1} = 21$. Resta calcularmos

$$-b \cdot a^{-1} = -10 \cdot 21 = -210 = 24 \text{ em } \mathbb{Z}_{26}.$$

Logo, em $\mathbb{Z}_{26}$, a função inversa de $f(x) = 5x + 10$ é

$$f^{-1}(x) = 21x + 24.$$

Para recuperar a mensagem original, associamos cada letra da mensagem cifrada a seu respectivo número e aplicamos f^{-1},

$$P \leftrightarrow 15 \text{ e } f^{-1}(15) = 21 \cdot 15 + 24 = 339 = 1 \text{ em } \mathbb{Z}_{26},$$

$$C \leftrightarrow 2 \text{ e } f^{-1}(2) = 21 \cdot 2 + 24 = 66 = 14 \text{ em } \mathbb{Z}_{26},$$

$$N \leftrightarrow 13 \text{ e } f^{-1}(13) = 21 \cdot 13 + 24 = 297 = 11 \text{ em } \mathbb{Z}_{26},$$

$$K \leftrightarrow 10 \text{ e } f^{-1}(10) = 21 \cdot 10 + 24 = 234 = 0 \text{ em } \mathbb{Z}_{26}.$$

Em resumo,

$$f^{-1}(15) = 1 \leftrightarrow B,$$

$$f^{-1}(2) = 14 \leftrightarrow O,$$

$$f^{-1}(13) = 11 \leftrightarrow L,$$

$$f^{-1}(10) = 0 \leftrightarrow A.$$

Portanto, recuperamos a mensagem original **BOLA**.

Descriptografar a mensagem cifrada **UKSHEKC** sabendo que foi criptografada com a função $f(x) = 5x + 10$ em $\mathbb{Z}_{26}$. Ora, acabamos de calcular a função inversa de $f(x) = 5x + 10$ em $\mathbb{Z}_{26}$, que é $f^{-1}(x) = 21x + 24$, basta associarmos cada letra da mensagem cifrada **UKSHEKC** ao seu respectivo número e aplicarmos f^{-1},

$U \leftrightarrow 20$ e $f^{-1}(20) = 21 \cdot 20 + 24 = 444 = 2$ em $\mathbb{Z}_{26}$,

$K \leftrightarrow 10$ e $f^{-1}(10) = 21 \cdot 10 + 24 = 234 = 0$ em $\mathbb{Z}_{26}$,

$S \leftrightarrow 18$ e $f^{-1}(18) = 21 \cdot 18 + 24 = 402 = 12$ em $\mathbb{Z}_{26}$,

$H \leftrightarrow 7$ e $f^{-1}(7) = 21 \cdot 7 + 24 = 171 = 15$ em $\mathbb{Z}_{26}$,

$E \leftrightarrow 4$ e $f^{-1}(4) = 21 \cdot 4 + 24 = 108 = 4$ em $\mathbb{Z}_{26}$,

$C \leftrightarrow 2$ e $f^{-1}(2) = 21 \cdot 2 + 24 = 66 = 14$ em $\mathbb{Z}_{26}$.

Em resumo, temos

$$f^{-1}(20) = 2 \leftrightarrow C,$$

$$f^{-1}(10) = 0 \leftrightarrow A,$$

$$f^{-1}(18) = 12 \leftrightarrow M,$$

$$f^{-1}(7) = 15 \leftrightarrow P,$$

$$f^{-1}(4) = 4 \leftrightarrow E,$$

$$f^{-1}(10) = 0 \leftrightarrow A,$$

$$f^{-1}(2) = 14 \leftrightarrow O.$$

Portanto, recuperamos a mensagem original **CAMPEAO**.

Vamos descriptografar a mensagem **UPNSZJ**, sabendo que foi criptografada com a função $f(x) = 19x + 19$ em $\mathbb{Z}_{26}$. Lembrando que, calculamos $MDC(19,26) = 1$ e, portanto, $a = 19$ tem inverso multiplicativo em $\mathbb{Z}_{26}$, e também determinamos este inverso multiplicativo, $a^{-1} = 11$. Logo, a função inversa de $f(x) = 19x + 19$ em $\mathbb{Z}_{26}$ é igual a

$$f^{-1}(x) = 11x - 19 \cdot 11 \Longrightarrow f^{-1}(x) = 11x + 25.$$

Acabamos de calcular a função inversa de

$$f(x) = 19x + 19 \text{ em } \mathbb{Z}_{26},$$

que é

$$f^{-1}(x) = 11x + 25.$$

Portanto, para descriptografar a mensagem cifrada **UPNSZJ** basta associarmos cada letra ao seu respectivo número e aplicarmos f^{-1},

$U \leftrightarrow 20$ e $f^{-1}(20) = 11 \cdot 20 + 25 = 245 = 11$ em $\mathbb{Z}_{26}$,

$P \leftrightarrow 15$ e $f^{-1}(15) = 11 \cdot 15 + 25 = 190 = 8$ em $\mathbb{Z}_{26}$,

$N \leftrightarrow 13$ e $f^{-1}(13) = 11 \cdot 13 + 25 = 168 = 12$ em $\mathbb{Z}_{26}$,

$S \leftrightarrow 18$ e $f^{-1}(18) = 11 \cdot 18 + 25 = 223 = 15$ em $\mathbb{Z}_{26}$,

$Z \leftrightarrow 25$ e $f^{-1}(25) = 11 \cdot 25 + 25 = 300 = 14$ em $\mathbb{Z}_{26}$,

$J \leftrightarrow 9$ e $f^{-1}(9) = 11 \cdot 9 + 25 = 124 = 20$ em $\mathbb{Z}_{26}$.

Em resumo, temos

$$f^{-1}(20) = 11 \leftrightarrow L,$$

$$f^{-1}(15) = 8 \leftrightarrow I,$$

$$f^{-1}(13) = 12 \leftrightarrow M,$$

$$f^{-1}(18) = 15 \leftrightarrow P,$$

$$f^{-1}(25) = 14 \leftrightarrow O,$$

$$f^{-1}(9) = 20 \leftrightarrow U.$$

Portanto, recuperamos a mensagem **LIMPOU**.

Recapitulando, de modo geral, aprendemos que para criptografar mensagens em $\mathbb{Z}_n$, utilizamos uma função do tipo

$$f(x) = ax + b,$$

onde, não existe restrição para escolha do $b \in \mathbb{Z}_n$, porém o valor de $a \in \mathbb{Z}_n$ deve obedecer a seguinte restrição,

$$MDC(a,n) = 1,$$

para que seja possível calcular a função inversa de $f(x)$, dada por $f^{-1}(x) = a^{-1}x - b \cdot a^{-1}$.

ADICIONANDO MAIS CARACTERES

Nossas mensagens estão limitadas a utilizar apenas as letras maiúsculas, veremos como adicionar mais caracteres no nosso alfabeto para utilizarmos no método criptográfico.

Adicionaremos o espaço em branco, representado pelo *underline* _, os caracteres de pontuação ! ? . , : e os caracteres numéricos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Nosso alfabeto de A a Z com 26 caracteres, está ganhando mais 16 caracteres, ficando com um total de 42 símbolos. Sendo assim, para poder associar cada caractere a um único número, teremos de trabalhar no conjunto

$$\mathbb{Z}_{42} = \{0,1,2,3,\ldots,39,40,41\}.$$

Manteremos a associação determinada previamente para as letras de A a Z

A↔0; B↔1; C↔2; ... X↔23; Y↔24; Z↔25,

e para os novos caracteres, faremos a associação

_ ↔ 26	! ↔27	? ↔28	. ↔29
, ↔30	: ↔31	0↔32	1↔33
2↔34	3↔35	4↔36	5↔37
6↔38	7↔39	8↔40	9↔41.

Para critptografar utilizando este novo alfabeto, composto de 42 caracteres, e uma função afim do tipo $f(x) = ax + b$ em $\mathbb{Z}_{42}$, lembramos que não tem restrição para $b \in \mathbb{Z}_{42}$, mas $MDC(a,42)$ deve ser igual a 1.

Vamos criptografar e descriptografar a mensagem **TUDO_BEM?** utilizando a função $f(x) = 23x + 13$ em $\mathbb{Z}_{42}$. Observamos que $a = 23, b = 13$ e $MDC(23,42) = 1$, ou seja, esta é uma função apta para criptografia no conjunto $\mathbb{Z}_{42}$. Para criptografarmos a mensagem original, associamos cada letra ao seu respectivo número e aplicamos a função.

$$T \leftrightarrow 19 \text{ e } f(19) = 23 \cdot 19 + 13 = 450 = 30 \text{ em } \mathbb{Z}_{42},$$

$$U \leftrightarrow 20 \text{ e } f(20) = 23 \cdot 20 + 13 = 473 = 11 \text{ em } \mathbb{Z}_{42},$$

$$D \leftrightarrow 3 \text{ e } f(3) = 23 \cdot 3 + 13 = 82 = 40 \text{ em } \mathbb{Z}_{42},$$

$$O \leftrightarrow 14 \text{ e } f(14) = 23 \cdot 14 + 13 = 335 = 41 \text{ em } \mathbb{Z}_{42},$$

$$\_ \leftrightarrow 26 \text{ e } f(26) = 23 \cdot 26 + 13 = 611 = 23 \text{ em } \mathbb{Z}_{42},$$

$$B \leftrightarrow 1 \text{ e } f(1) = 23 \cdot 1 + 13 = 36 \text{ em } \mathbb{Z}_{42},$$

$$E \leftrightarrow 4 \text{ e } f(4) = 23 \cdot 4 + 13 = 105 = 21 \text{ em } \mathbb{Z}_{42},$$

$$M \leftrightarrow 12 \text{ e } f(12) = 23 \cdot 12 + 13 = 289 = 37 \text{ em } \mathbb{Z}_{42},$$

$$? \leftrightarrow 28 \text{ e } f(28) = 23 \cdot 28 + 13 = 657 = 27 \text{ em } \mathbb{Z}_{42}.$$

Em resumo, temos

$$f(19) = 30 \leftrightarrow ,$$

$$f(20) = 11 \leftrightarrow L$$

$$f(3) = 40 \leftrightarrow 8$$

$$f(14) = 41 \leftrightarrow 9$$

$$f(26) = 23 \leftrightarrow X$$

$$f(1) = 36 \leftrightarrow 4$$

$$f(4) = 21 \leftrightarrow V$$

$$f(12) = 37 \leftrightarrow 5$$

$$f(28) = 27 \leftrightarrow !$$

Portanto, a mensagem original **TUDO_BEM?** é cifrada na mensagem **,L89X4V5!** utilizando a função $f(x) = 23x + 13$ em $\mathbb{Z}_{42}$.

Para descriptografar a mensagem **,L89X4V5!** sabendo que foi criptografada utilizando a função $f(x) = 23x + 13$ em $\mathbb{Z}_{42}$, devemos determinar a função inversa $f^{-1}(x) = a^{-1}x - b \cdot a^{-1}$ de $f(x)$. Primeiro, calculamos a^{-1}, inverso multiplicativo de $a = 23$ em $\mathbb{Z}_{42}$, para tanto, começamos dividindo 42 por 23,

$$42 = 23 \cdot 1 + 19.$$

Sendo o resto desta divião igual a $19 \neq 1$, dividimos 23 por 19,

$$23 = 19 \cdot 1 + 4.$$

Sendo o resto desta divião igual a $4 \neq 1$, dividimos 19 por 4,

$$19 = 4 \cdot 4 + 3.$$

Sendo o resto desta divião igual a $3 \neq 1$, dividimos 4 por 3,

$$4 = 3 \cdot 1 + 1.$$

Sendo o resto desta última divisão igual a 1, organizamos as esquações para obtermos

$$1 = 23 \cdot 11 - 6 \cdot 42.$$

Logo, chegamos em uma equação do tipo $a \cdot a^{-1} + q \cdot n = 1$, onde $a = 23, a^{-1} = 11, q = -6, n = 42$, e, concluímos que $a^{-1} = 11$ é o inverso multiplicativo de $a = 23$ em $\mathbb{Z}_{42}$, e

$$-b \cdot a^{-1} = -13 \cdot 11 = -142 = 25 \text{ em } \mathbb{Z}_{42}.$$

Portanto, $f^{-1}(x) = 11x + 25$. Para decifrar a mensagem **,L89X4V5!**, basta associarmos cada caractere ao seu respectivo número e aplicar f^{-1}.

,$\leftrightarrow 30$ e $f^{-1}(30) = 11 \cdot 30 + 25 = 355 = 19$ em $\mathbb{Z}_{42}$,

$L \leftrightarrow 11$ e $f^{-1}(11) = 11 \cdot 11 + 25 = 146 = 20$ em $\mathbb{Z}_{42}$,

$8 \leftrightarrow 40$ e $f^{-1}(40) = 11 \cdot 40 + 25 = 465 = 3$ em $\mathbb{Z}_{42}$,

$9 \leftrightarrow 41$ e $f^{-1}(41) = 11 \cdot 41 + 25 = 476 = 14$ em $\mathbb{Z}_{42}$,

$X \leftrightarrow 23$ e $f^{-1}(23) = 11 \cdot 23 + 25 = 278 = 26$ em $\mathbb{Z}_{42}$,

$4 \leftrightarrow 36$ e $f^{-1}(36) = 11 \cdot 36 + 25 = 421 = 1$ em $\mathbb{Z}_{42}$,

$V \leftrightarrow 21$ e $f^{-1}(21) = 11 \cdot 21 + 25 = 256 = 4$ em $\mathbb{Z}_{42}$,

$5 \leftrightarrow 37$ e $f^{-1}(37) = 11 \cdot 37 + 25 = 432 = 12$ em $\mathbb{Z}_{42}$,

$! \leftrightarrow 27$ e $f^{-1}(27) = 11 \cdot 27 + 25 = 322 = 28$ em $\mathbb{Z}_{42}$.

Em resumo,

$$f^{-1}(30) = 19 \leftrightarrow T$$

$$f^{-1}(11) = 20 \leftrightarrow U$$

$$f^{-1}(40) = 3 \leftrightarrow \mathrm{D}$$

$$f^{-1}(41) = 14 \leftrightarrow O$$

$$f^{-1}(23) = 26 \leftrightarrow \_$$

$$f^{-1}(36) = 1 \leftrightarrow B$$

$$f^{-1}(21) = 4 \leftrightarrow E$$

$$f^{-1}(37) = 12 \leftrightarrow M$$

$$f^{-1}(27) = 28 \leftrightarrow ?$$

e recuperamos a mensagem original **TUDO_BEM?**.

Vamos partir para outro exemplo. Descriptografar a mensagem cifrada **VH,9LXRNO59I**, sabendo que foi criptografada com a função $f(x) = 23x + 13$ em $\mathbb{Z}_{42}$. Ora, como já temos a função inversa, $f^{-1}(x) = 11x + 25$ de $f(x)$, basta associarmos cada caractere ao seu respectivo número e aplicar f^{-1}.

$V \leftrightarrow 21$ e $f^{-1}(21) = 11 \cdot 21 + 25 = 256 = 4$ em $\mathbb{Z}_{42}$,

$H \leftrightarrow 7$ e $f^{-1}(7) = 11 \cdot 7 + 25 = 102 = 18$ em $\mathbb{Z}_{42}$,

$, \leftrightarrow 30$ e $f^{-1}(30) = 11 \cdot 30 + 25 = 355 = 19$ em $\mathbb{Z}_{42}$,

$9 \leftrightarrow 41$ e $f^{-1}(41) = 11 \cdot 41 + 25 = 476 = 14$ em $\mathbb{Z}_{42}$,

$L \leftrightarrow 11$ e $f^{-1}(11) = 11 \cdot 11 + 25 = 146 = 20$ em $\mathbb{Z}_{42}$,

$X \leftrightarrow 23$ e $f^{-1}(23) = 11 \cdot 23 + 25 = 278 = 26$ em $\mathbb{Z}_{42}$,

$R \leftrightarrow 17$ e $f^{-1}(17) = 11 \cdot 17 + 25 = 213 = 2$ em $\mathbb{Z}_{42}$,

$N \leftrightarrow 13$ e $f^{-1}(13) = 11 \cdot 13 + 25 = 168 = 0$ em $\mathbb{Z}_{42}$,

$O \leftrightarrow 14$ e $f^{-1}(14) = 11 \cdot 14 + 25 = 179 = 11$ em $\mathbb{Z}_{42}$,

$5 \leftrightarrow 37$ e $f^{-1}(37) = 11 \cdot 37 + 25 = 432 = 12$ em $\mathbb{Z}_{42}$,

$I \leftrightarrow 8$ e $f^{-1}(8) = 11 \cdot 8 + 25 = 113 = 29$ em $\mathbb{Z}_{42}$.

Em resumo,

$$f^{-1}(21) = 4 \leftrightarrow E$$

$$f^{-1}(7) = 18 \leftrightarrow S$$

$$f^{-1}(30) = 19 \leftrightarrow T$$

$$f^{-1}(41) = 14 \leftrightarrow O$$

$$f^{-1}(11) = 20 \leftrightarrow U$$

$$f^{-1}(23) = 26 \leftrightarrow \_$$

$$f^{-1}(17) = 3 \leftrightarrow C$$

$$f^{-1}(13) = 0 \leftrightarrow A$$

$$f^{-1}(14) = 11 \leftrightarrow L$$

$$f^{-1}(37) = 12 \leftrightarrow M$$

$$f^{-1}(41) = 14 \leftrightarrow O$$

$$f^{-1}(8) = 29 \leftrightarrow .$$

Portanto, recuperamos a mensagem original **ESTOU_CALMO.**.

ADICIONANDO AINDA MAIS CARACTERES

O nosso alfabeto para criptografar possui os seguintes caracteres: letras maiúsculas de A a Z, espaço em branco, representado pelo *underline* _ , os caracteres de pontuação ! ? . , : e os caracteres numéricos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Respeitando a associação numérica definida anteriormente, adicionaremos ao nosso alfabeto as letras minúsculas de a a z, com a seguinte associação numérica

a ↔ 42	b ↔43	c ↔44	d ↔45
e ↔46	f ↔47	g↔48	h↔49
i↔50	j↔51	k↔52	l↔53
m↔54	n↔55	o↔56	p↔57
q↔58	r↔59	s↔60	t↔61
u↔62	v↔63	w↔64	x↔65
y↔66	z↔67.		

Nosso alfabeto, tem agora, no total, 68 caracteres, sendo assim, teremos de trabalhar no conjunto

$$\mathbb{Z}_{68} = \{0,1,2,...,65,66,67\}.$$

Utilizaremos funções do tipo $f(x) = ax + b$ em $\mathbb{Z}_{68}$ para criptografar e descriptografar mensagens, onde $b \in \mathbb{Z}_{68}$ não

tem restrição, porém $MDC(a,68)$ deve ser igual a um, para que possamos calcular a função inversa $f^{-1}(x) = a^{-1}x - b \cdot a^{-1}$.

Utilizaremos a função $f(x) = 7x + 36$ em $\mathbb{Z}_{68}$ para criptografar mensagens. Observamos que $MDC(7,68) = 1$ e também vale a seguinte igualdade

$$7 \cdot 39 + (-3) \cdot 68 = 1.$$

Assim, temos que $a = 7, a^{-1} = 39, q = -3$ e $n = 68$. Logo, como $b = 36$,

$$-b \cdot a^{-1} = -36 \cdot 39 = 24 \text{ em } \mathbb{Z}_{68}.$$

Portanto, $f^{-1}(x) = 39x + 24$ é a função inversa de $f(x) = 7x + 36$ em $\mathbb{Z}_{68}$.

Vamos criptografar a mensagem original **Ola,Cicrano.** com $f(x) = 7x + 36$ em $\mathbb{Z}_{68}$. Associamos cada caractere da mensagem original com seu respectivo valor numérico e aplicamos f.

Em resumo,

$$O \leftrightarrow 14 \text{ e } f(14) = 66 \leftrightarrow y$$

$$l \leftrightarrow 53 \text{ e } f(53) = 67 \leftrightarrow z$$

$$a \leftrightarrow 42 \text{ e } f(42) = 58 \leftrightarrow q$$

$$, \leftrightarrow 30 \text{ e } f(30) = 42 \leftrightarrow a$$

$$C \leftrightarrow 2 \text{ e } f(2) = 50 \leftrightarrow i$$

$$i \leftrightarrow 50 \text{ e } f(50) = 46 \leftrightarrow e$$

$$c \leftrightarrow 44 \text{ e } f(44) = 4 \leftrightarrow E$$

$$r \leftrightarrow 59 \text{ e } f(59) = 41 \leftrightarrow 9$$

$$n \leftrightarrow 55 \text{ e } f(55) = 13 \leftrightarrow N$$

$$o \leftrightarrow 56 \text{ e } f(56) = 20 \leftrightarrow U$$

$$. \leftrightarrow 29 \text{ e } f(29) = 35 \leftrightarrow 3$$

Portanto, a mensagem original **Ola,Cicrano.** quando criptografada com $f(x) = 7x + 36$ em $\mathbb{Z}_{68}$, obtemos a mensagem cifrada **yzqaieE9qNU3**.

Vamos descriptografar a mensagem cifrada **_!U9nfBSNES** sabendo que foi criptografada com a função $f(x) = 7x + 36$ em $\mathbb{Z}_{68}$. Para tanto, associamos cada caractere da mensagem cifrada ao seu respectivo número e aplicamos a função inversa $f^{-1}(x) = 39x + 24$.

Em resumo,

$$\_ \leftrightarrow 26 \text{ e } f^{-1}(26) = 18 \leftrightarrow S$$

$$! \leftrightarrow 27 \text{ e } f^{-1}(27) = 57 \leftrightarrow p$$

$$U \leftrightarrow 20 \text{ e } f^{-1}(20) = 56 \leftrightarrow o$$

$$9 \leftrightarrow 41 \text{ e } f^{-1}(41) = 59 \leftrightarrow r$$

$$n \leftrightarrow 55 \text{ e } f^{-1}(55) = 61 \leftrightarrow t$$

$$f \leftrightarrow 47 \text{ e } f^{-1}(47) = 26 \leftrightarrow \_$$

$$B \leftrightarrow 1 \text{ e } f^{-1}(1) = 21 \leftrightarrow V$$

$$S \leftrightarrow 18 \text{ e } f^{-1}(18) = 46 \leftrightarrow e$$

$$N \leftrightarrow 13 \text{ e } f^{-1}(13) = 55 \leftrightarrow n$$

$$E \leftrightarrow 4 \text{ e } f^{-1}(4) = 44 \leftrightarrow c$$

Portanto, recuperamos a mensagem original **SportVence**.

Vamos descriptografar a mensagem cifrada **3Qqnb7Zym6**, sabendo que foi criptografada utilizando a função $f(x) = 41x + 5$ em $\mathbb{Z}_{68}$. A função inversa de $f(x) = 41x + 5$ em $\mathbb{Z}_{68}$ é $f^{-1}(x) = 5x + 43$, logo, basta associarmos cada caractere da mensagem cifrada ao seu respectivo caractere e aplicar f^{-1}.

Em resumo,

$$3 \leftrightarrow 35 \text{ e } f^{-1}(35) = 14 \leftrightarrow O$$
$$Q \leftrightarrow 16 \text{ e } f^{-1}(16) = 55 \leftrightarrow n$$
$$q \leftrightarrow 58 \text{ e } f^{-1}(58) = 61 \leftrightarrow t$$
$$n \leftrightarrow 55 \text{ e } f^{-1}(55) = 46 \leftrightarrow e$$

$$b \leftrightarrow 43 \text{ e } f^{-1}(43) = 54 \leftrightarrow m$$

$$7 \leftrightarrow 39 \text{ e } f^{-1}(39) = 34 \leftrightarrow 2$$

$$Z \leftrightarrow 25 \text{ e } f^{-1}(25) = 32 \leftrightarrow 0$$

$$y \leftrightarrow 66 \text{ e } f^{-1}(66) = 33 \leftrightarrow 1$$

$$m \leftrightarrow 54 \text{ e } f^{-1}(54) = 41 \leftrightarrow 9$$

$$6 \leftrightarrow 38 \text{ e } f^{-1}(38) = 29 \leftrightarrow .$$

Portanto, recuperamos a mensagem original **Ontem2019.**.

REFERÊNCIAS

[1] Holden, J. *The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*, Princeton University Press, 2017.

[2] Koblitz, N. *A Course in Number Theory and Cryptography*, Springer, 1994.

[3] Lemos, M. *Criptografia, Números Primos e Algoritmos*, Publicações Matemáticas, IMPA, 2010. <http://impa.br/wp-content/uploads/2017/04/PM_04.pdf>

[4] Miller, G. *'The intelligence coup of the century'*, The Washington Post, 2020. <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-cryptoencryption-machines-espionage/>

[5] *O jogo da imitação*. Direção de Morten Tyldum. Reino Unido, Estados Unidos da América: Black Bear Pictures, FilmNation Entertainment (in association with), Bristol Automotive, Orange Corp, 2014. (115 min.).

[6] Silva, A. A. *Números, Relações e Criptografia*, Departamento de Matemática, Centro de Ciências Exatas e da Natureza, Universidade Federal de Paraíba. <http://www.mat.ufpb.br/sergio/provas/me_i/livro-andrade.pdf>

SOBRE O AUTOR

José Laudelino de Menezes Neto é bacharel em Matemática pela Universidade Federal da Paraíba (UFPB), Mestre e Doutor em Matemática pela Universidade Federal de Pernambuco (UFPE), e é professor do Departamento de Ciências Exatas do Campus IV da UFPB.

Este livro foi
diagramado pela
Editora UFPB em 2021.

O livro ensina,de modo leve e didático, os procedimentos para cifrar e decifrar uma mensagem, utilizando um método de criptografia que utiliza uma função afim do tipo f(x)=ax+b.