Introdução a Criptografia

por José Laudelino de M. Neto (laudelino@dcx.ufpb.br)

Professor do Departamento de Ciências Exatas (DCX) - CCAE - UFPB

Este texto foi desenvolvido com o intuito de servir de guia para um minicurso de introdução a criptografia, com um enfoque mais prático em exemplos dos sistemas criptográficos, sem se aprofundar tanto nos conceitos matemáticos.

Sumário

1 Criptografia Simples

Criptografia: arte de cifrar/codificar mensagens

Definir alfabeto (caracteres) a ser utilizado

A	B	C	D	E	F	G	H	I	J	K	L	M
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
13	14	15	16	17	18	19	20	21	22	23	24	25

Distinguir maiusculas de minusculas, incluir, se necessário, números, caracteres de pontuação (! ? . , ; : etc) e caracteres especiais ($ & # % + - = etc).

Observe que cada letra/caractere está associada a um número e nosso alfabeto (mapa de caracteres a ser utilizado) possui 26 caracteres, apenas letras maiusculas.

Utilizamos uma função para criptografar. A função deve ser bijetiva para que se possa criptografar e descriptografar uma mensagem.

$$\text{Texto original} \quad \leftrightarrows \quad \text{Texto cifrado}$$

Função mais eficaz e simples para criptografar: $f(x) = ax + b$ com inversa $f^{-1}(x) = a'x + b'$, onde $a' = a^{-1}$ e $b' = -a^{-1}b$.

Observação: a^{-1} denota inverso multiplicativo, se $a \neq 0$ é um número, então $a \cdot a^{-1} = 1$.

Este tipo de **criptografia** é do tipo **simétrico**, de **chave de codificação secreta** (não pública). A chave de codificação são os valores a e b da função $f(x) = ax + b$ e a chave de decoficação são os valores a' e b' da função inversa de $f(x)$, $f^{-1}(x) = a'x + b'$. O motivo da chave ser não pública é que caso divulgado a e b, é muito fácil determinar a chave de decodificação $a' = a^{-1}$ e $b' = -a^{-1}b$.

Exemplo 1.1 *Vamos criptografar a mensagem* ***BOLA*** *utilizando a função* $f(x) = 2x + 6$.

Associamos cada letra da mensagem ao número correspondente,

$$B \to 1, \ O \to 14, \ L \to 11, \ A \to 0,$$

e aplicamos a função $f(x) = 2x + 6$,

$$f(1) = 8, f(14) = 34, f(11) = 28, f(0) = 6.$$

A mensagem cifrada/codificada será a sequência de números 8, 34, 28, 6.

Para decodificar a mensagem cifrada 8, 34, 28, 6, sabendo que foi codificada com $f(x) = 2x + 6$, *devemos calcular* $f^{-1}(x) = a'x + b'$. *Neste caso,*

$$a' = a^{-1} = 2^{-1} = \frac{1}{2}, \qquad b' = -a^{-1} \cdot b = -2^{-1} \cdot 6 = -\frac{6}{2} = -3.$$

Assim,

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

Aplicamos $f^{-1}(x) = \frac{x}{2} - 3$ *na mensagem cifrada 8, 34, 28, 6,*

$$f^{-1}(8) = 1 \to B, \quad f^{-1}(34) = 14 \to O, \quad f^{-1}(28) = 11 \to L, \quad f^{-1}(6) = 0 \to A,$$

e recuperamos o texto original ***BOLA***.

Exercício 1.1 *Descriptografe a mensagem 60, 5, 126, 203, 159, sabendo que foi criptografada com* $f(x) = 11x + 5$. *(Descobrir* $f^{-1}(x)$ *e descriptografar a mensagem)*

2 Melhorando a criptografia: congruências de números inteiros

Para melhorar a forma de criptografar, vamos utilizar congruências de números inteiros

$$a \equiv b (\text{mod } n) \Leftrightarrow a - b = q \cdot n.$$

Estamos trabalhando com um alfabeto (caracteres) que tem 26 símbolos, então iremos trabalhar com congruências módulo 26. (Caso o alfabeto tivesse 36 símbolos/caracteres, deve-se trabalhar com congruências módulo 36. De um modo geral, se trabalha com congruência módulo *quantidade de símbolos/caracteres do alfabeto*)

Como vamos trabalhar com congruências módulo 26, então a função que criptografa $f(x) = ax + b$ deve satisfazer $\text{mdc}(a, 26) = 1$.

(Caso trabalhassemos com congruências módulo 36, então a função que criptografa $f(x) = ax + b$ deveria satisfazer $\text{mdc}(a, 36) = 1$.)

Observação: mdc=máximo divisor comum.

Utilizando congruências módulo 26, não é possível usar a função $f(x) = 2x + 6$ para criptografar, porque $\text{mdc}(2, 26) = 2 \neq 1$.

Explicação matemática: O motivo é que $\text{mdc}(a, n) = 1 \Rightarrow$ é possível calcular o inverso multiplicativo de a, a^{-1}, na congruência módulo n.

Descobrir o inverso mulplicativo de algum número inteiro a na congruência módulo n é o mesmo que resolver um tipo de *Equação Diofantina*, a saber: determinar $p, q \in \mathbb{Z}$ que satisfazem $ap + nq = 1$ (este tipo de equação tem solução caso $\text{mdc}(a, n) = 1$).

Exemplo 2.1 *A função $g(x) = 3x + 5$ pode ser utilizada para criptografar mensagens com congruências módulo 26, porque $mdc(3, 26) = 1$. Vamos criptografar a mensagem* ***RUA****.*

Associamos cada letra da palavra ***RUA*** *ao seu respectivo número,*

$$R \to 17, \;\; U \to 20, \;\; A \to 0,$$

aplicamos a função $g(x) = 3x + 5$,

$$g(17) = 56 \equiv 4(mod 26) \text{ e } 4 \text{ associa com a letra } E,$$

$$g(20) = 65 \equiv 13(mod 26) \text{ e } 13 \text{ associa com a letra } N,$$

$$g(0) = 5 \equiv 5(mod 26) \text{ e } 5 \text{ associa com a letra } F.$$

Logo, a mensagem original ***RUA*** *é cifrada na mensagem* ENF *através da função $g(x) = 3x + 5$ utilizando congruências módulo 26.*

Para descriptografar a mensagem ENF *que foi criptografada com a função $g(x) = 3x + 5$ utilizando congruências módulo 26, precisamos calcular 3^{-1} na congruência módulo 26 para determinar $g^{-1}(x) = a'x + b'$.*

Consideremos $3^{-1} = p$, então nosso objetivo é resolver

$$3p \equiv 1(mod 26) \Leftrightarrow 3p - 1 = 26q \Rightarrow 3p - 26q = 1 \text{ (tipo de Equação Diofantina).}$$

Procedemos da seguinte maneira, dividimos 26 por 3.

$$26 = \boldsymbol{3} \cdot 8 + 2$$

dividimos ***3*** *por 2*

$$3 = \boldsymbol{2} \cdot 1 + 1$$

agora dividimos ***2*** *por 1*

$$2 = \boldsymbol{1} \cdot 2 + 0$$

como o resto dessa última divisão foi zero, significa que terminamos. Reorganizamos o que foi feito da seguinte forma

$$1 = 3 - \boldsymbol{2} \cdot 1 \quad e \quad \boldsymbol{2} = 26 - 3 \cdot 8$$

assim,

$$\begin{aligned} 1 &= 3 - (26 - 3 \cdot 8)1 \\ &\Downarrow \\ 1 &= 3 - 26 + 3 \cdot 8 \\ &\Downarrow \\ 1 &= 3 \cdot 9 - 26 \cdot 1 \quad (3^{-1} = p = 9 \ e \ q = 1). \end{aligned}$$

Logo, $3 \cdot 9 = 27 \equiv 1(mod 26)$*,*

$$a' = 9, \quad b' = -9 \cdot 5 = -45 \equiv 7(mod 26)$$

e $g^{-1}(x) = 9x + 7$ *em congruências módulo 26.*

Para decodificar a mensagem cifrada ENF*, associamos cada letra ao número associado*

$$E \to 4, \ N \to 13, \ F \to 5,$$

e aplicamos a função inversa de $g(x)$*,* $g^{-1}(x) = 9x + 7$*,*

$$g^{-1}(4) = 43 \equiv 17(mod 26) \ e \ 17 \ associa \ com \ a \ letra \ R,$$

$$g^{-1}(13) = 124 \equiv 20(mod 26) \ e \ 20 \ associa \ com \ a \ letra \ U,$$

$$g^{-1}(5) = 52 \equiv 0(mod 26) \ e \ 0 \ associa \ com \ a \ letra \ A.$$

Portanto, obtemos a mensagem original ***RUA****.*

Se utilizar congruências módulo 26 e criptografar mensagens com $g(x) = 3x + 5$, então descriptografa as mensagens com $g^{-1}(x) = 9x + 7$.

Exemplo 2.2 *Observamos que* $mdc(11, 26) = 1$*, então vamos determinar o inverso multiplicativo de 11 em congruências módulo 26.*

Procedemos da seguinte maneira, dividimos 26 por 11.

$$26 = \boldsymbol{11} \cdot 2 + \textit{4}$$

dividimos $\boldsymbol{11}$ *por* 4

$$11 = \boldsymbol{4} \cdot 2 + \textit{3}$$

agora dividimos $\boldsymbol{4}$ *por* 3

$$4 = \boldsymbol{3} \cdot 1 + \textit{1}$$

finalmente, dividimos $\boldsymbol{3}$ *por* 1

$$3 = \boldsymbol{1} \cdot 3 + \textit{0}$$

como o resto dessa última divisão foi zero, significa que terminamos. Reorganizamos o que foi feito da seguinte forma

$$1 = 4 - \boldsymbol{3} \cdot 1, \qquad \boldsymbol{3} = 11 - \textit{4} \cdot 2 \qquad e \quad \textit{4} = 26 - 11 \cdot 2$$

assim,

$$\begin{aligned} 1 &= 4 - (11 - 4 \cdot 2)1 \\ &\Downarrow \\ 1 &= 4 \cdot 3 - 11 \\ &\Downarrow \\ 1 &= (26 - 11 \cdot 2) \cdot 3 - 11 \\ &\Downarrow \\ 1 &= 26 \cdot 3 + 11 \cdot (-7). \end{aligned}$$

Portanto, $-7 \equiv 19(mod 26)$ *e* $11^{-1} = 19$ *em congruência módulo 26.*

Para testar se está correto, basta verificar se o resto da divisão de $11 \cdot 19 = 209$ *por* 26 *é 1.*

Exemplo 2.3 *Observamos que* $mdc(15, 26) = 1$*, então vamos determinar o inverso multiplicativo de 15 em congruências módulo 26.*

Procedemos da seguinte maneira, dividimos 26 por 15.

$$26 = \boldsymbol{15} \cdot 1 + \textit{11}$$

dividimos ***15*** *por 11*

$$15 = \boldsymbol{11} \cdot 1 + 4$$

dividimos ***11*** *por 4*

$$11 = \boldsymbol{4} \cdot 2 + 3$$

agora dividimos ***4*** *por 3*

$$4 = \boldsymbol{3} \cdot 1 + 1$$

finalmente, dividimos ***3*** *por* 1

$$3 = \boldsymbol{1} \cdot 3 + 0$$

como o resto dessa última divisão foi zero, significa que terminamos. Reorganizamos o que foi feito da seguinte forma

$$1 = 4 - \boldsymbol{3} \cdot 1, \qquad \boldsymbol{3} = 11 - 4 \cdot 2, \qquad 4 = 15 - 11 \cdot 1, \quad e \quad 11 = 26 - 15 \cdot 1$$

assim,

$$\begin{aligned}
1 &= 4 - (11 - 4 \cdot 2)1 \\
&\Downarrow \\
1 &= 4 \cdot 3 - 11 \\
&\Downarrow \\
1 &= (15 - 11 \cdot 1) \cdot 3 - 11 \\
&\Downarrow \\
1 &= 15 \cdot 3 + 11 \cdot (-4) \\
&\Downarrow \\
1 &= 15 \cdot 3 + (26 - 15 \cdot 1) \cdot (-4) \\
&\Downarrow \\
1 &= 15 \cdot 7 + 26 \cdot (-4).
\end{aligned}$$

Portanto, $15^{-1} = 7$ *em congruência módulo 26.*

Para testar se está correto, basta verificar se o resto da divisão de $15 \cdot 7 = 105$ *por* 26 *é 1.*

Exercício 2.1 *Decodifique a mensagem cifrada* SAT*, sabendo que foi codificada com* $f(x) = 11x + 2$*.*

(DICA: Determine o inverso multiplicativo de 11 em congruência módulo 26 - foi feito em um exemplo acima - e, em seguida, calcule $f^{-1}(x) = a'x + b'$*)*

Exercício 2.2 *Decodifique a mensagem cifrada* YTFP*, sabendo que foi codificada com* $h(x) = 23x + 5$.
(DICA: Determine o inverso multiplicativo de 23 em congruência módulo 26 e, em seguida, calcule $h^{-1}(x) = a'x + b'$*)*

3 Adicionando Novos Caracteres

Vamos adicionar no nosso alfabeto os caracteres 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9. Agora teremos 26 letras mais estes 10 números, teremos agora a seguinte relação

A	B	C	D	E	F	G	H	I	J	K	L	M
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
13	14	15	16	17	18	19	20	21	22	23	24	25

0	1	2	3	4	5	6	7	8	9
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
26	27	28	29	30	31	32	33	34	35

De agora em diante, vamos trabalhar com congruências módulo 36, pois nosso alfabeto possui 36 caracteres/símbolos.

Veja que a função $g(x) = 3x + 5$ (utilizada em um exemplo anterior) não serve para criptografar em congruências módulo 36, pois $\text{mdc}(3, 36) = 3 \neq 1$.

Exemplo 3.1 *Podemos usar a função* $h(x) = 11x + 4$ *para criptografar em congruências módulo 36, porque* $mdc(11, 36) = 1$*. Vamos criptografar a mensagem* ***FELIZ2017*** *com a função* $h(x)$*.*

Primeiro, associamos cada caractere com seu respectivo número

$$\begin{array}{ccccccccc} F & E & L & I & Z & 2 & 0 & 1 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 11 & 8 & 25 & 28 & 26 & 27 & 33 \end{array}$$

Aplicamos a função $h(x)$ *em cada valor*

$$h(5) = 11 \cdot 5 + 4 = 59 \equiv 23 (mod\ 36)\ \textit{e 23 equivale a X,}$$

$$h(4) = 11 \cdot 4 + 4 = 48 \equiv 12 (mod\ 36)\ \textit{e 12 equivale a M,}$$

$$h(11) = 11 \cdot 11 + 4 = 125 \equiv 17 (mod\ 36)\ \textit{e 17 equivale a R,}$$

$$h(8) = 11 \cdot 8 + 4 = 92 \equiv 20 (mod\ 36)\ \textit{e 20 equivale a U,}$$

$$h(25) = 11 \cdot 25 + 4 = 279 \equiv 27 (mod\ 36)\ \textit{e 27 equivale a 1,}$$

$$h(28) = 11 \cdot 28 + 4 = 312 \equiv 24 (mod\ 36)\ \textit{e 24 equivale a Y,}$$

$$h(26) = 11 \cdot 26 + 4 = 290 \equiv 2 (mod\ 36)\ \textit{e 2 equivale a C,}$$

$$h(27) = 11 \cdot 27 + 4 = 301 \equiv 13 (mod\ 36)\ \textit{e 13 equivale a N,}$$

$$h(33) = 11 \cdot 33 + 4 = 367 \equiv 7 (mod\ 36)\ \textit{e 7 equivale a H.}$$

Assim, temos a mensagem cifrada XMRU1YCNH.

Para decodificar a mensagem cifrada XMRU1YCNH *sabendo que foi codificada com a função* $h(x) = 11x + 4$ *em congruência módulo 36, devemos calcular* $h^{-1}(x) = a'x + b'$, *onde*

$a' = a^{-1} = 11^{-1}$ *determinar o inverso multiplicativo de 11 em congruências módulo 36,*

$$b' = -a^{-1}b.$$

Determinando o inverso multiplicativo de 11 em congruências módulo 36:

$$\textit{dividimos 36 por 11,}\ 36 = 11 \cdot 3 + 3,$$

$$\textit{dividimos 11 por 3,}\ 11 = 3 \cdot 3 + 2,$$

$$\textit{dividimos 3 por 2,}\ 3 = 2 \cdot 1 + 1,$$

$$\textit{dividimos 2 por 1,}\ 2 = 1 \cdot 2 + 0,$$

Agora reorganizamos

$$1 = 3 - 2 \cdot 1, \quad 2 = 11 - 3 \cdot 3, \quad 3 = 36 - 11 \cdot 3$$

logo,

$$1 = 3 - (11 - 3 \cdot 3) = 3 - 11 + 3 \cdot 3 = -11 + 3 \cdot 4$$

$$1 = -11 + (36 - 11 \cdot 3) \cdot 4 = -11 + 36 \cdot 4 - 11 \cdot 3 \cdot 4 = -11 + 36 \cdot 4 - 11 \cdot 12 = 36 \cdot 4 + 11(-13)$$

portanto, $11^{-1} = -13 \equiv 23 (mod\ 36)$. *De fato,* $11 \cdot 23 = 253 \equiv 1 (mod\ 36)$.

Assim, $a' = 23$ *e* $b' = -23 \cdot 4 = -92 \equiv 16 (mod\ 36)$ *e* $h^{-1}(x) = 23x + 16$.

Aplicamos a função $h^{-1}(x) = 23x + 16$ *no texto cifrado* XMRU1YCNH *para recuperar a mensagem original* ***FELIZ2017***.

Exercício 3.1 *Decodifique a mensagem* 93K6 *sabendo que foi codificada com* $h(x) = 11x + 4$.

Exercício 3.2 *Seja* $f(x) = 7x + 30$, *determine* $f^{-1}(x)$ *em congruências módulo 36. Em seguida, decodifique a mensagem* C14WM *sabendo que foi codificada com* $f(x) = 7x + 30$.

4 Criptografando em Blocos

A criptografia que fizemos até agora foi em blocos de 1 caractere. Nosso objetivo agora é criptografar em blocos de 2 caracteres. Para tanto, precisamos saber como escrever um número em uma base qualquer. A base usual é base dez (decimal), pois utiliza dez símbolos 0,1,2,3,4,5,6,7,8,9. Base binária utiliza dois símbolos 0 e 1. Base hexadecimal utiliza dezesseis símbolos 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.

Vamos escrever o número 323 em base 2 (binário). Começamos dividindo 323 por 2,

$$323 = 2 \cdot 161 + 1,$$

$$161 = 2 \cdot 80 + 1,$$

$$80 = 2 \cdot 40 + 0,$$

$$40 = 2 \cdot 20 + 0,$$

$$20 = 2 \cdot 10 + 0,$$

$$10 = 2 \cdot 5 + 0,$$

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

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

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

logo, basta pegar os restos de cada divisão de baixo para cima,

$$323 = (101000011)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

Vamos escrever 323 em base hexadecimal. Começamos dividindo 323 por 16,

$$323 = 16 \cdot 20 + 3$$

$$20 = 16 \cdot 1 + 4$$

$$1 = 16 \cdot 0 + 1$$

logo, pegamos os restos de cada divisão de baixo para cima, $323 = (143)_{16} = 1{\cdot}16^2{+}4{\cdot}16^1{+}3{\cdot}16^0$.

Como nosso alfabeto possui 36 símbolos (letras de A a Z e números de 0 a 9), para criptografar em blocos de 2 caracteres, passaremos a trabalhar com congruências módulo $36^2 = 1296$. Para criptografar com uma função $f(x) = ax + b$ em congruências módulo 1296, lembramos que $\text{mdc}(a, 1296) = 1$.

Vamos ver se é possível utilizar $f(x) = 121x + 35$. Devemos verificar se $\text{mdc}(121, 1296) = 1$. Procedemos como anteriormente, dividimos 1296 por 121,

$$1296 = 121 \cdot 10 + 86$$

$$121 = 86 \cdot 1 + 35$$

$$86 = 35 \cdot 2 + 16$$

$$35 = 16 \cdot 2 + 3$$

$$16 = 3 \cdot 5 + 1$$

$$3 = 1 \cdot 3 + 0$$

a última equação tem resto zero, então $\text{mdc}(121, 1296) = 1$ que é o resto da penúltima equação. Utilizando estas equações, obtemos o inverso de 121 em congruências módulo 1296.

$$1 = 16 - 3 \cdot 5, \quad 3 = 35 - 16 \cdot 2, \quad 16 = 86 - 35 \cdot 2,$$

$$35 = 121 - 86, \quad 86 = 1296 - 121 \cdot 10,$$

Assim,

$$1 = 38 \cdot 1296 + 121(-407) \Rightarrow -407 \equiv 889 (\text{mod } 1296).$$

Assim, o inverso multiplicativo de 121 é 889 em congruências módulo 1296, de fato,

$$121 \cdot 889 = 107569 \equiv 1 (\text{mod } 1296).$$

Assim, $f^{-1}(x) = 889x + 1285$.

Exemplo 4.1 *Vamos criptografar a mensagem* ***PRATA*** *utilizando* $f(x) = 121x+35$ *em blocos de 2 caracteres. Primeiro, vemos que* ***PRATA*** *possui uma quantidade ímpar de caracteres, devemos adicionar um símbolo para que fique com quantidade par, então adicionamos 0 no fim* ***PRATA0****. Separamos a mensagem em blocos de 2 caracteres* ***PR-AT-A0*** *e associamos cada símbolo ao seu número*

$$\begin{array}{cccccccc} P & R & - & A & T & - & A & 0 \\ \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow & \downarrow \\ 15 & 17 & & 0 & 19 & & 0 & 26 \end{array}$$

cada par de símbolo associa com um número escrito na base 36 da seguinte maneira

$$\begin{array}{ccccc} PR & - & AT & - & A0 \\ \downarrow & & \downarrow & & \downarrow \\ 36 \cdot 15 + 17 = 557 & & 36 \cdot 0 + 19 = 19 & & 36 \cdot 0 + 26 = 26 \end{array}$$

Aplicamos $f(x) = 121x + 35$ *nos três valores obtidos:*

$$f(557) = 121 \cdot 557 + 35 = 67432 \equiv 40 (mod\ 1296),$$

$$f(19) = 121 \cdot 19 + 35 = 2334 \equiv 1038 (mod\ 1296),$$

$$f(26) = 121 \cdot 26 + 35 = 3181 \equiv 589 (mod\ 1296).$$

Para obter cada par cifrado, devemos escrever os números 40, 1038 e 589 na base 36.

Escrevendo 40 na base 36:

$40 = 36 \cdot 1 + 4$

$1 = 36 \cdot 0 + 1$

$40 = (14)_{36} = 1 \cdot 36^1 + 4 \cdot 36^0 \rightarrow BE.$

Escrevendo 1038 na base 36:

$1038 = 36 \cdot 28 + 30$

$28 = 36 \cdot 0 + 28$

$1038 = 28 \cdot 36^1 + 30 \cdot 36^0 \rightarrow 24.$

Escrevendo 589 na base 36:

$589 = 36 \cdot 16 + 13$

$16 = 36 \cdot 0 + 16$

$589 = 16 \cdot 36^1 + 13 \cdot 36^0 \rightarrow QN.$

Portanto, a mensagem ***PRATA0*** *é cifrada na mensagem* BE24QN *pela função* $f(x) = 121x + 35$.

Para decodificar BE24QN*, associamos cada símbolo ao seu valor numérico, para, em seguida, obter o valor de cada par de símbolo*

$$\begin{array}{ccccc} BE & - & 24 & - & QN \\ \downarrow & & \downarrow & & \downarrow \\ 36 \cdot 1 + 4 = 40 & & 36 \cdot 28 + 30 = 1038 & & 36 \cdot 16 + 13 = 589 \end{array}$$

Como o texto foi cifrado com a função $f(x) = 121x + 35$*, então decodificamos ele usando a função inversa* $f^{-1}(x) = 889x + 1285$*, que já foi calculada.*

$$f^{-1}(40) = 889 \cdot 40 + 1285 = 36845 \equiv 557 (mod\ 1296),$$

$$f^{-1}(1038) = 889 \cdot 1038 + 1285 = 924067 \equiv 19 (mod\ 1296),$$

$$f^{-1}(589) = 889 \cdot 589 + 1285 = 524906 \equiv 26 (mod\ 1296).$$

Logo,

$$557 = 15 \cdot 36 + 17 \rightarrow \ PR,$$

$$19 = 0 \cdot 36 + 19 \rightarrow \ AT,$$

$$26 = 0 \cdot 36 + 26 \rightarrow \ A0,$$

recuperamos a mensagem original ***PRATA0****.*

Exercício 4.1 *Decodifique a mensagem* 99TCR8EYF6 *sabendo que foi codificada em blocos de 2 caracteres utilizando a função* $f(x) = 121x + 35$*.*

5 Criptografia RSA

5.1 Criptografia Assimétrica

O sistema de criptografia visto nas seções anteriores é chamado simétrico, porque, como foi visto, a chave usada para codificação é, de certa forma, igual a chave usada para decodificação, ou, equivalentemente, a partir de uma delas obtemos a outra. Por isso, os sistemas simétricos são interessantes quando um transmissor conversa apenas com um receptor. Caso um transmissor converse com vários receptores, então todos os receptores estarão aptos para decodificar o texto-cifrado. Para contornar este problema, apresentaremos um outro sistema de criptografia, chamado RSA, que foi desenvolvido por **R**ivest, **S**hamir e **A**dleman em 1978.

O RSA é um sistema criptográfico assimétrico e este tipo de sistema diferencia-se dos simétricos justamente pelo fato de permitir que vários indivíduos conversem entre si, onde cada um terá uma chave de codificação que é pública, ou seja, todos a conhecem, e por isto este tipo de sistema também é conhecido por sistema de criptografia com chave pública, e uma outra chave de decodificação que é mantida secreta.

No sistema assimétrico é, de um modo geral, impossível determinar uma chave a partir da outra, isto é, se sei a chave de codificação, já que esta é pública, é muito difícil obter a chave de decodificação.

5.2 Mecânica do Sistema Assimétrico

Suponhamos que exista um grupo de usuários u_j, $j = 1, 2, \ldots, n$ e eles desejam se comunicar entre si. Primeiro os usuários devem determinar o alfabeto que irão utilizar e a associação de cada símbolo do alfabeto com um número inteiro. Então, cada usuário u_j irá determinar um par de chaves $k_{c,j}$ e $k_{d,j}$ tais que

$$k_{c,j} \circ k_{d,j}(\mathbf{u}) = \mathbf{u} \quad \text{e} \quad k_{d,j} \circ k_{c,j}(\mathbf{u}) = \mathbf{u},$$

onde $\mathbf{u}$ é uma mensagem unitária do texto-original. A chave $k_{d,j}$ é mantida secreta e irá servir para o usuário u_j decodificar as mensagens criptografadas com a chave pública de codificação $k_{c,j}$.

Feito isso, se um usuário u_i deseja enviar uma mensagem $\mathbf{u}$ ao usuáro u_j, então, u_i utiliza a chave pública de codificação $k_{c,j}$ na mensagem $\mathbf{u}$ e obtem a mensagem codificada $\mathbf{d}$,

$$k_{c,j}(\mathbf{u}) = \mathbf{d}.$$

Em seguida o usuário u_i envia a mensagem codificada $\mathbf{d}$ a u_j e este ao recebê-la, decofica aplicando a chave secreta de decoficação $k_{d,j}$, recuperando, assim, a mensagem original $\mathbf{u}$,

$$k_{d,j}(\mathbf{d}) = \mathbf{u}.$$

Note que, caso um outro usuário u_k interceptasse a mensagem $\mathbf{d}$, enviada de u_i para u_j, ele não teria como decodificá-la, pois não possui a chave secreta de decodificação $k_{d,j}$.

5.3 A Função ϕ de Euler

A Função ϕ de Euler é utilizada na criptografia RSA.

Em $\mathbb{Z}_n$ um número $a \in \mathbb{Z}_n^*$ nem sempre terá um inverso multiplicativo, ou seja, não existe $a^{-1} \in \mathbb{Z}_n^*$ tal que $a^{-1} \cdot a = 1$. Por exemplo, o 2 não possui inverso multiplicativo em $\mathbb{Z}_4$. Explicamos isto porque a Função ϕ de Euler nos diz o número de elementos inversíveis de $\mathbb{Z}_n$. Por exemplo,

$$\phi(4) = 2, \quad \text{ou seja, } \mathbb{Z}_4 \text{ só possui dois elementos com inverso multiplicativo,}$$

pois em $\mathbb{Z}_4$ os únicos elementos inversíveis são 1 e 3.

Se p é um número primo, então em $\mathbb{Z}_p$ todos os elementos são inversíveis com exceção do 0, logo

$$\phi(p) = p - 1.$$

OBSERVAÇÃO: Lembramos que um número $a \in \mathbb{Z}_n$ tem inverso multiplicativo em $\mathbb{Z}_n$ se, e somente se, $mdc(a, n) = 1$.

Teorema 5.1 *Sejam $a, n \in \mathbb{N}$, com $mdc(a, n) = 1$. Se $r, t \in \mathbb{N}$ são tais que $rt \equiv 1\,(mod\ \phi(n))$, então*

$$a^{rt} \equiv a\,(mod\ n)\,.$$

Corolário 5.2 *Sejam $n, r, t \in \mathbb{N}$. Se $mdc(t, \phi(n)) = 1$, então a função*

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \text{ dada por } f(x) = x^t$$

é uma correspondência biunívoca com $f^{-1}(x) = x^r$, onde

$$rt \equiv 1\,(mod\ \phi(n))\,.$$

5.4 Sistema RSA

Em um sistema de criptografia com chave pública RSA, cada usuário u_i escolhe dois números primos distintos, extremamente grandes, p_i e q_i para determinar $n_i = p_i \cdot q_i$ e aleatoriamente um inteiro qualquer t_i tal que

$$mdc(t_i, \phi(n_i)) = 1.$$

A seguir u_i calcula $r_i \equiv t_i^{-1}\,(\text{mod}\ \phi(n_i))$. Agora, o usuário u_i torna público a chave de codificação

$$k_{c,i} = (n_i, t_i)$$

e mantém secreta a chave de decodificação

$$k_{d,i} = (n_i, r_i).$$

O processo de codificação é dado pela função

$$f : \mathbb{Z}_{n_i} \longrightarrow \mathbb{Z}_{n_i}, \qquad f(x) = x^{t_i}$$

e o processo de decodificação é dado pela função

$$f^{-1} : \mathbb{Z}_{n_i} \longrightarrow \mathbb{Z}_{n_i}, \quad f^{-1}(x) = x^{r_i}.$$

OBSERVAÇÃO: Se $n_i = p_i \cdot q_i$ com p_i e q_i números primos, então $\phi(n_i) = (p_i - 1)(q_i - 1)$. Por exemplo, $6 = 2 \cdot 3$ com 2 e 3 sendo números primos, logo $\phi(6) = (2-1)(3-1) = 1 \cdot 2 = 2$. Outro exemplo, $35 = 5 \cdot 7$ com 5 e 7 números primos, portanto $\phi(35) = (5-1)(7-1) = 4 \cdot 6 = 24$.

Seja $\mathbb{F}$ um alfabeto com n símbolos. Vamos dividir nosso texto-original em mensagens unitárias com blocos de k símbolos, os quais são vistos como um inteiro (conforme feito na seção Criptografando em Blocos)

$$x = x_{k-1}n^{k-1} + \ldots + x_2 n^2 + x_1 n + x_0 \in \mathbb{Z}_{n^k}, \quad x_r \in \mathbb{Z}_n, \quad r \in \{0, 1, \ldots, k-1\},$$

e cada um destes blocos será codificado em um só bloco com l símbolos, com $k < l$. Para fazer isto, cada usuário u_i deve escolher os dois números primos distintos p_i e q_i de modo que $n_i = p_i \cdot q_i$ satisfaça

$$n^k < n_i < n^l.$$

Então, qualquer mensagem unitária $\mathbf{u}$ do texto-original, isto é, um inteiro menor do que n^k, corresponde a um elemento de $\mathbb{Z}_{n_i}$ e, como $n_i < n^l$, a imagem $f(\mathbf{u}) \in \mathbb{Z}_{n_i}$ pode ser escrita de modo único como um bloco de l símbolos.

Exemplo 5.1 *Neste exemplo, vamos utilizar o seguinte alfabeto $\mathbb{F}$ (com 26 símbolos),*

A	B	C	$\ldots$	K	L	M	$\ldots$	V	W	X	Y	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\ldots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\ldots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	$\ldots$	10	11	12	$\ldots$	21	22	23	24	25.

Escolhemos $k = 3$ e $l = 4$, ou seja, vamos criptografar mensagens com blocos de 3 caracteres para blocos de 4 caracteres. Para enviarmos a mensagem

"FIM"

para um usuário u_j com chave de codificação

$$k_{c,j} = (35183, 4459),$$

primeiro determinamos a equivalência numérica

$$FIM$$

$$\updownarrow$$

$$5 \cdot 26^2 + 8 \cdot 26 + 12 = 3600$$

e, então, calculamos

$$3600^{4459} \, (mod \; 35183) \, ,$$

que é

$$8808 = 0 \cdot 26^3 + 13 \cdot 26^2 + 0 \cdot 26 + 20$$

e equivale a mensagem "ANAU". O usuário u_j sabe a chave de decodificação

$$k_{d,j} = (35183, 9139)$$

e, então, calcula

$$8808^{9139} \, (mod \; 35183) \, ,$$

que equivale a $3600 = 5 \cdot 26^2 + 8 \cdot 26 + 12$ e, portanto, recupera a mensagem "FIM".

OBSERVAÇÃO: O usuário u_j gerou suas chaves multiplicando os números primos $p_j = 151$ e $q_j = 233$ para obter n_j, depois escolheu aleatoriamente o número t_j tal que $mdc(t_j, \phi(n_j)) = 1$. Finalmente, determinou $r_j \equiv t_j^{-1} \, (\text{mod } \phi(n_j))$. Note que os números p_j, q_j e r_j permanecem secretos.

Exemplo 5.2 *Vamos utilizar o mesmo alfabeto $\mathbb{F}$ do Exemplo 5.1.*

Escolhemos k=1, l=2, ou seja, criptografaremos mensagens de blocos de 1 caractere para blocos de 2 caracteres. Escolhemos $n_j = 17 \cdot 37 = 629$. Note que $26^1 < 629 < 26^2$.
Calculando $\phi(629) = (17-1)(37-1) = 16 \cdot 36 = 576$; escolhemos aleatoriamente $t_j = 245$ satisfazendo $mdc(t_j, \phi(n_j)) = mdc(245, 576) = 1$.
Determinando $r_j = t_j^{-1}$ em congruência módulo $\phi(n_j) = 576$:

$$576 = 245 \cdot 2, \qquad 245 = 86 \cdot 2 + 73, \qquad 86 = 73 \cdot 1 + 13, \qquad 73 = 13 \cdot 5 + 8,$$

$$13 = 8 \cdot 1 + 5, \qquad 8 = 5 \cdot 1 + 2, \qquad 3 = 2 \cdot 1 + 1, \qquad 2 = 1 \cdot 2 + 0.$$

Organizando estas equações acima, obtemos

$$1 = 221 \cdot 245 - 94 \cdot 576 \quad \Rightarrow \quad r_j = t_j^{-1} = 245^{-1} \equiv 221 (mod \; 576).$$

Logo, a chave de codificação (pública) é

$$k_{c,j} = (n_j, t_j) = (629, 245),$$

e a chave de decodificação (secreta) é

$$k_{d,j} = (n_j, r_j) = (629, 221).$$

Vamos codificar a mensagem ***BOM****:*

$$\begin{array}{ccccc} B & - & O & - & M \\ \downarrow & & \downarrow & & \downarrow \\ 1 & & 14 & & 12. \end{array}$$

Calculamos

$$1^{245} \equiv 1(mod\ 629), \quad 14^{245} \equiv 29(mod\ 629), \quad 12^{245} \equiv 292(mod\ 629),$$

e obtemos

$$1 = 0 \cdot 26 + 1 \to AB, \quad 29 = 1 \cdot 26 + 3 \to BD, \quad 292 = 11 \cdot 26 + 6 \to LG,$$

o que nos dá a mensagem cifrada ABBDLG*.*

Decodificando a mensagem cifrada ABBDLG*:*

Sabemos que está codificada em blocos de 2 caracteres, assim

$$\begin{array}{ccccc} AB & - & BD & - & LG \\ \downarrow & & \downarrow & & \downarrow \\ 0 \cdot 26 + 1 = 1 & & 1 \cdot 26 + 3 = 29 & & 11 \cdot 26 + 6 = 292. \end{array}$$

Calculamos

$$1^{221} \equiv 1(mod\ 629), \quad 29^{221} \equiv 14(mod\ 629), \quad 292^{221} \equiv 12(mod\ 629),$$

e recuperamos a mensagem original $1 \to B$*,* $14 \to O$*,* $12 \to M$*:* ***BOM****.*

OBSERVAÇÃO: A segurança do sistema RSA está na dificuldade em fatorar o inteiro n_i. Caso n_i fosse fatorado, poderiamos determinar o inteiro r_i e, consequentemente, a chave de decodificação $k_{d,i} = (n_i, r_i)$.

6 Criptografia de Curvas Elípticas

EM BREVE...

Referências

[1] SILVA, A. A. **Números, Relações e Criptografia**, Departamento de Matemática, Centro de Ciências Exatas e da Natureza, Universidade Federal de Paraíba. Disponível em: www.mat.ufpb.br/bruno/wa_files/Andrade.pdf (29/07/2017).

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

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