Criptografia RSA - Dia 1

Priscilla Pereira de Souza

⋆ ⋆ ⋆

Dia 1 - Tipos de Criptografia

- Código de César
- Código em Blocos
- Chave Privada x Chave Pública
- Criptografia em Matrizes

Criptografia

Criptografia

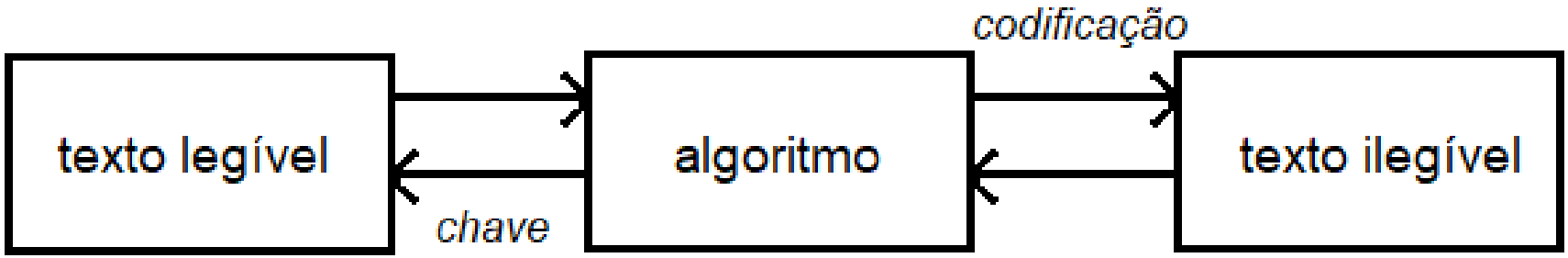
Definição

*A **criptografia** é o estudo de métodos e técnicas para transformar um texto legível em algo ilegível, podendo reverter o processo e obter o texto original.*

Criptografia

Definição

*A **criptografia** é o estudo de métodos e técnicas para transformar um texto legível em algo ilegível, podendo reverter o processo e obter o texto original.*



Criptografia

Exemplo

Bianca deseja enviar uma mensagem $\boldsymbol{m}$ *para João*

Criptografia

Exemplo

Bianca deseja enviar uma mensagem $\boldsymbol{m}$ *para João*

- *Eles combinam entre si qual será a chave de criptação e de decodificação.*

Criptografia

Exemplo

Bianca deseja enviar uma mensagem $\boldsymbol{m}$ *para João*

- *Eles combinam entre si qual será a chave de criptação e de decodificação.*
- $c(m)$*: função de criptação*

Criptografia

Exemplo

Bianca deseja enviar uma mensagem $\boldsymbol{m}$ *para João*

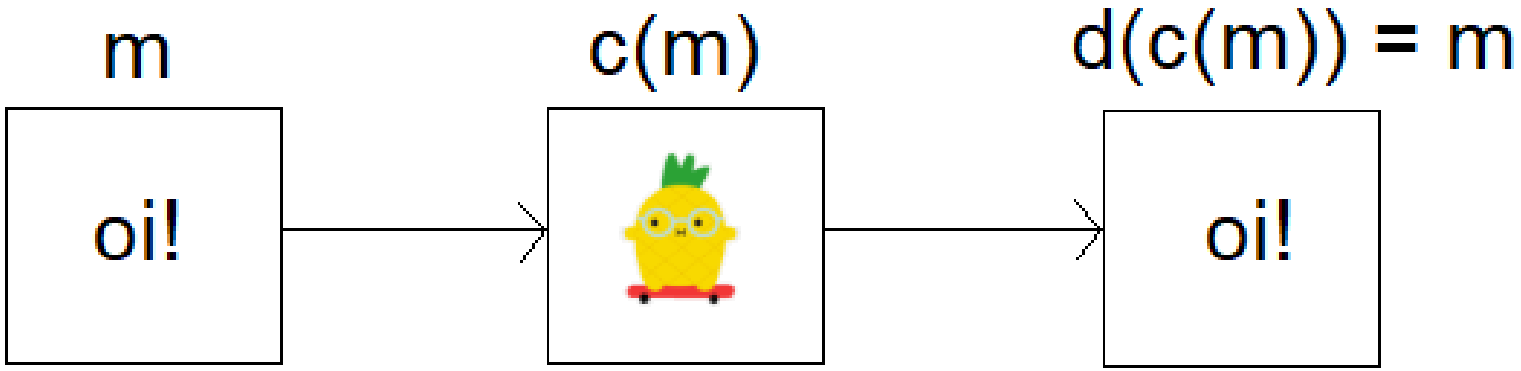
- *Eles combinam entre si qual será a chave de criptação e de decodificação.*
- $c(m)$*: função de criptação*
- $d(m)$*: função de decodificação*

Criptografia

Exemplo

Bianca deseja enviar uma mensagem $\boldsymbol{m}$ *para João*

- *Eles combinam entre si qual será a chave de criptação e de decodificação.*
- $c(m)$*: função de criptação*
- $d(m)$*: função de decodificação*



Criptografia

A criptografia não é usada apenas para mensagens escritas.

Criptografia

A criptografia não é usada apenas para mensagens escritas.

- Bitcoin

Criptografia

A criptografia não é usada apenas para mensagens escritas.

- Bitcoin

Criptografia

A criptografia não é usada apenas para mensagens escritas.

- Bitcoin

- Código Morse

Criptografia

A criptografia não é usada apenas para mensagens escritas.

- Bitcoin

- Código Morse

-... . – / ...- .. -. -.. — ... / / .- / ... . – .- -. .- / .- -.-. .- -..
. – .. -.-. .- / -.. — / -.-. ..- .-. ... — / -.. . / – .- - . – .- - ..
-.-. .- /

Código de César

Definição

A técnica de substituição ou transposição de letras é chamada de ***cifra****.*

Fato histórico: Em 50 a.C. na cidade de Roma, Júlio César usou uma cifra de substituição para proteger comunicações governamentais. Método conhecido como *Código de César*.

Código de César

Método: Desviar todas as letras, de uma mensagem, em três posições para a frente no alfabeto.

Código de César

Método: Desviar todas as letras, de uma mensagem, em três posições para a frente no alfabeto.

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

Código de César

Método: Desviar todas as letras, de uma mensagem, em três posições para a frente no alfabeto.

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

Exemplo: MATEMATICA

Código de César

Método: Desviar todas as letras, de uma mensagem, em três posições para a frente no alfabeto.

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

Exemplo: MATEMATICA $\rightarrow$ PDWHPDWLFD.

Código de César

Método: Desviar todas as letras, de uma mensagem, em três posições para a frente no alfabeto.

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

Exemplo: MATEMATICA $\rightarrow$ PDWHPDWLFD.
Fato histórico: O Código de César foi utilizado por muito tempo, e juntamente com alguns truques, permaneceu indecifrável por séculos.

Código de César

Pergunta:

Código de César

Pergunta: Como decifrar o código?

Código de César

Pergunta: Como decifrar o código?

Estudo da frequência das letras em textos

Código de César

Pergunta: Como decifrar o código?

Estudo da frequência das letras em textos

- *1º Passo:* Pegue um texto qualquer

Código de César

Pergunta: Como decifrar o código?

Estudo da frequência das letras em textos

- *1º Passo:* Pegue um texto qualquer
- *2º Passo:* Tabele a frequência de cada letra nele

Código de César

Pergunta: Como decifrar o código?

Estudo da frequência das letras em textos

- *1º Passo:* Pegue um texto qualquer
- *2º Passo:* Tabele a frequência de cada letra nele
- *3º Passo:* Tabele a frequência de cada letra do texto codificado

Código de César

Pergunta: Como decifrar o código?

Estudo da frequência das letras em textos

- *1º Passo:* Pegue um texto qualquer
- *2º Passo:* Tabele a frequência de cada letra nele
- *3º Passo:* Tabele a frequência de cada letra do texto codificado
- *4º Passo:* Associe as letras de mesma frequência dos passos 2 e 3.

Código César

Passos 1 e 2:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
14.63	1.04	3.88	4.99	12.57	1.02	1.30	1.28	6.18
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
0.40	0.02	2.78	4.74	5.05	10.73	2.52	1.20	6.53
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
1.81	4.74	4.63	1.67	0.01	0.21	0.01	0.47	

Código de César

Exemplo

Decifre a mensagem a seguir usando análise de frequência.

VHMD EHP YLQGR D VHPDQD DFDGHPLFD

Código de César

Exemplo

Decifre a mensagem a seguir usando análise de frequência.

VHMD EHP YLQGR D VHPDQD DFDGHPLFD

1º Passo:

Código de César

Exemplo

Decifre a mensagem a seguir usando análise de frequência.

VHMD EHP YLQGR D VHPDQD DFDGHPLFD

1º Passo: Feito

Código de César

Exemplo

Decifre a mensagem a seguir usando análise de frequência.

VHMD EHP YLQGR D VHPDQD DFDGHPLFD

1º Passo: Feito

2º Passo:

Código de César

Exemplo

Decifre a mensagem a seguir usando análise de frequência.

VHMD EHP YLQGR D VHPDQD DFDGHPLFD

1º Passo: Feito

2º Passo: Temos 28 caractéres.

Código de César

Exemplo

Decifre a mensagem a seguir usando análise de frequência.

VHMD EHP YLQGR D VHPDQD DFDGHPLFD

1º Passo: Feito

2º Passo: Temos 28 caractéres.

3º Passo: E a frequência de cada letra do texto codificado é dada pela tabela:

Código de César

Exemplo

Decifre a mensagem a seguir usando análise de frequência.

VHMD EHP YLQGR D VHPDQD DFDGHPLFD

1º Passo: Feito

2º Passo: Temos 28 caractéres.

3º Passo: E a frequência de cada letra do texto codificado é dada pela tabela:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	0	0	7	1	1	2	4	0	0	0	2	1
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	0	3	2	1	0	0	0	2	0	0	1	0

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u
- Tome $\begin{cases} D = a \\ H = e \end{cases}$

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u
- Tome $\begin{cases} D = a \\ H = e \end{cases}$
- Substituindo na mensagem:

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u
- Tome $\begin{cases} D = a \\ H = e \end{cases}$
- Substituindo na mensagem:

  VeMa EeP YLQGR a VePaQa aFaGePLFa

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u
- Tome $\begin{cases} D = a \\ H = e \end{cases}$
- Substituindo na mensagem:

  VeMa EeP YLQGR a VePaQa aFaGePLFa
- EeP

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u
- Tome $\begin{cases} D = a \\ H = e \end{cases}$
- Substituindo na mensagem:

  VeMa EeP YLQGR a VePaQa aFaGePLFa
- EeP
  $\Longrightarrow$ P = m ou P = r

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u
- Tome $\begin{cases} D = a \\ H = e \end{cases}$
- Substituindo na mensagem:

  VeMa EeP YLQGR a VePaQa aFaGePLFa
- EeP
  $\Longrightarrow$ P = m ou P = r
- Tomando P = m

Código de César

- As letras D e H aparecem com uma frequência de 7 e 4 vezes, respectivamente.
  $\Longrightarrow$ a, e, i, o , u
- Tome $\begin{cases} D = a \\ H = e \end{cases}$
- Substituindo na mensagem:

  VeMa EeP YLQGR a VePaQa aFaGePLFa
- EeP
  $\Longrightarrow$ P = m ou P = r
- Tomando P = m

  VeMa Eem YLQGR a VemaQa aFaGemLFa

Código de César

- VemaQa

Código de César

- VemaQa = semana

Código de César

- VemaQa = semana

$$\Longrightarrow \begin{cases} V = s \\ Q = n \end{cases}$$

Código de César

- VemaQa = semana

$$\Longrightarrow \begin{cases} V = s \\ Q = n \end{cases}$$

- Substituindo na mensagem:

Código de César

- VemaQa = semana

$$\Longrightarrow \begin{cases} V = s \\ Q = n \end{cases}$$

- Substituindo na mensagem:

seMa Eem YLQGR a semana aFaGemLFa

Código de César

- VemaQa = semana
$$\Longrightarrow \begin{cases} V = s \\ Q = n \end{cases}$$
- Substituindo na mensagem:

  seMa Eem YLQGR a semana aFaGemLFa
- É fácil ver que:

Código de César

- VemaQa = semana
$$\Longrightarrow \begin{cases} V = s \\ Q = n \end{cases}$$
- Substituindo na mensagem:

  seMa Eem YLQGR a semana aFaGemLFa
- É fácil ver que:

  seja bem YLQGR a semana aFaGemLFa

Código de César

- VemaQa = semana

$$\Longrightarrow \begin{cases} V = s \\ Q = n \end{cases}$$

- Substituindo na mensagem:

seMa Eem YLQGR a semana aFaGemLFa

- É fácil ver que:

seja bem YLQGR a semana aFaGemLFa

- $$\Longrightarrow \begin{cases} Y = v \\ L = i \\ C = d \\ R = o \\ M = j \end{cases}$$

Código de César

seja bem vindo a semana aFaGemiFa

Código de César

seja bem vindo a semana aFaGemiFa

- Mensagem descriptografada:

  Seja bem vindo a semana acadêmica

Código em Blocos

Definição

Esse método consiste em dividirmos a mensagem em blocos e embaralharmos suas letras. Daí o nome ***Código em Bloco*** *para este processo.*

Código em Blocos

Definição

Esse método consiste em dividirmos a mensagem em blocos e embaralharmos suas letras. Daí o nome ***Código em Bloco*** *para este processo.*

Exemplo

Criptografe a mensagem AMO A SEMANA DA MATEMÁTICA

Código em Blocos

Definição

Esse método consiste em dividirmos a mensagem em blocos e embaralharmos suas letras. Daí o nome ***Código em Bloco*** *para este processo.*

Exemplo

Criptografe a mensagem AMO A SEMANA DA MATEMÁTICA

1º Passo: Retire os espaços entre as palavras e adicione um A no final caso haja um número ímpar de letras

Código em Blocos

Definição

Esse método consiste em dividirmos a mensagem em blocos e embaralharmos suas letras. Daí o nome ***Código em Bloco*** *para este processo.*

Exemplo

Criptografe a mensagem AMO A SEMANA DA MATEMÁTICA

1º Passo: Retire os espaços entre as palavras e adicione um A no final caso haja um número ímpar de letras

2º Passo: Divida a frase em blocos de duas letras.

Código em Blocos

Definição

Esse método consiste em dividirmos a mensagem em blocos e embaralharmos suas letras. Daí o nome ***Código em Bloco*** *para este processo.*

Exemplo

Criptografe a mensagem AMO A SEMANA DA MATEMÁTICA

1º Passo: Retire os espaços entre as palavras e adicione um A no final caso haja um número ímpar de letras

2º Passo: Divida a frase em blocos de duas letras.

3º Passo: Em cada bloco, permute as letras de lugar.

Código em Blocos

Exemplo

4º Passo: Troque as posições dos blocos "ímpares" da seguinte forma: - primeiro com o último
- terceiro com o antepenúltimo
$\vdots$
e assim por diante, deixando os blocos "pares" parados.

Código em Blocos

Exemplo

1º Passo:

Código em Blocos

Exemplo

1º Passo:

$$AMOASEMANADAMATEMATICA$$

Código em Blocos

Exemplo

1º Passo:

$$AMOASEMANADAMATEMATICA$$

2º Passo:

Código em Blocos

Exemplo

1º Passo:

$$AMOASEMANADAMATEMATICA$$

2º Passo:

$$AM\ OA\ SE\ MA\ NA\ DA\ MA\ TE\ MA\ TI\ CA$$

Código em Blocos

Exemplo

1º Passo:

$$AMOASEMANADAMATEMATICA$$

2º Passo:

$$AM\ OA\ SE\ MA\ NA\ DA\ MA\ TE\ MA\ TI\ CA$$

3º Passo:

Código em Blocos

Exemplo

1º Passo:

$$AMOASEMANADAMATEMATICA$$

2º Passo:

$$AM\ OA\ SE\ MA\ NA\ DA\ MA\ TE\ MA\ TI\ CA$$

3º Passo:

$$MA\ AO\ ES\ AM\ AN\ AD\ AM\ ET\ AM\ IT\ AC$$

Código em Blocos

Exemplo

1º Passo:

$$AMOASEMANADAMATEMATICA$$

2º Passo:

$$AM\ OA\ SE\ MA\ NA\ DA\ MA\ TE\ MA\ TI\ CA$$

3º Passo:

$$MA\ AO\ ES\ AM\ AN\ AD\ AM\ ET\ AM\ IT\ AC$$

4º Passo:

Código em Blocos

Exemplo

1º Passo:

$$AMOASEMANADAMATEMATICA$$

2º Passo:

$$AM\ OA\ SE\ MA\ NA\ DA\ MA\ TE\ MA\ TI\ CA$$

3º Passo:

$$MA\ AO\ ES\ AM\ AN\ AD\ AM\ ET\ AM\ IT\ AC$$

4º Passo:

$$AC\ AO\ AM\ AM\ AM\ AD\ AN\ ET\ ES\ IT\ MA$$

Código em Blocos

Exemplo

Justapondo os blocos novamente, temos a seguinte mensagem criptografada:

Código em Blocos

Exemplo

Justapondo os blocos novamente, temos a seguinte mensagem criptografada:

$$ACAOAMAMAMADANETESITMA$$

Código em Blocos

Exemplo

Justapondo os blocos novamente, temos a seguinte mensagem criptografada:

$$ACAOAMAMAMADANETESITMA$$

Observação. O código em bloco é um exemplo de criptografia de chave privada.

Pergunta.

Código em Blocos

Exemplo

Justapondo os blocos novamente, temos a seguinte mensagem criptografada:

$$ACAOAMAMAMADANETESITMA$$

Observação. O código em bloco é um exemplo de criptografia de chave privada.

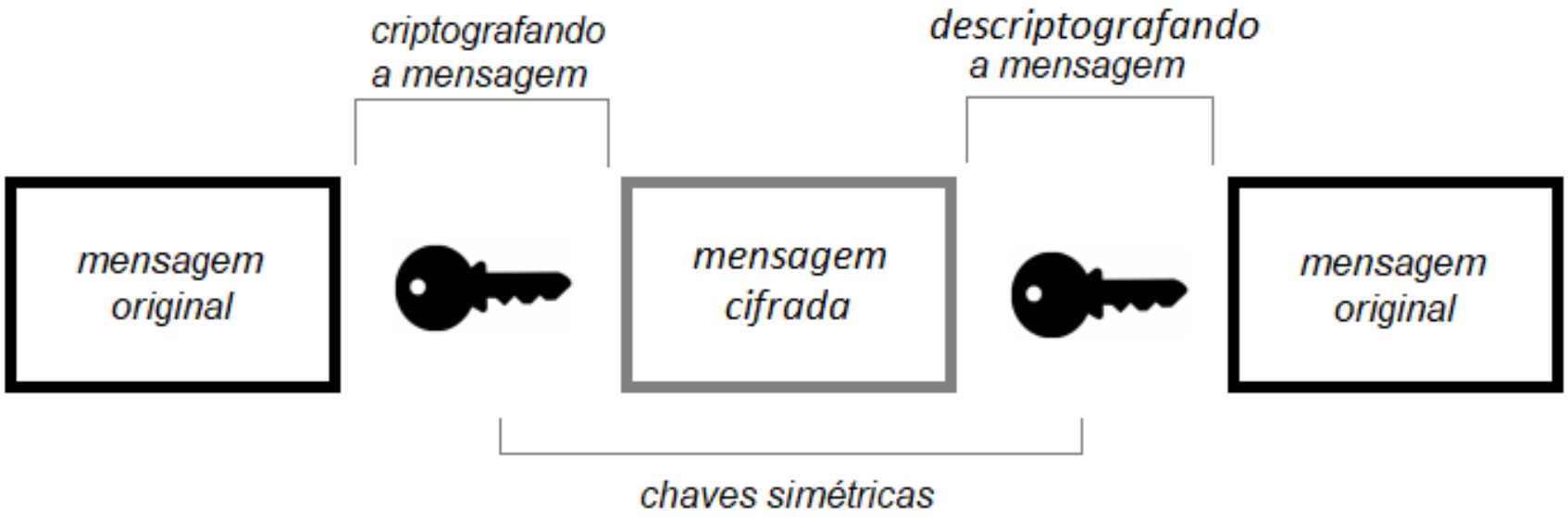
Pergunta. Mas o que é chave privada?

Chave Privada x Chave Pública

A criptografia de **chave privada** utiliza apenas uma chave. A mensagem é criptografada com essa chave pelo emissor, e descriptografada com a mesma, pelo receptor.

Chave Privada x Chave Pública

A criptografia de **chave privada** utiliza apenas uma chave. A mensagem é criptografada com essa chave pelo emissor, e descriptografada com a mesma, pelo receptor.



Chave Privada x Chave Pública

Observação. Durante o processo de envio da mensagem, um terceiro pode interceptá-la e descobrir a chave, já que é apenas uma.

Chave Privada x Chave Pública

Observação. Durante o processo de envio da mensagem, um terceiro pode interceptá-la e descobrir a chave, já que é apenas uma.

Solução. Chave Pública.

Chave Privada x Chave Pública

Observação. Durante o processo de envio da mensagem, um terceiro pode interceptá-la e descobrir a chave, já que é apenas uma.

Solução. Chave Pública.

Exemplo

Digamos que Bianca e João desejam se comunicar secretamente. Para tal, Bianca possui um cadeado $\boldsymbol{B}$*, e para abri-lo, uma chave* $\boldsymbol{b}$*. Analogamente, João possui um cadeado* $\boldsymbol{J}$ *e uma chave* $\boldsymbol{j}$*.*

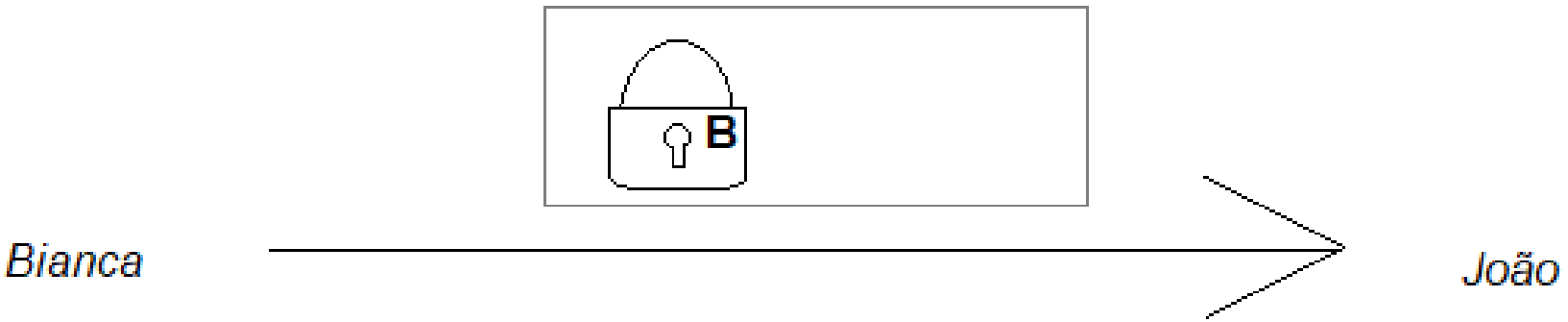
Chave Privada x Chave Pública

Observação. Durante o processo de envio da mensagem, um terceiro pode interceptá-la e descobrir a chave, já que é apenas uma.

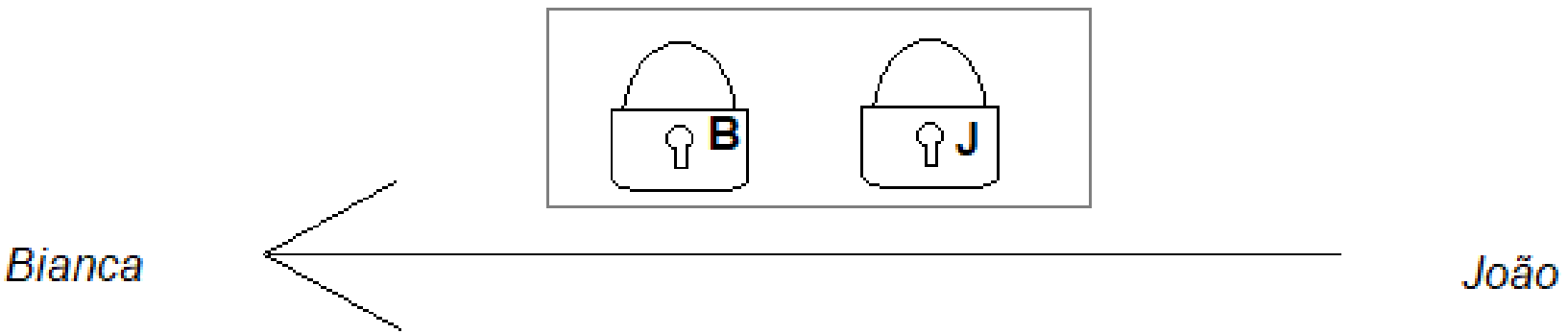
Solução. Chave Pública.

Exemplo

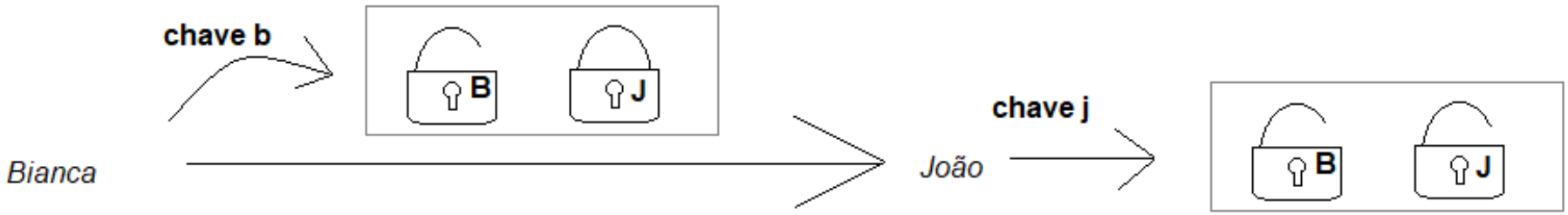
Digamos que Bianca e João desejam se comunicar secretamente. Para tal, Bianca possui um cadeado $\boldsymbol{B}$*, e para abri-lo, uma chave* $\boldsymbol{b}$*. Analogamente, João possui um cadeado* $\boldsymbol{J}$ *e uma chave* $\boldsymbol{j}$*.*



Chave Privada x Chave Pública



Chave Privada x Chave Pública



Criptografia em Matrizes

Um outro método de **criptografia é via matrizes**.

Criptografia em Matrizes

Um outro método de **criptografia é via matrizes**.
Chave. Uma *matriz quadrada* invertível.

Criptografia em Matrizes

Um outro método de **criptografia é via matrizes**.
Chave. Uma *matriz quadrada* invertível.
Método:

Criptografia em Matrizes

Um outro método de **criptografia é via matrizes**.
Chave. Uma *matriz quadrada* invertível.
Método:
1º Passo: Converter cada letra em um número, e separá-los em vetores coluna.

Criptografia em Matrizes

Um outro método de **criptografia é via matrizes**.
Chave. Uma *matriz quadrada* invertível.
Método:
1º Passo: Converter cada letra em um número, e separá-los em vetores coluna.
2º Passo: Para criptografar a mensagem, faremos o produto da matriz chave por cada vetor, afim de encontrar um novo vetor coluna.

Criptografia em Matrizes

Um outro método de **criptografia é via matrizes**.
Chave. Uma *matriz quadrada* invertível.
Método:
1º Passo: Converter cada letra em um número, e separá-los em vetores coluna.
2º Passo: Para criptografar a mensagem, faremos o produto da matriz chave por cada vetor, afim de encontrar um novo vetor coluna.
3º Passo: Por fim, converteremos novamente cada número na letra correspondente na tabela de conversão, e encontraremos a mensagem criptografada.

Código em Matrizes

Exemplo

Considere a mensagem:

$$AMO\ MATEMÁTICA$$

Código em Matrizes

Exemplo

Considere a mensagem:

AMO MATEMÁTICA

Iremos usar a seguinte tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Código em Matrizes

1º Passo:

Código em Matrizes

1º Passo: Cada letra será associada ao número de sua posição no alfabeto

Código em Matrizes

1º Passo: Cada letra será associada ao número de sua posição no alfabeto

$$AMO\ MATEMATICA$$

Código em Matrizes

1º Passo: Cada letra será associada ao número de sua posição no alfabeto

$$AMO\ MATEMATICA$$

$$A\ M\ O\ M\ A\ T\ E\ M\ A\ T\ I\ C\ A$$

Código em Matrizes

1º Passo: Cada letra será associada ao número de sua posição no alfabeto

$$AMO\ MATEMATICA$$

$$A\ M\ O\ M\ A\ T\ E\ M\ A\ T\ I\ C\ A$$

$$1\ 13\ 15\ 13\ 1\ 20\ 5\ 13\ 1\ 20\ 9\ 3\ 1$$

Código em Matrizes

1º Passo: Cada letra será associada ao número de sua posição no alfabeto

$$AMO\ MATEMATICA$$

$$A\ M\ O\ M\ A\ T\ E\ M\ A\ T\ I\ C\ A$$

$$1\ 13\ 15\ 13\ 1\ 20\ 5\ 13\ 1\ 20\ 9\ 3\ 1$$

$$\underbrace{\begin{pmatrix} 1 \\ 13 \end{pmatrix}}_{v_1} \underbrace{\begin{pmatrix} 15 \\ 13 \end{pmatrix}}_{v_2} \underbrace{\begin{pmatrix} 1 \\ 20 \end{pmatrix}}_{v_3} \underbrace{\begin{pmatrix} 5 \\ 13 \end{pmatrix}}_{v_4} \underbrace{\begin{pmatrix} 1 \\ 20 \end{pmatrix}}_{v_5} \underbrace{\begin{pmatrix} 9 \\ 3 \end{pmatrix}}_{v_6} \underbrace{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{v_7}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C)$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} \; C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} \; C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} \; C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} \; C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} \; C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} \; C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} \quad C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} \quad C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} \quad C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} \quad C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} \quad C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} \quad C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} \quad C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix}$$

Código em Matrizes

2º Passo: Escolhemos a seguinte matriz:

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \implies det(C) = 3 \cdot 1 - 2 \cdot 2 = -1 \neq 0$$

Tendo escolhida nossa chave, multiplicaremos a mesma por cada vetor coluna, resultando em:

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

3º Passo:

- $27 = 26 + \mathbf{1} = A$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

3º Passo:

- $27 = 26 + \mathbf{1} = A$
- $41 = 26 + \mathbf{15} = O$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

3º Passo:

- $27 = 26 + \mathbf{1} = A$
- $41 = 26 + \mathbf{15} = O$
- $41 = 26 + \mathbf{15} = O$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

3º Passo:

- $27 = 26 + \mathbf{1} = A$
- $41 = 26 + \mathbf{15} = O$
- $41 = 26 + \mathbf{15} = O$
- $69 = 26 \cdot 2 + \mathbf{17} = Q$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

3º Passo:

- $27 = 26 + \mathbf{1} = A$
- $41 = 26 + \mathbf{15} = O$
- $41 = 26 + \mathbf{15} = O$
- $69 = 26 \cdot 2 + \mathbf{17} = Q$
- $41 = 26 + \mathbf{15} = O$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

3º Passo:

- $27 = 26 + \mathbf{1} = A$
- $41 = 26 + \mathbf{15} = O$
- $41 = 26 + \mathbf{15} = O$
- $69 = 26 \cdot 2 + \mathbf{17} = Q$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$

Código em Matrizes

$$C \cdot v_1 = \begin{pmatrix} 27 \\ 41 \end{pmatrix} C \cdot v_2 = \begin{pmatrix} 41 \\ 69 \end{pmatrix} C \cdot v_3 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_4 = \begin{pmatrix} 31 \\ 49 \end{pmatrix}$$

$$C \cdot v_5 = \begin{pmatrix} 41 \\ 62 \end{pmatrix} C \cdot v_6 = \begin{pmatrix} 15 \\ 27 \end{pmatrix} C \cdot v_7 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

3º Passo:

- $27 = 26 + \mathbf{1} = A$
- $41 = 26 + \mathbf{15} = O$
- $41 = 26 + \mathbf{15} = O$
- $69 = 26 \cdot 2 + \mathbf{17} = Q$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$
- $31 = 26 + \mathbf{5} = E$

Código em Matrizes

- $49 = 26 + \mathbf{23} = W$
- $41 = 26 + \mathbf{15} = O$

Código em Matrizes

- $49 = 26 + \mathbf{23} = W$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$

Código em Matrizes

- $49 = 26 + \mathbf{23} = W$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$
- $\mathbf{15} = O$

Código em Matrizes

- $49 = 26 + \mathbf{23} = W$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$
- $\mathbf{15} = O$
- $27 = 26 + \mathbf{1} = A$

Código em Matrizes

- $49 = 26 + \mathbf{23} = W$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$
- $\mathbf{15} = O$
- $27 = 26 + \mathbf{1} = A$
- $\mathbf{3} = C$

Código em Matrizes

- $49 = 26 + \mathbf{23} = W$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$
- $\mathbf{15} = O$
- $27 = 26 + \mathbf{1} = A$
- $\mathbf{3} = C$
- $\mathbf{5} = E$

Assim a mensagem criptograda é:

Código em Matrizes

- $49 = 26 + \mathbf{23} = W$
- $41 = 26 + \mathbf{15} = O$
- $62 = 26 \cdot 2 + \mathbf{10} = J$
- $\mathbf{15} = O$
- $27 = 26 + \mathbf{1} = A$
- $\mathbf{3} = C$
- $\mathbf{5} = E$

Assim a mensagem criptograda é:

$$AOOQOJEWOJOACE$$

Código em Matrizes

- Descriptografando a mensagem

$$AOOQOJEWOJOACE$$

Código em Matrizes

- Descriptografando a mensagem

$$AOOQOJEWOJOACE$$

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

Código em Matrizes

- Descriptografando a mensagem

$$AOOQOJEWOJOACE$$

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

$$C^{-1} = \frac{1}{(3 \cdot 1) - (2 \cdot 2)} \cdot \begin{pmatrix} 3 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -3 & 2 \\ 2 & -1 \end{pmatrix}$$

Código em Matrizes

$$2\ C^{-1} \cdot \begin{pmatrix} 27 \\ 41 \end{pmatrix} = \begin{pmatrix} 1 \\ 13 \end{pmatrix}$$

Código em Matrizes

$$2\ C^{-1} \cdot \begin{pmatrix} 27 \\ 41 \end{pmatrix} = \begin{pmatrix} 1 \\ 13 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 41 \\ 69 \end{pmatrix} = \begin{pmatrix} 15 \\ 13 \end{pmatrix}$$

Código em Matrizes

$$2\ C^{-1} \cdot \begin{pmatrix} 27 \\ 41 \end{pmatrix} = \begin{pmatrix} 1 \\ 13 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 41 \\ 69 \end{pmatrix} = \begin{pmatrix} 15 \\ 13 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 41 \\ 62 \end{pmatrix} = \begin{pmatrix} 1 \\ 20 \end{pmatrix}$$

Código em Matrizes

$$2\ C^{-1} \cdot \begin{pmatrix} 27 \\ 41 \end{pmatrix} = \begin{pmatrix} 1 \\ 13 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 41 \\ 69 \end{pmatrix} = \begin{pmatrix} 15 \\ 13 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 41 \\ 62 \end{pmatrix} = \begin{pmatrix} 1 \\ 20 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 31 \\ 49 \end{pmatrix} = \begin{pmatrix} 5 \\ 13 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 41 \\ 62 \end{pmatrix} = \begin{pmatrix} 1 \\ 20 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 15 \\ 27 \end{pmatrix} = \begin{pmatrix} 9 \\ 3 \end{pmatrix}$$

$$C^{-1} \cdot \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Código em Matrizes

Voltando a tabela, encontramos as letras da codificação, voltando a mensagem original.

1	13	15	13	1	20	5	13	1	20	9	13	1	1
A	M	O	M	A	T	E	M	A	T	I	C	A	A

Exercícios

- Cifre o seu nome completo.
- Use a cifra de substituição com -8 posições para cifrar a mensagem: “O Naruto pode ser um pouco duro às vezes”.
- Use a cifra de César para criptografar a mensagem “Aprender Matemática fica mais fácil quando gostamos dela”.
- Utilizando o algoritmo de criptografia em blocos, decifre a mensagem abaixo:

AHIUSLIVOANEANASHECIQA

Exercícios

- Verifique se as matrizes abaixo poderiam ser utilizadas como chave para codificar mensagens:
  2
  a) $A = \begin{pmatrix} -1 & 3 \\ 2 & 2 \end{pmatrix}$
  b) $B = \begin{pmatrix} -3 & 5 \\ -1 & 2 \end{pmatrix}$
  c) $C = \begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}$
  d) $D = \begin{pmatrix} 8 & 4 \\ 2 & 1 \end{pmatrix}$
- Utilizando a chave $C = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$ e a tabela de conversão apresentada no capítulo, codifique a mensagem FIBONACCI.

Muito Obrigada!

Referências

COUTINHO, S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro, IMPA/SBM, 1997.

.