

# MATEMÁTICA DISCRETA 2

## Aula 17

### Aplicações – Congruência Criptografia RSA

*Cristiane Loesch*

Brasília  
2025

# Aplicações de Congruência

## ISBN (International Standard Book Number)

- padrão internacional de numeração de livro
- ISBN-10 (até 2007) e ISBN-13 (atualmente)

The diagram shows the breakdown of the ISBN 817525766-0 into its constituent parts: Grupo (8), Editor (17), Item (525), and Dígito de verificação (6). Below this, the equivalent 13-digit EAN-13 barcode is shown, with its components: EAN (9), Grupo (788), Editor (175), Item (257), and Dígito de verificação (665). The text explains that the ISBN consists of 10 digits and its equivalent in 13 digits, along with the respective barcode, where the verification digit differs from each of the other digits.

Os componentes de um ISBN de 10 dígitos e do equivalente em 13 dígitos e o respetivo código de barras, onde é possível observar o dígito de verificação diferente de cada um.

# Aplicações de Congruência

ISBN (International Standard Book Number)

ISBN-10 e a Congruência Modular:

- utilizada no cálculo do BIT de verificação;
- BIT de verificação:
  - 11 dígitos possíveis  
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X (representando o no. 10)
- Cálculo:
  - os 9 primeiros dígitos do ISBN são multiplicados por  
10, 9, 8, 7, 6, 5, 4, 3 e 2  
respectivamente;
  - seus produtos são, então, adicionados obtendo-se um número y;
  - o dígito verificador é então obtido fazendo-se:

$$d + y \equiv 0 \pmod{11}$$

# Aplicações de Congruência

ISBN (International Standard Book Number)

**EXEMPLO 1:** ISBN 0 – 673 – 38582 – D

# Aplicações de Congruência

ISBN (International Standard Book Number)

**EXEMPLO 1:** ISBN 0 – 673 – 38582 – D

$$y = 10 \cdot 0 + 9 \cdot 6 + 8 \cdot 7 + 7 \cdot 3 + 6 \cdot 3 + 5 \cdot 8 + 4 \cdot 5 + 3 \cdot 8 + 2 \cdot 2$$

# Aplicações de Congruência

ISBN (International Standard Book Number)

**EXEMPLO 1:** ISBN 0 – 673 – 38582 – D

$$y = 10 \cdot 0 + 9 \cdot 6 + 8 \cdot 7 + 7 \cdot 3 + 6 \cdot 3 + 5 \cdot 8 + 4 \cdot 5 + 3 \cdot 8 + 2 \cdot 2$$

$$y = 237$$

# Aplicações de Congruência

ISBN (International Standard Book Number)

**EXEMPLO 1:** ISBN 0 – 673 – 38582 – D

$$y = 10 \cdot 0 + 9 \cdot 6 + 8 \cdot 7 + 7 \cdot 3 + 6 \cdot 3 + 5 \cdot 8 + 4 \cdot 5 + 3 \cdot 8 + 2 \cdot 2$$

$$y = 237$$

$$D + 237 \equiv 0 \pmod{11}$$

# Aplicações de Congruência

ISBN (International Standard Book Number)

**EXEMPLO 1:** ISBN 0 – 673 – 38582 – D

$$y = 10 \cdot 0 + 9 \cdot 6 + 8 \cdot 7 + 7 \cdot 3 + 6 \cdot 3 + 5 \cdot 8 + 4 \cdot 5 + 3 \cdot 8 + 2 \cdot 2$$

$$y = 237$$

$$D + 237 \equiv 0 \pmod{11}$$

$$5 + 237 \equiv 0 \pmod{11}$$

$$242 \equiv 0 \pmod{11}$$

logo, ISBN 0 – 673 – 38582 – 5



# Aplicações de Congruência

ISBN (International Standard Book Number)

**EXEMPLO 1:** ISBN 0 – 673 – 38582 – D

$$y = 10 \cdot 0 + 9 \cdot 6 + 8 \cdot 7 + 7 \cdot 3 + 6 \cdot 3 + 5 \cdot 8 + 4 \cdot 5 + 3 \cdot 8 + 2 \cdot 2$$

$$y = 237$$

$$D + 237 \equiv 0 \pmod{11}$$

$$5 + 237 \equiv 0 \pmod{11}$$

$$242 \equiv 0 \pmod{11}$$

logo, ISBN 0 – 673 – 38582 – 5

**EXEMPLO 2:** ISBN 0 – 321 – 30515 – D

# Aplicações de Congruência

ISBN (International Standard Book Number)

**EXEMPLO 1:** ISBN 0 – 673 – 38582 – D

$$y = 10 \cdot 0 + 9 \cdot 6 + 8 \cdot 7 + 7 \cdot 3 + 6 \cdot 3 + 5 \cdot 8 + 4 \cdot 5 + 3 \cdot 8 + 2 \cdot 2$$

$$y = 237$$

$$D + 237 \equiv 0 \pmod{11}$$

$$5 + 237 \equiv 0 \pmod{11}$$

$$242 \equiv 0 \pmod{11}$$

logo, ISBN 0 – 673 – 38582 – 5

**EXEMPLO 2:** ISBN 0 – 321 – 30515 – D

$$Y = 10 \cdot 0 + 9 \cdot 3 + 8 \cdot 2 + 7 \cdot 1 + 6 \cdot 3 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 1 + 2 \cdot 5 = 101$$

$$D + 101 \equiv 0 \pmod{11} \rightarrow D = 9$$

# Aplicações de Congruência

## CPF (Cadastro de Pessoa Física)

→ Por meio da Lei 4.862 de 29 de novembro de 1965, foi instituído o Registro das Pessoas Físicas para que a administração tributária nacional pudesse coletar as informações das Pessoas Físicas que eram obrigadas a apresentar a declaração de rendimentos e bens. Em 1968, pelo Decreto-Lei 401, de 30 de dezembro de 1968, esse Registro das Pessoas Físicas foi transformado no cadastro de pessoas físicas.



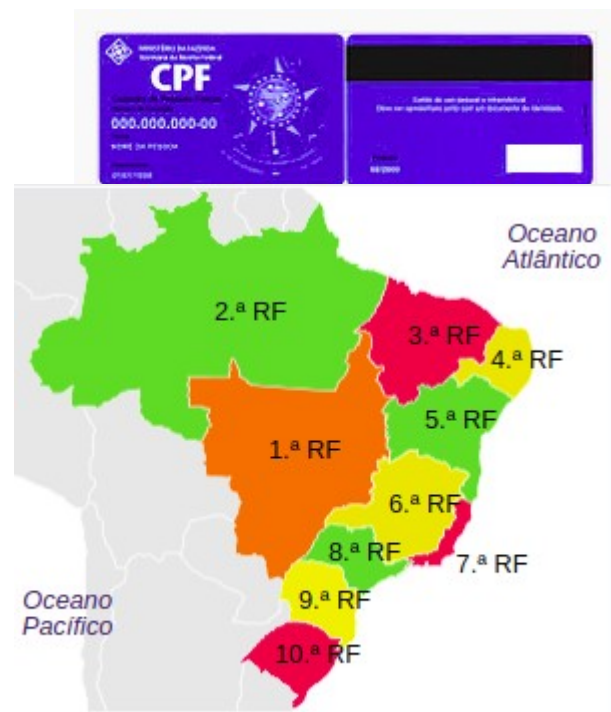
# Aplicações de Congruência

## CPF (Cadastro de Pessoa Física)

- possui 11 dígitos
  - 8 primeiros dígitos aleatórios\*
  - 9º dígito é referente à região de fiscal

1: Distrito Federal (DF), Goiás (GO), Mato Grosso do Sul (MS), Mato Grosso (MT) e Tocantins (TO);  
2: Acre (AC), Amazonas (AM), Amapá (AP), Pará (PA), Rondônia (RO) e Roraima (RR);  
3: Ceará (CE), Maranhão (MA) e Piauí (PI);  
4: Alagoas (AL), Paraíba (PB), Pernambuco (PE) e Rio Grande do Norte (RN);  
5: Bahia (BA) e Sergipe (SE);  
6: Minas Gerais (MG);  
7: Espírito Santo (ES) e Rio de Janeiro (RJ);  
8: São Paulo (SP);  
9: Paraná (PR) e Santa Catarina (SC);  
0: Rio Grande do Sul (RS).

- 10º e 11º dígitos são verificadores



FONTE: Wikipédia

# Aplicações de Congruência

CPF (Cadastro de Pessoa Física)

CPF e a Congruência Modular:

→ utilizada no cálculo dos dígitos de verificação ;

CPF:

abc. def. ghi -  $D_1D_2$

$$1a + 2b + 3c + 4d + 5e + 6f + 7g + 8h + 9i = X$$

$$D_1 \equiv X \pmod{11}$$

$$0a + 1b + 2c + 3d + 4e + 5f + 6g + 7h + 8i + 9D_1 = Y$$

$$D_2 \equiv Y \pmod{11}$$

# Aplicações de Congruência

CPF (Cadastro de Pessoa Física)

EXEMPLO:

012.345.678 -  $D_1D_2$

$$1 \cdot 0 + 2 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + 5 \cdot 4 + 6 \cdot 5 + 7 \cdot 6 + 8 \cdot 7 + 9 \cdot 8 = 240$$

$$D_1 \equiv 240 \pmod{11}$$

$$9 \equiv 240 \pmod{11}$$

$$0 \cdot 0 + 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 + 7 \cdot 7 + 8 \cdot 8 + 9 \cdot 9 = 285$$

$$D_2 \equiv 285 \pmod{11}$$

$$10 \equiv 285 \pmod{11}$$

$$D_2 = 0$$

por convenção quando o cálculo tem resto 10, este deverá ser substituído por zero

012.345.678 - 90

# Criptografia

*Cryptos* = secreto, oculto (grego)

# Criptografia





# Criptografia

A LÍNGUA  
DO P



Pêvo pêcê pêco pênehe pêce pea pêlin pêgua pêdo pêpê ?

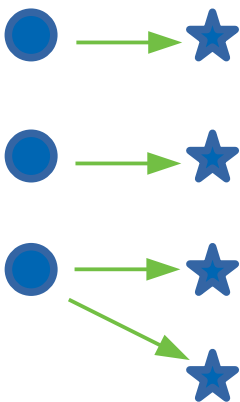
# Criptografia

- Utiliza a teoria dos números para codificar e decodificar mensagens
- Processo de transformação, através de uma chave secreta, de informação legível (mensagem) em informação ilegível (criptograma) possibilitando a reversão do processo.
- Exigências:
  - Reversibilidade
    - ao codificar uma mensagem tem que ser possível decodificá-la
  - Receptor tenha a chave
    - para decodificar

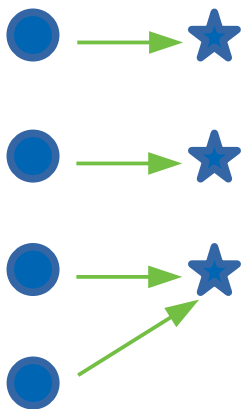
Codificar uma mensagem é pegar sua versão original e transformar num outro conjunto de informações que não possa ser identificado por qualquer pessoa apenas pelo receptor

# Criptografia

Obs: Garantir que não há ambiguidade

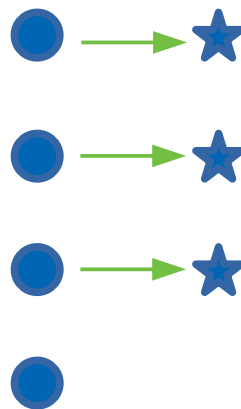


Não pode!



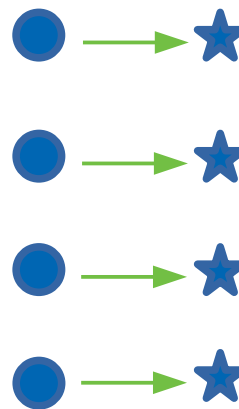
Não pode!

no retorno vai para  
onde?



Não pode!

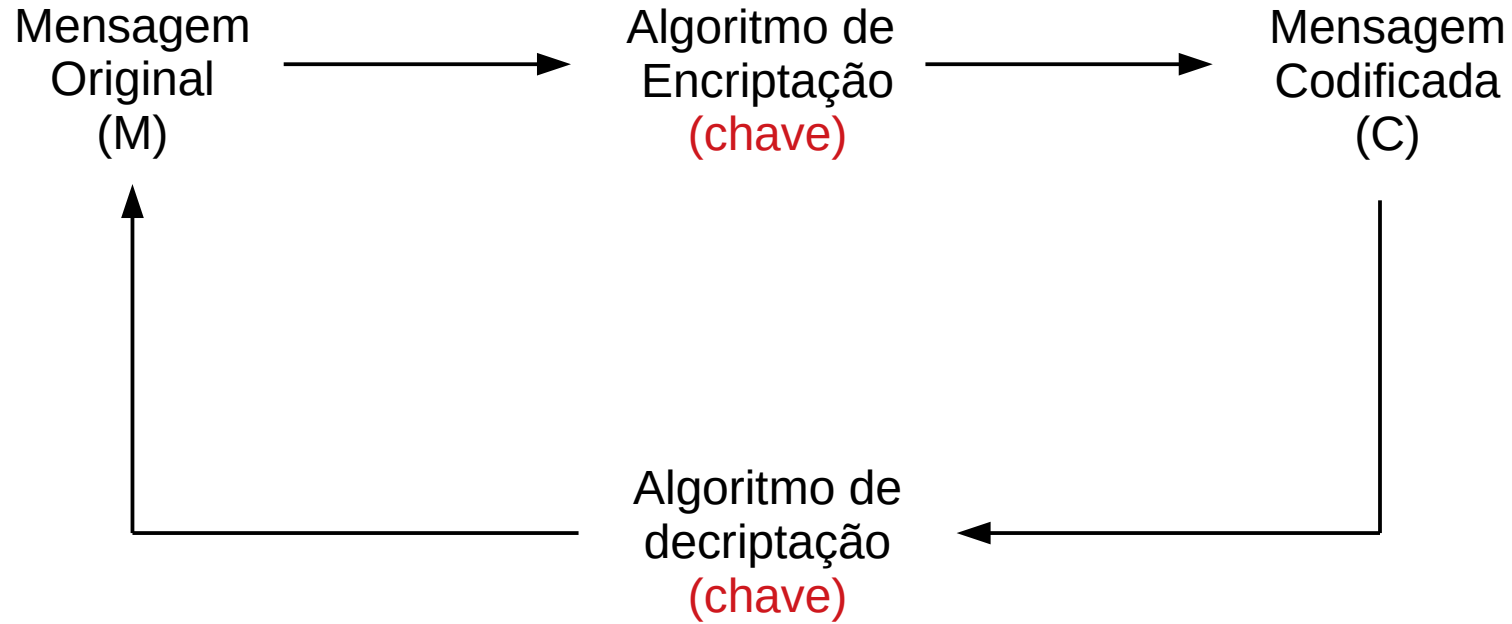
Não transforma tudo.



OK!

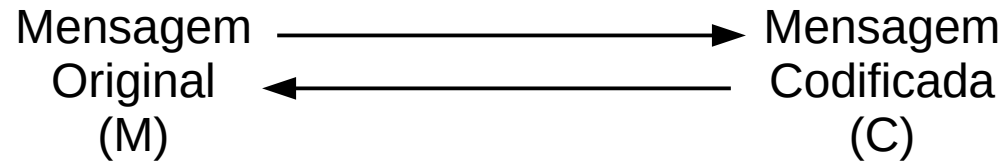
Função Bijetora

# Criptografia



# Criptografia

- Principal aplicação
  - sistemas de segurança
    - confiabilidade
    - integridade
    - autenticidade
- Criptografar



# Criptografia

## CLASSIFICAÇÃO:

### 1) Quanto ao tipo de operações

#### a) Substituição

→ cada elemento do texto original (bit, letra, etc) é mapeado em um elemento no texto cifrado

#### b) Transposição

→ quando os elementos do texto original tem sua posição alterada no texto cifrado

# Criptografia

## CLASSIFICAÇÃO:

### 1) Quanto ao tipo de operações

#### a) Substituição

- cada elemento do texto original (bit, letra, etc) é mapeado em um elemento no texto cifrado

#### b) Transposição

- quando os elementos do texto original tem sua posição alterada no texto cifrado

**EXEMPLO:** separa em duas colunas, lê a primeira e em seguida a segunda

Mensagem: TROQUEASCAIXAS

# Criptografia

## CLASSIFICAÇÃO:

### 1) Quanto ao tipo de operações

#### a) Substituição

- cada elemento do texto original (bit, letra, etc) é mapeado em um elemento no texto cifrado

#### b) Transposição

- quando os elementos do texto original tem sua posição alterada no texto cifrado

**EXEMPLO:** separa em duas colunas, lê a primeira e em seguida a segunda

Mensagem: TROQUEASCAIXAS

T O U A C I A  
R Q E S A X S



# Criptografia

## CLASSIFICAÇÃO:

### 1) Quanto ao tipo de operações

#### a) Substituição

→ cada elemento do texto original (bit, letra, etc) é mapeado em um elemento no texto cifrado

#### b) Transposição

→ quando os elementos do texto original tem sua posição alterada no texto cifrado

**EXEMPLO:** separa em duas colunas, lê a primeira e em seguida a segunda

Mensagem: TROQUEASCAIXAS

Criptograma:

T O U A C I A  
R Q E S A X S

—————→

TOUACIARQESAXS

cifra rail fence em Python    mensagem: atacaremos ao amanhecer.

```
| | | | | | | | | | | | | | | | | | - 1
| | | | | | | | | | | | | | | | | | - 2
| | | | | | | | | | | | | | | | | | - 3
| | | | | | | | | | | | | | | | | | - 4
```

```
| a | | | | | | | | | | | | | | | | | | - 1
| | t | | | | | | | | | | | | | | | | | - 2
| | | a | | | | | | | | | | | | | | | | - 3
| | | | c | | | | | | | | | | | | | | | | - 4
```

```
| a | | | | | e | | | | | | | | | | | | | - 1
| | t | | | | r | | | | | | | | | | | | | - 2
| | | a | a | | | | | | | | | | | | | | - 3
| | | | c | | | | | | | | | | | | | | | - 4
```

```
| a | | | | | e | | | | | a | | | | | c | | | - 1 - aeac
| | t | | | | r | m | | | | o | m | | | | e | e | - 2 - trmomee
| | | a | a | | | | o | a | | | | a | h | | | | r | - 3 - aaoaahr
| | | | c | | | | | s | | | | | n | | | | | | - 4 - csn
```

# Criptografia

A chave privada fica com o proprietário da mensagem! Ele é o único capaz de decodificá-la

## CLASSIFICAÇÃO:

### 2) Quanto ao número de chaves

#### a) Simétrica

→ convencional ou de chave privada

- Remetente e destinatário utilizam uma única chave  
→ chave compartilhada

#### b) Assimétrica

→ de chave pública ou dupla

- Remetente e destinatário utilizam chaves diferentes  
→ chave privada → conhecida só pelo dono  
→ chave pública → supõem-se que todos possam conhecê-la
- Mais lento, porém mais seguro que o simétrico

A chave pública esta a disposição de qualquer pessoa e é utilizada para codificar uma mensagem

# Criptografia

## CLASSIFICAÇÃO:

### 3) Quanto à forma de processamento

#### a) por bloco

→ processa um bloco de cada vez produzindo assim um bloco de saída de cada vez

#### b) por stream (fluxo)

→ processa os elementos de entrada de forma contínua  
( bit por bit , byte por byte)

# Técnicas Clássicas

CONVENCIONAL

$$C = E \cdot k(M)$$

$$M = D \cdot k(C)$$

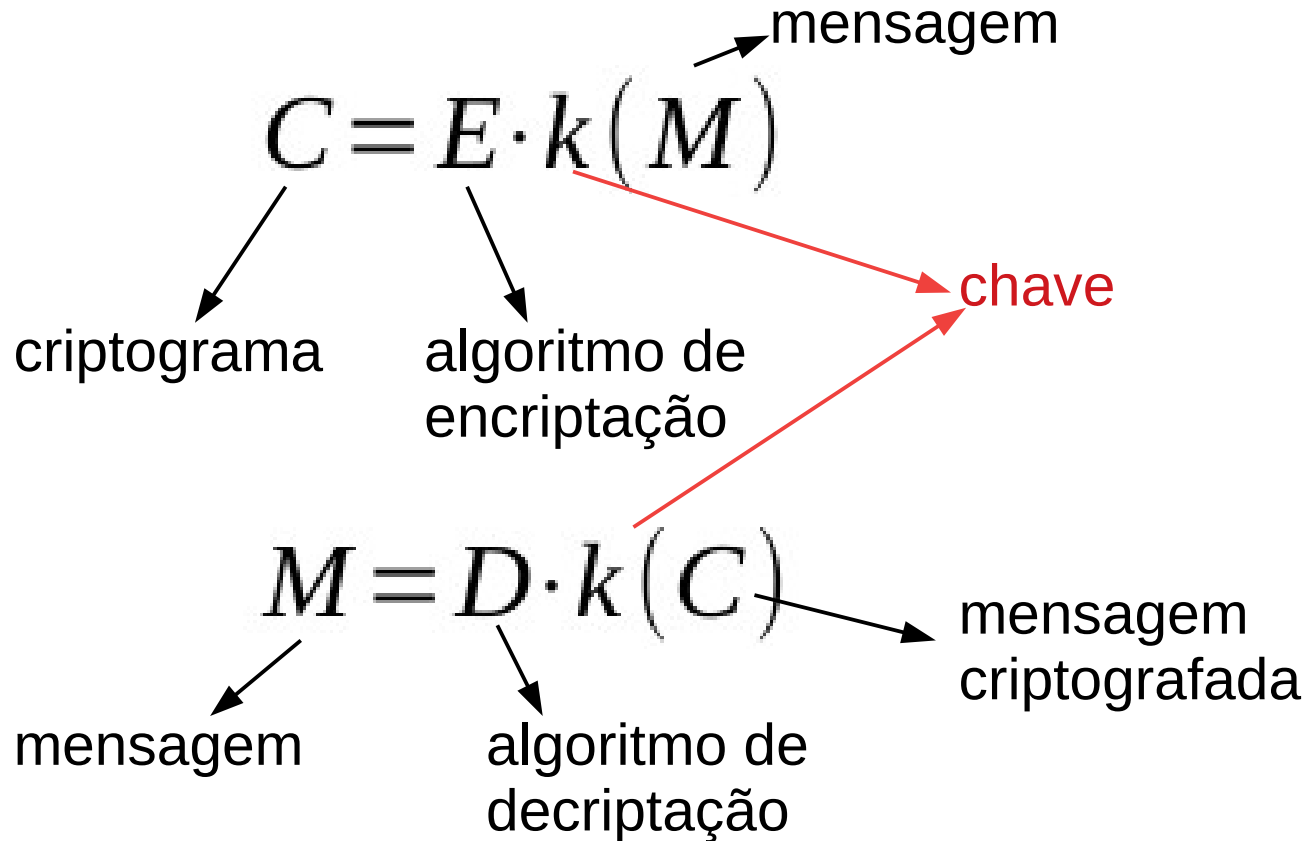
# Técnicas Clássicas

## CONVENCIONAL

Importante:

Manter a chave  
secreta!!

Um canal seguro  
para distribuir a  
chave.



### CONVENCIONAL

#### **EXEMPLOS:**

- TRANSPOSIÇÃO DE COLUNAS
- CIFRA DE CÉSAR
- CIFRA MONOALFABÉTICA
- CIFRA POLIALFABÉTICA (tipo batalha naval)
- ETC

### CONVENCIONAL **CIFRA DE CÉSAR**

O texto original é cifrado a partir da troca de cada uma das letras por outra letra do alfabeto.

$$C = E(p) = (P + k) \bmod 26$$

$$P = D(p) = (C - k) \bmod 26$$




### CONVENCIONAL **CIFRA DE CÉSAR**

#### **EXEMPLO:**

Original: *A B C D E F G ... Z*  
Cifrado: *D E F G H I J ... C*

Regra: 3 posições à frente




FESTA CONFIRMADA NO PROXIMO SABADO A NOITE

### CONVENCIONAL **CIFRA DE CÉSAR**

#### **EXEMPLO:**

Original: *A B C D E F G ... Z*  
Cifrado: *D E F G H I J ... C*

Regra: 3 posições à frente



FESTA CONFIRMADA NO PROXIMO SABADO A NOITE  
IHVWD FRQILUPDGD QR SURALPR VDEDGR D QRLWH

## Técnicas Clássicas

### CONVENCIONAL **CIFRA DE CÉSAR**

#### **EXEMPLO:**

Original:	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>...</i>	<i>Z</i>	}
Cifrado:	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>...</i>	<i>C</i>	
Regra: 3 posições à frente										

SUA VEZ!

*CESAR*

## Técnicas Clássicas

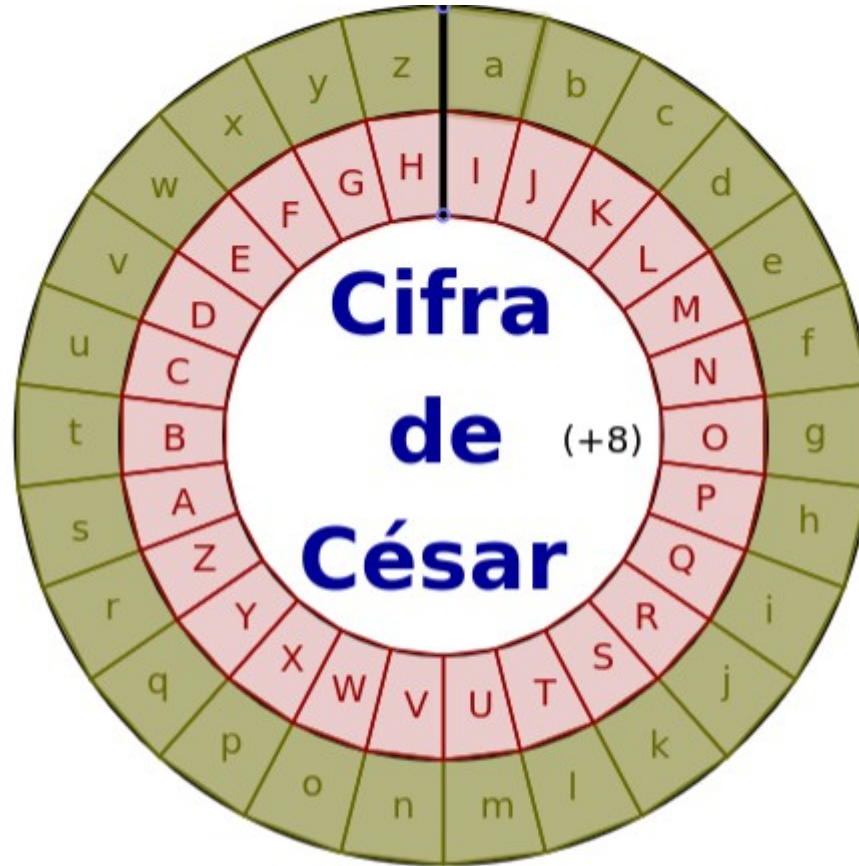
### CONVENCIONAL **CIFRA DE CÉSAR**

#### **EXEMPLO:**

Original:	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>...</i>	<i>Z</i>	}
Cifrado:	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>...</i>	<i>C</i>	
Regra: 3 posições à frente										

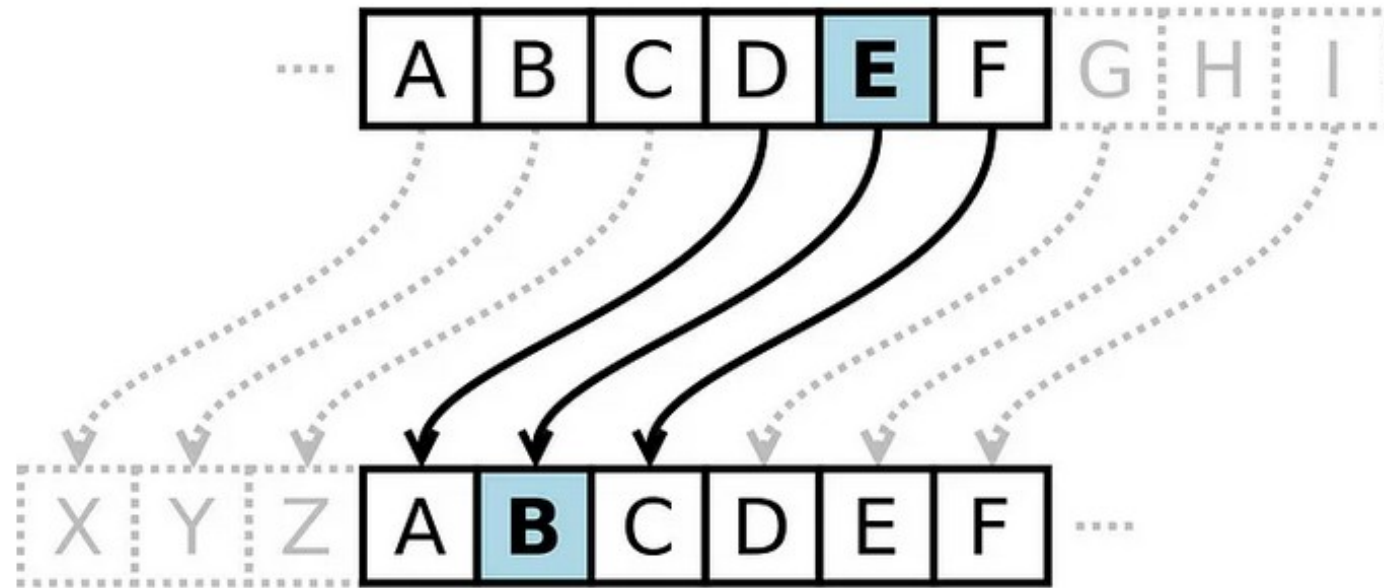
SUA VEZ!

*CESAR*  
*FHVDU*



<https://www.geogebra.org/m/kF6WJReU>

# Cifra de César em Python



# Método RSA

- 1978 – Ron Rivest , Adi Shamir , Leonard Adleman
- assimétrico
- $\left\{ \begin{array}{l} + \text{ popular} \\ + \text{ fácil de entender} \\ + \text{ fácil de implementar} \end{array} \right.$
- utilizado para garantir confiabilidade e assinatura digital
- segurança baseada na fatoração de números grandes

## Método RSA

### MÉTODO

1) Definir 2 números primos entre si  $p$  e  $q$  —————→

ex.: cada um com 1024 bits

Qto maior melhor (300 – 600 digitos)  
→ algoritmo mais seguro



## Método RSA

### MÉTODO

1) Definir 2 números primos entre si  $p$  e  $q$

2) Criar uma chave pública  $\longrightarrow n = p \cdot q$

Obs:

Mesmo que  $n$  seja público e conhecido, não é possível decodificá-lo sem  $p$  e  $q$ .

## Método RSA

### MÉTODO

1) Definir 2 números primos entre si  $p$  e  $q$

2) Criar uma chave pública  $\longrightarrow n = p \cdot q$

3) Calcular  $z$   $\longrightarrow z = (p-1)(q-1)$   
(função totiente ou de Euler)

4) Definir o número  $E$   $\longrightarrow \begin{matrix} E < n \\ E < z \end{matrix}$  e  $\text{mdc}(E, z) = 1$

5) Definir o número  $D$   $\longrightarrow (E \cdot D) \bmod z = 1$   $1 = DE + k z$

$DE - 1$  divisível por  $z$

## Método RSA

### MÉTODO

#### 6) Definir as chaves

→ para encriptar → utiliza-se  $E$  e  $n$  (chave pública)

→ para desencriptar → utiliza-se  $D$  e  $n$  (chave privada)

sendo:

$$\text{texto}_{\text{criptografado}} = \left( \text{texto}_{\text{original}} \right)^E \bmod n$$

$$\text{texto}_{\text{original}} = \left( \text{texto}_{\text{criptografado}} \right)^D \bmod n$$

## Método RSA

Mensagem original  $b$

Pré codificar a mensagem

Escolher  $p$  e  $q$

Calcular a Chave Pública  $\longrightarrow n = p \cdot q$

tamanho do  
bloco  $< n$

← Quebrar pré-codificação em blocos

Codificar bloco a bloco  $\longrightarrow$  Escolher  $e \in \mathbb{N}$   
 $b^e \equiv a \pmod{n}$

Mensagem codificada  $a$

$d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$  ← Chave Privada (de decodificação)

Decodificar bloco a bloco  $\longrightarrow a^d \equiv b \pmod{n}$

Mensagem decodificada  $b$

## Método RSA

### OBS: Pré-codificar

- Definir valores numéricos que representam as letras do alfabeto.
- Usual é redefinir o alfabeto de :

ou

10 a 35

11 a 36

Para evitar ambiguidade!

## Método RSA

### OBS: Pré-codificar

- Definir valores numéricos que representam as letras do alfabeto.
- Usual é redefinir o alfabeto de :

ou

10 a 35

11 a 36

Para evitar ambiguidade!

### EXEMPLO:

*AMOR*

1131518

11 , 1 e 13??

Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Tabela de pré-codificação

<i>A</i>	10	<i>G</i>	16	<i>M</i>	22	<i>S</i>	28	<i>Y</i>	34
<i>B</i>	11	<i>H</i>	17	<i>N</i>	23	<i>T</i>	29	<i>Z</i>	35
<i>C</i>	12	<i>I</i>	18	<i>O</i>	24	<i>U</i>	30		
<i>D</i>	13	<i>J</i>	19	<i>P</i>	25	<i>V</i>	31		
<i>E</i>	14	<i>K</i>	20	<i>Q</i>	26	<i>W</i>	32		
<i>F</i>	15	<i>L</i>	21	<i>R</i>	27	<i>X</i>	33		

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem:

*AMOR*

Utilizando:

$p=5$

$q=3$

$e=3$



## Método RSA

Mensagem original  $b$

Pré codificar a mensagem

Escolher  $p$  e  $q$

Calcular a Chave Pública  $\longrightarrow n = p \cdot q$

tamanho do  
bloco  $< n$

$\longleftarrow$  Quebrar pré-codificação em blocos

Codificar bloco a bloco  $\longrightarrow$  Escolher  $e \in \mathbb{N}$   
 $b^e \equiv a \pmod{n}$

Mensagem codificada  $a$

$d \cdot e \equiv 1 \pmod{(p-1)(q-1)} \longleftarrow$  Chave Privada (de decodificação)

Decodificar bloco a bloco  $\longrightarrow a^d \equiv b \pmod{n}$

Mensagem decodificada  $b$

**Exemplo 7.3** Queremos usar o esquema acima para codificar e, em seguida, recuperar a mensagem *DOIS É PRIMO*. Usando a tabela, temos que a mensagem é

$$m = 132418289914992527182224$$

© 2012 Pearson Education, Inc. All rights reserved.

**Exemplo 7.3** Queremos usar o esquema acima para codificar e, em seguida, recuperar a mensagem *DOIS É PRIMO*. Usando a tabela, temos que a mensagem é

$$m = 132418289914992527182224$$

*Separando em blocos, temos*

$$1324 - 182 - 899 - 1499 - 252 - 718 - 222 - 4$$

**Exemplo 7.3** Queremos usar o esquema acima para codificar e, em seguida, recuperar a mensagem *DOIS É PRIMO*. Usando a tabela, temos que a mensagem é

$$m = 132418289914992527182224$$

Separando em blocos, temos

$$1324 - 182 - 899 - 1499 - 252 - 718 - 222 - 4$$

Sejam  $p = 17$  e  $q = 101$ , então  $n = 1717$  (por que não é uma boa escolha?) e  $\phi(n) = 16 \times 100 = 1600$ . Escolhemos ainda  $e = 13$ , pois  $\text{mdc}(13, 1600) = 1$ . Para codificar a mensagem, fazemos  $C(b_i) \equiv b_i^e \pmod{n}$  para cada bloco  $b_i$ .

**Exemplo 7.3** Queremos usar o esquema acima para codificar e, em seguida, recuperar a mensagem *DOIS É PRIMO*. Usando a tabela, temos que a mensagem é

$$m = 132418289914992527182224$$

*Separando em blocos, temos*

$$1324 - 182 - 899 - 1499 - 252 - 718 - 222 - 4$$

*Sejam  $p = 17$  e  $q = 101$ , então  $n = 1717$  (por que não é uma boa escolha?) e  $\phi(n) = 16 \times 100 = 1600$ . Escolhemos ainda  $e = 13$ , pois  $\text{mdc}(13, 1600) = 1$ . Para codificar a mensagem, fazemos  $C(b_i) \equiv b_i^e \pmod{n}$  para cada bloco  $b_i$ .*

Porque é um número com poucos algarismos, isso compromete a segurança da encriptação




**Exemplo 7.3** Queremos usar o esquema acima para codificar e, em seguida, recuperar a mensagem DOIS É PRIMO. Usando a tabela, temos que a mensagem é

$$m = 132418289914992527182224$$

Separando em blocos, temos

$$\underline{1324} - 182 - 899 - 1499 - 252 - 718 - 222 - 4$$

Sejam  $p = 17$  e  $q = 101$ , então  $n = 1717$  (por que não é uma boa escolha?) e  $\phi(n) = 16 \times 100 = 1600$ . Escolhemos ainda  $e = 13$ , pois  $\text{mdc}(13, 1600) = 1$ . Para codificar a mensagem, fazemos  $C(b_i) \equiv b_i^e \pmod{n}$  para cada bloco  $b_i$ . Assim


$$C(1324) \equiv \underline{1324}^{\underline{13}} \equiv 104 \pmod{\underline{1717}}$$

**Exemplo 7.3** Queremos usar o esquema acima para codificar e, em seguida, recuperar a mensagem *DOIS É PRIMO*. Usando a tabela, temos que a mensagem é

$$m = 132418289914992527182224$$

Separando em blocos, temos

$$1324 - 182 - 899 - 1499 - 252 - 718 - 222 - 4$$

Sejam  $p = 17$  e  $q = 101$ , então  $n = 1717$  (por que não é uma boa escolha?) e  $\phi(n) = 16 \times 100 = 1600$ . Escolhemos ainda  $e = 13$ , pois  $\text{mdc}(13, 1600) = 1$ . Para codificar a mensagem, fazemos  $C(b_i) \equiv b_i^e \pmod{n}$  para cada bloco  $b_i$ . Assim

$$C(1324) \equiv 1324^{13} \equiv 104 \pmod{1717}$$

$$C(182) \equiv 182^{13} \equiv 1102 \pmod{1717}$$

$$C(899) \equiv 899^{13} \equiv 495 \pmod{1717}$$

$$C(1499) \equiv 1499^{13} \equiv 104 \pmod{1717}$$

$$C(252) \equiv 252^{13} \equiv 1671 \pmod{1717}$$

$$C(718) \equiv 718^{13} \equiv 1619 \pmod{1717}$$

$$C(222) \equiv 222^{13} \equiv 817 \pmod{1717}$$

$$C(4) \equiv 4^{13} \equiv 1636 \pmod{1717}$$



*E a mensagem codificada é*

$$104 - 1102 - 495 - 913 - 1671 - 1619 - 817 - 1636$$

*Para decodificar, precisamos primeiro encontrar  $d$  tal que  $de \equiv 1 \pmod{\phi(n)}$ , isto é,  $13d \equiv 1 \pmod{1600}$ . Note que isso é equivalente a encontrar  $d, k$  tais que  $13d + 1600k = 1$ . Como  $1599 = 13 \times 123$ , temos que  $13 \times (-123) + 1600 \times 1 = 1$ , assim  $d \equiv -123 \pmod{1600}$ , isto é,  $d = 1477$ .*




*E a mensagem codificada é*

$$\underline{104} - 1102 - 495 - 913 - 1671 - 1619 - 817 - 1636$$

*Para decodificar, precisamos primeiro encontrar  $d$  tal que  $de \equiv 1 \pmod{\phi(n)}$ , isto é,  $13d \equiv 1 \pmod{1600}$ . Note que isso é equivalente a encontrar  $d, k$  tais que  $13d + 1600k = 1$ . Como  $1599 = 13 \times 123$ , temos que  $13 \times (-123) + 1600 \times 1 = 1$ , assim  $d \equiv -123 \pmod{1600}$ , isto é,  $\underline{d = 1477}$ .*

*Fazemos, então,  $D(C(b_i)) \equiv C(b_i)^d \pmod{n}$  para cada  $C(b_i)$  recebido. Por exemplo, para  $i = 1$ :*


$$D(104) \equiv \underline{104}^{\underline{1477}} \equiv 1324 \pmod{1717}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Pré- codificação:

$R$	$S$	$A$
27	28	10

P e Q:

$p=5$        $q=7$        $\longrightarrow$  para criar a chave pública

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Pré- codificação:

$R$	$S$	$A$
27	28	10

P e Q:

$p=5$        $q=7$        $\longrightarrow$  para criar a chave pública

n e z:

$n = p \cdot q = 35$        $\longrightarrow$  chave de codificação  
 $z = (p-1)(q-1) = 24$        $\longrightarrow$  usado na decodificação

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Pré- codificação:

$R \quad S \quad A$   
 $27 \quad 28 \quad 10$

P e Q:

$p=5 \quad q=7 \quad \longrightarrow$  para criar a chave pública

n e z:

$n = p \cdot q = 35 \quad \longrightarrow$  chave de codificação  
 $z = (p-1)(q-1) = 24 \quad \longrightarrow$  usado na decodificação

blocos:

$27 \quad - \quad 28 \quad - \quad 10 \quad \longrightarrow$  tamanho do bloco  $< n$   
 $\rightarrow$  número de algarismos pode variar \*\*\* - \*\* - \*

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Pré- codificação:

$R \quad S \quad A$   
 $27 \quad 28 \quad 10$

P e Q:

$p=5 \quad q=7 \quad \longrightarrow$  para criar a chave pública

n e z:

$n = p \cdot q = 35 \quad \longrightarrow$  chave de codificação  
 $z = (p-1)(q-1) = 24 \quad \longrightarrow$  usado na decodificação

blocos:

$27 \quad - \quad 28 \quad - \quad 10 \quad \longrightarrow$  tamanho do bloco  $< n$   
 $\rightarrow$  número de algarismos pode variar \*\*\* - \*\* - \*

e:

$e=7 \quad \longrightarrow \quad mdc(e, z)=1 \quad e \in \mathbb{N} \quad , \quad e < n$

# Método RSA

## EXEMPLO: Codificar e depois decodificar a mensagem: RSA

## Pré- codificação:

$R$	$S$	$A$
27	28	10

P e Q:

$$p=5 \quad q=7$$

→ para criar a chave pública

n e z:

$$n = p \cdot q = \underline{\underline{35}}$$

→ chave de codificação

$$z=(p-1)(q-1)=24$$

→ usado na decodificação

## blocos:

27 - 28 - 10

→ tamanho do bloco  $< n$

→ número de algoritmos pode variar \*\*\* - \*\* - \*

e:

$$e=7$$
$$\longrightarrow mdc(e, z) = 1 \quad e \in \mathbb{N} \quad , \quad e < n$$

# Codificar

(bloco a bloco)

$$\underline{b^e} \equiv a \pmod{\underline{n}}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35}$$

$$28^7 \equiv a \pmod{35}$$

$$10^7 \equiv a \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$



## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

$$27^7 \equiv (36) (-6) (-8) \pmod{35}$$



## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

$$27^7 \equiv (36) (-6) (-8) \pmod{35} \longrightarrow 36 = 35q + 1$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

$$27^7 \equiv (36) (-6) (-8) \pmod{35} \longrightarrow 36 = 35q + 1$$

$$27^7 \equiv 1(-6)(-8) \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

$$27^7 \equiv (36) (-6) (-8) \pmod{35} \longrightarrow 36 = 35q + 1$$

$$27^7 \equiv 1(-6)(-8) \pmod{35}$$

$$27^7 \equiv 48 \pmod{35}$$

## EXEMPLO: Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

$$27^7 \equiv (36) (-6) (-8) \pmod{35} \longrightarrow 36 = 35q + 1$$

$$27^7 \equiv 1(-6)(-8) \pmod{35}$$

$$27^7 \equiv 48 \pmod{35}$$



Observe que não é possível finalizar aqui. Pois 48 não pertence a  $\mathbb{Z}_{35}$ .

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

$$27^7 \equiv (36) (-6) (-8) \pmod{35} \longrightarrow 36 = 35q + 1$$

$$27^7 \equiv 1(-6)(-8) \pmod{35}$$

$$27^7 \equiv 48 \pmod{35} \longrightarrow 48 = 35q + 13$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$27^7 \equiv (-8)^7 \pmod{35} \longrightarrow \text{falta } -8 \text{ para } 35$$

$$27^7 \equiv [(-8)^2]^3 (-8) \pmod{35}$$

$$27^7 \equiv [64]^3 (-8) \pmod{35} \longrightarrow 70 = 2 \cdot 35 \longrightarrow 64 \text{ para } 70 \rightarrow 6$$

$$27^7 \equiv [-6]^3 (-8) \pmod{35}$$

$$27^7 \equiv [-6]^2 (-6) (-8) \pmod{35}$$

$$27^7 \equiv (36) (-6) (-8) \pmod{35} \longrightarrow 36 = 35q + 1$$

$$27^7 \equiv 1(-6)(-8) \pmod{35}$$

$$27^7 \equiv 48 \pmod{35} \longrightarrow 48 = 35q + 13$$

$$27^7 \equiv 13 \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35}$$

$$10^7 \equiv a \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$28^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$28^7 \equiv (-7)^7 \pmod{35}$$

$$28^7 \equiv [(-7)^2]^3 (-7) \pmod{35}$$

$$28^7 \equiv (49)^3 (-7) \pmod{35} \longrightarrow 49 = 35q + 14$$

$$28^7 \equiv (14)^3 (-7) \pmod{35}$$

$$28^7 \equiv (14)^2 (14) (-7) \pmod{35}$$

$$28^7 \equiv 196 (14) (-7) \pmod{35} \longrightarrow 196 = 35Q + 21$$

$$28^7 \equiv 21 (14) (-7) \pmod{35}$$

$$28^7 \equiv 294 (-7) \pmod{35}$$

$$28^7 \equiv 14 (-7) \pmod{35}$$

$$28^7 \equiv -98 \pmod{35}$$

$$28^7 \equiv 7 \pmod{35}$$



## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$10^7 \equiv a \pmod{35} \longrightarrow a = ?$$

$$10^7 \equiv (10)^7 \pmod{35}$$

$$10^7 \equiv [(10)^2]^3 (10) \pmod{35}$$

$$10^7 \equiv (100)^3 (10) \pmod{35} \longrightarrow 100 = 35q - 5$$

$$10^7 \equiv (100)^3 (10) \pmod{35}$$

$$10^7 \equiv (-5)^3 (10) \pmod{35}$$

$$10^7 \equiv -125 (10) \pmod{35}$$

$$10^7 \equiv 15 (10) \pmod{35}$$

$$10^7 \equiv 150 \pmod{35}$$

$$10^7 \equiv 10 \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem codificada:

13 – 7 – 10

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem codificada:

13 – 7 – 10



## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem codificada:

13 – 7 – 10

d:

$$e \cdot d \equiv 1 \pmod{z}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem codificada:

13 – 7 – 10

d:

$$e \cdot d \equiv 1 \pmod{z}$$

$$7d \equiv 1 \pmod{24}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem codificada:

13 – 7 – 10

d:

$$e \cdot d \equiv 1 \pmod{z}$$

$$7d \equiv 1 \pmod{24}$$

$$7 \cdot 7 \equiv 1 \pmod{24} \longrightarrow d = 7$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem codificada:

13 – 7 – 10

d:

$$d=7$$

→ Chave de decodificação



## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Codificar

(bloco a bloco)

$$b^e \equiv a \pmod{n}$$

$$27^7 \equiv a \pmod{35} \longrightarrow 27^7 \equiv 13 \pmod{35}$$

$$28^7 \equiv a \pmod{35} \longrightarrow 28^7 \equiv 7 \pmod{35}$$

$$10^7 \equiv a \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem codificada:

13 - 7 - 10

d:

$$d=7$$

→ Chave de decodificação

Decodificar

(bloco a bloco)

$$\underline{a}^d \equiv b \pmod{\underline{n}}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35}$$

$$7^7 \equiv b \pmod{35}$$

$$10^7 \equiv b \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar  
(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow b = ?$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow b = ?$$

$$13^7 \equiv [(13)^2]^3 13 \pmod{35}$$

$$13^7 \equiv 169^3 \cdot 13 \pmod{35}$$

$$13^7 \equiv (-6)^3 \cdot 13 \pmod{35}$$

$$13^7 \equiv -216 \cdot 13 \pmod{35}$$

$$13^7 \equiv -6 \cdot 13 \pmod{35}$$

$$13^7 \equiv -78 \pmod{35}$$

$$13^7 \equiv 27 \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

$$7^7 \equiv b \pmod{35} \longrightarrow b = ?$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

$$7^7 \equiv b \pmod{35} \longrightarrow b = ?$$

$$7^7 \equiv [(7)^2]^3 (7) \pmod{35}$$

$$7^7 \equiv 49^3 (7) \pmod{35} \longrightarrow 49 - 35 = 14$$

$$7^7 \equiv 14^3 (7) \pmod{35}$$

$$7^7 \equiv 14^2 \cdot 14 (7) \pmod{35}$$

$$7^7 \equiv 196 \cdot 14 (7) \pmod{35} \longrightarrow 210 - 196 = 14$$

$$7^7 \equiv -14 \cdot 14 (7) \pmod{35}$$

$$7^7 \equiv -196 (7) \pmod{35}$$

$$7^7 \equiv 14 (7) \pmod{35}$$

$$7^7 \equiv 98 \pmod{35}$$

$$7^7 \equiv 28 \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

$$7^7 \equiv b \pmod{35} \longrightarrow 7^7 \equiv 28 \pmod{35}$$



## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

$$7^7 \equiv b \pmod{35} \longrightarrow 7^7 \equiv 28 \pmod{35}$$

$$10^7 \equiv b \pmod{35} \longrightarrow b = ?$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

$$7^7 \equiv b \pmod{35} \longrightarrow 7^7 \equiv 28 \pmod{35}$$

$$10^7 \equiv b \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

$$7^7 \equiv b \pmod{35} \longrightarrow 7^7 \equiv 28 \pmod{35}$$

$$10^7 \equiv b \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem decodificada:      27 – 28 – 10

## Método RSA

**EXEMPLO:** Codificar e depois decodificar a mensagem: RSA

Decodificar

(bloco a bloco)

$$a^d \equiv b \pmod{n}$$

$$13^7 \equiv b \pmod{35} \longrightarrow 13^7 \equiv 27 \pmod{35}$$

$$7^7 \equiv b \pmod{35} \longrightarrow 7^7 \equiv 28 \pmod{35}$$

$$10^7 \equiv b \pmod{35} \longrightarrow 10^7 \equiv 10 \pmod{35}$$

Mensagem decodificada:      27   –   28   –   10

R   S   A

### **POR QUE O MÉTODO RSA FUNCIONA??**

Veja video OBMEP:

<https://www.youtube.com/watch?v=arYNdvC4XtQ>

### **E POR QUE É SEGURO?**

Leia:

[https://dcc.ufrj.br/~collier/CursosGrad/cripto/notas\\_de\\_aula.pdf](https://dcc.ufrj.br/~collier/CursosGrad/cripto/notas_de_aula.pdf)

## **EXEMPLO DE PROGRAMAÇÃO DE CRIPTOGRAFIA RSA**

Veja a dissertação:

[https://teses.usp.br/teses/disponiveis/55/55136/tde-06042017-164507/publico/DanieleHelenaBonfim\\_revisada.pdf](https://teses.usp.br/teses/disponiveis/55/55136/tde-06042017-164507/publico/DanieleHelenaBonfim_revisada.pdf)



# EXERCÍCIOS

1) Palavra à criptografar usando o método RSA: OMEG

Considere:  $p=5$        $q=7$

<i>A</i>	10	<i>G</i>	16	<i>M</i>	22	<i>S</i>	28	<i>Y</i>	34
<i>B</i>	11	<i>H</i>	17	<i>N</i>	23	<i>T</i>	29	<i>Z</i>	35
<i>C</i>	12	<i>I</i>	18	<i>O</i>	24	<i>U</i>	30		
<i>D</i>	13	<i>J</i>	19	<i>P</i>	25	<i>V</i>	31		
<i>E</i>	14	<i>K</i>	20	<i>Q</i>	26	<i>W</i>	32		
<i>F</i>	15	<i>L</i>	21	<i>R</i>	27	<i>X</i>	33		

$$n=p\cdot q$$

$$z=(p-1)(q-1):$$

$$e=5$$

$$b^e\equiv a(mod\,n)$$



# RESOLUÇÃO DOS EXERCÍCIOS

## 1) Palavra à criptografar usando o método RSA: OMEG

Substituindo as letras do alfabeto por números usando a seguinte regra (4.1.8)

$$A=10, B=11, C=12, D=13 \dots Y=34, Z=35$$

temos que a palavra OMEG pode ser escrita da seguinte forma: 24 22 14 16.

Tomando  $e = 5$  e os números primos  $p = 5$  e  $q = 7$ , determinamos o valor de  $n = p \cdot q = 5 \cdot 7 = 35$ . Para criptografar usaremos a fórmula já definida:  $b^e \equiv a \pmod{n}$ .

# RESOLUÇÃO DOS EXERCÍCIOS

1)

$b_1^e \equiv a_1 \pmod{n}$	$b_2^e \equiv a_2 \pmod{n}$
$24^5 \equiv a_1 \pmod{35}$	$22^5 \equiv a_2 \pmod{35}$
$24 \equiv -11 \pmod{35}$	$22 \equiv -13 \pmod{35}$
$24^2 \equiv 121 \pmod{35}$	$22^2 \equiv 169 \pmod{35}$
$24^2 \equiv 16 \pmod{35}$	$22^2 \equiv -6 \pmod{35}$
$(24^2)^2 \equiv 256 \pmod{35}$	$(22^2)^2 \equiv 36 \pmod{35}$
$24^4 \equiv -24 \pmod{35}$	$22^4 \equiv 1 \pmod{35}$
$24^4 \cdot 24 \equiv -24 \cdot (-11) \pmod{35}$	$22^4 \cdot 22 \equiv 1 \cdot (-13) \pmod{35}$
$24^5 \equiv 19 \pmod{35}$	$22^5 \equiv 22 \pmod{35}$
$a_1 = 19$	$a_2 = 22$

# RESOLUÇÃO DOS EXERCÍCIOS

1)

$b_3^e \equiv a_3 \pmod{n}$	$b_4^e \equiv a_4 \pmod{n}$
$14^5 \equiv a_3 \pmod{35}$	$16^5 \equiv a_4 \pmod{35}$
$14 \equiv -21 \pmod{35}$	$16 \equiv -19 \pmod{35}$
$14^2 \equiv 441 \pmod{35}$	$16^2 \equiv 361 \pmod{35}$
$14^2 \equiv 21 \pmod{35}$	$16^2 \equiv 11 \pmod{35}$
$(14^2)^2 \equiv 21^2 \pmod{35}$	$(16^2)^2 \equiv 11^2 \pmod{35}$
$14^4 \equiv 441 \pmod{35}$	$16^4 \equiv 121 \pmod{35}$
$14^4 \equiv -14 \pmod{35}$	$16^4 \equiv -19 \pmod{35}$
$14^4 \cdot 14 \equiv -14 \cdot (-21) \pmod{35}$	$16^4 \equiv -19 \cdot (-19) \pmod{35}$
$14^5 \equiv 294 \pmod{35}$	$16^5 \equiv 361 \pmod{35}$
$14^5 \equiv 14 \pmod{35}$	$16^5 \equiv 11 \pmod{35}$
$a_3 = 14$	$a_4 = 11$

Fonte:

<https://repositorio.bc.ufg.br/tede/bitstream/tede/8579/5/Disserta%C3%A7%C3%A3o%20-%20Rodolfo%20Cavalcante%20Pinheiro%20-%202018.pdf>

# RESOLUÇÃO DOS EXERCÍCIOS

- 1) Portanto a mensagem criptografada é representada pelos números: 19 22 14 11. Para o processo de decodificação da mensagem, já em posse da chave pública  $n$ , seguimos a regra:  $a^d \equiv b \pmod{n}$ . Sendo  $d$  o inverso de  $e \pmod{(p-1)(q-1)}$ , que significa dizer:  $e.d \equiv 1 \pmod{(p-1)(q-1)}$  e  $b$  a mensagem original. Para nosso exemplo vamos decifrar o termo 19 e deixaremos os outros a cargo do leitor. Usando o processo descrito temos que:  $e = 5$ ,  $p = 5$ ,  $q = 7$ ,  $n = 35$  e  $(p-1).(q-1) = 4.6 = 24$ . Resolvendo a congruência  $5.d \equiv 1 \pmod{24}$  temos que  $d = 5$ . Assim:

# RESOLUÇÃO DOS EXERCÍCIOS

1)

$$a_1^d \equiv b_1 \pmod{n}$$

$$19^5 \equiv b_1 \pmod{35}, \text{ Mas :}$$

$$19 \equiv -16 \pmod{35}$$

$$19^2 \equiv 256 \pmod{35}$$

$$19^2 \equiv 11 \pmod{35}$$

$$(19^2)^2 \equiv 11^2 \pmod{35}$$

$$19^4 \equiv 121 \pmod{35}$$

$$19^4 \equiv -19 \pmod{35}$$

$$19^4 \cdot 19 \equiv -19 \cdot (-16) \pmod{35}$$

$$19^5 \equiv 304 \pmod{35}$$

$$19^5 \equiv 24 \pmod{35}$$

# RESOLUÇÃO DOS EXERCÍCIOS

1)

Portanto o 19 na mensagem criptografada refere-se ao 24 na mensagem original, voltando a simbologia letra/número chegamos a letra O da palavra OMEG. Como vimos determinar os números primos que geraram a chave pública  $n = 35$  é fundamental para decifrar a mensagem criptografada, no exemplo que usamos esse processo não é complicado, então buscamos encerrar o curso discutindo com os alunos o porque do método RSA ser tão eficiente pedindo a eles que determinassem os números primos que gerariam uma nova chave pública  $n = 14.558.801$ . Após breve discussão concluímos que seria inviável determinar tais números em pouco tempo, assim mostramos a solução:  $p_1 = 4093$  e  $p_2 = 3557$ .

Fonte:

<https://repositorio.bc.ufg.br/tede/bitstream/tede/8579/5/Disserta%C3%A7%C3%A3o%20-%20Rodolfo%20Cavalcante%20Pinheiro%20-%202018.pdf>