

# Criptografia RSA

Gabriel Alves de Lima

Universidade Federal do Paraná

13 de agosto de 2020



# Motivação

- Ron Rivest, Adi Shamir e Leonard Adleman;

# Motivação

- Ron Rivest, Adi Shamir e Leonard Adleman;
- Rivest e Shamir, cientistas da computação; e Adleman, matemático.

# Motivação

- Ron Rivest, Adi Shamir e Leonard Adleman;
- Rivest e Shamir, cientistas da computação; e Adleman, matemático.
- Algoritmo amplamente usado;

# Motivação

- Ron Rivest, Adi Shamir e Leonard Adleman;
- Rivest e Shamir, cientistas da computação; e Adleman, matemático.
- Algoritmo amplamente usado;
- Chave pública;

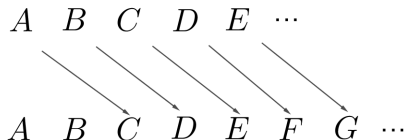
# Motivação

- Ron Rivest, Adi Shamir e Leonard Adleman;
- Rivest e Shamir, cientistas da computação; e Adleman, matemático.
- Algoritmo amplamente usado;
- Chave pública;
- Produto de primos, exemplo  $p = 457$  e  $q = 523$

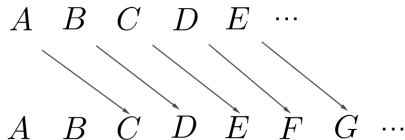
$$p \cdot q = 457 \cdot 523 = 239011.$$



# Chave Pública vs Chave Privada: Cifra de César



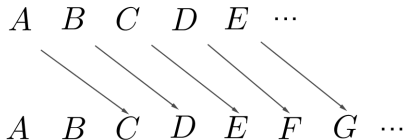
# Chave Pública vs Chave Privada: Cifra de César



- “tangerina”  $\leftrightarrow$  “vcpigtkpc” ;

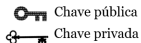


# Chave Pública vs Chave Privada: Cifra de César





- “tangerina”  $\leftrightarrow$  “vcpigtkpc” ;
- Só usa chave privada.

# Chave Pública vs Chave Privada



# Chave Pública vs Chave Privada

 Chave pública  
 Chave privada



 **Cliente**  


 **Servidor**  


 **Cliente** 

 **Servidor** 

# Chave Pública vs Chave Privada

 Chave pública  
 Chave privada

 Cliente  


 Servidor  


 Cliente 


 Servidor 

 Cliente  




 Mensagem



 Servidor 

 Mensagem → Mensagem

# Chave Pública vs Chave Privada

 Chave pública  
 Chave privada

 Cliente  


 Servidor  


 Cliente 

 Servidor 

 Cliente  
 Mensagem



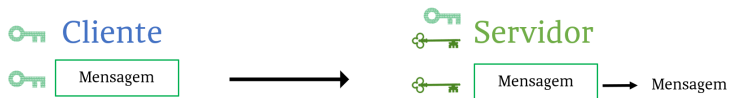
 Servidor   
 Mensagem → Mensagem

 Cliente   
 Mensagem → Mensagem



 Servidor  
 Mensagem

# Chave Pública vs Chave Privada



# RSA: Funcionamento

- Pré-Codificação
- Codificação
- Decodificação

## RSA: Pré-Codificação

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

Usamos 99 para espaços.



# Exemplo

- Vamos converter:  
*Eu amo matemática.*

# Exemplo

- Vamos converter:  
*Eu amo matemática.*

14	30	99	10	22	24	99	22	10	29	14
E	U	-	A	M	O	-	M	A	T	E
22	10	29	18	12	10	-	-	-	-	-
M	A	T	I	C	A					

# Exemplo

- Vamos converter:  
*Eu amo matemática.*

14	30	99	10	22	24	99	22	10	29	14
E	U	-	A	M	O	-	M	A	T	E
22	10	29	18	12	10	-	-	-	-	-
M	A	T	I	C	A					

- 1430991022249922102914221029181210

# RSA

- Escolhemos  $n = p \cdot q$ , onde  $p \neq q$  são primos;

# RSA

- Escolhemos  $n = p \cdot q$ , onde  $p \neq q$  são primos;
- Quebramos a mensagem em blocos (cada um menor do que  $n$ )

# Exemplo

$$\blacksquare p = 11 \text{ e } q = 13 \Rightarrow n = p \cdot q = 11 \cdot 13 = 143$$

# Exemplo

- $p = 11$  e  $q = 13 \Rightarrow n = p \cdot q = 11 \cdot 13 = 143$

- 1430991022249922102914221029181210

# Exemplo

■  $p = 11$  e  $q = 13 \Rightarrow n = p \cdot q = 11 \cdot 13 = 143$

■ 1430991022249922102914221029181210

■ 
$$\begin{array}{cccccccccccccc} 14 & 30 & 99 & 102 & 2 & 24 & 99 & 22 & 102 & 91 & 42 & 2 & 10 & 29 \\ 18 & 12 & 10 & & & & & & & & & & & \end{array}$$



# Codificação

■ Lembre-se,

1.  $\phi(n) = \#\{x \in \mathbb{N}, x \leq n \mid \text{mdc}(n, x) = 1\}$ ;
2.  $\phi(m \cdot n) = \phi(m)\phi(n)$  se  $\text{mdc}(m, n) = 1$ ;
3.  $\phi(p) = p - 1$ , se  $p$  é primo.

# Codificação

- Lembre-se,

1.  $\phi(n) = \#\{x \in \mathbb{N}, x \leq n \mid \text{mdc}(n, x) = 1\}$ ;
2.  $\phi(m \cdot n) = \phi(m)\phi(n)$  se  $\text{mdc}(m, n) = 1$ ;
3.  $\phi(p) = p - 1$ , se  $p$  é primo.

- Usamos  $n$  e precisamos de um  $e$ , onde

$$\text{mdc}(\phi(n), e) = 1$$

# Codificação

- Lembre-se,

1.  $\phi(n) = \#\{x \in \mathbb{N}, x \leq n \mid \text{mdc}(n, x) = 1\}$ ;
2.  $\phi(m \cdot n) = \phi(m)\phi(n)$  se  $\text{mdc}(m, n) = 1$ ;
3.  $\phi(p) = p - 1$ , se  $p$  é primo.

- Usamos  $n$  e precisamos de um  $e$ , onde

$$\text{mdc}(\phi(n), e) = 1$$

- Assim,  $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$ .

# Codificação

- Lembre-se,

1.  $\phi(n) = \#\{x \in \mathbb{N}, x \leq n \mid \text{mdc}(n, x) = 1\}$ ;
2.  $\phi(m \cdot n) = \phi(m)\phi(n)$  se  $\text{mdc}(m, n) = 1$ ;
3.  $\phi(p) = p - 1$ , se  $p$  é primo.

- Usamos  $n$  e precisamos de um  $e$ , onde

$$\text{mdc}(\phi(n), e) = 1$$

- Assim,  $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$ .

- $(n, e) \longrightarrow$  chave de codificação do sistema RSA.

# Codificação

- Denote por  $b$  um bloco e  $C(b)$  a codificação;

# Codificação

- Denote por  $b$  um bloco e  $C(b)$  a codificação;
- $C(b) \doteq$  resto da divisão de  $b^e$  por  $n$  ou a forma reduzida de  $b^e$  módulo  $n$ .

# Exemplo

- Temos

$$\phi(n) = \phi(143) = \phi(11 \cdot 13) = \phi(11) \cdot \phi(13) = 10 \cdot 12 = 120$$

# Exemplo

- Temos

$$\phi(n) = \phi(143) = \phi(11 \cdot 13) = \phi(11) \cdot \phi(13) = 10 \cdot 12 = 120$$

- Temos que escolher  $e$  tal que  $\text{mdc}(e, 120) = 1$



# Exemplo

- Temos

$$\phi(n) = \phi(143) = \phi(11 \cdot 13) = \phi(11) \cdot \phi(13) = 10 \cdot 12 = 120$$

- Temos que escolher  $e$  tal que  $\text{mdc}(e, 120) = 1$

- $120 = 10 \cdot 12 = 2 \cdot 5 \cdot 2 \cdot 6 = 2^3 \cdot 3 \cdot 5$

# Exemplo

- Temos

$$\phi(n) = \phi(143) = \phi(11 \cdot 13) = \phi(11) \cdot \phi(13) = 10 \cdot 12 = 120$$

- Temos que escolher  $e$  tal que  $\text{mdc}(e, 120) = 1$

- $120 = 10 \cdot 12 = 2 \cdot 5 \cdot 2 \cdot 6 = 2^3 \cdot 3 \cdot 5$

- Vamos tomar  $e = 7$ .

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10
- Codificando 12, ou seja,  $12^7$  módulo 143;

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$12^7$

■ Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

■ Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12$$

■ Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

■ Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12$$

■ Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

■ Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12$$



■ Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

■ Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12$$

■ Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

■ Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7 \equiv -41^7$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41$$



- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv 35^3 \cdot 41$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \end{aligned}$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \equiv 35^2(143 \cdot 10 + 5) \end{aligned}$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \equiv 35^2(143 \cdot 10 + 5) \equiv 35^2 \cdot 5 \end{aligned}$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \equiv 35^2(143 \cdot 10 + 5) \equiv 35^2 \cdot 5 \equiv \\ &\equiv 35 \cdot 175 \end{aligned}$$



- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \equiv 35^2(143 \cdot 10 + 5) \equiv 35^2 \cdot 5 \equiv \\ &\equiv 35 \cdot 175 \equiv 35 \cdot 32 \end{aligned}$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \equiv 35^2(143 \cdot 10 + 5) \equiv 35^2 \cdot 5 \equiv \\ &\equiv 35 \cdot 175 \equiv 35 \cdot 32 \equiv 1120 \end{aligned}$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \equiv 35^2(143 \cdot 10 + 5) \equiv 35^2 \cdot 5 \equiv \\ &\equiv 35 \cdot 175 \equiv 35 \cdot 32 \equiv 1120 \equiv (143 \cdot 7 + 119) \end{aligned}$$

- Blocos anteriores: 14 30 99 102 2 24 99 22 102  
91 42 2 10 29 18 12 10

- Codificando 12, ou seja,  $12^7$  módulo 143;

$$12^7 \equiv 12^6 \cdot 12 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv 1^3 \cdot 12 \equiv 12 \pmod{143}$$

- Vamos codificar 102, ou seja,  $102^7$  módulo 143;

$$\begin{aligned} 102^7 &\equiv (-41)^7 \equiv -41^7 \equiv (-1)(41^2)^3 \cdot 41 \equiv (-1)1681^3 \cdot 41 \equiv \\ &\equiv (-1)(11 \cdot 143 + 108)^3 \cdot 41 \equiv (-1)108^3 \cdot 41 \equiv (-1)(-35)^3 \cdot 41 \equiv \\ &\equiv 35^3 \cdot 41 \equiv 35^2 \cdot 1435 \equiv 35^2(143 \cdot 10 + 5) \equiv 35^2 \cdot 5 \equiv \\ &\equiv 35 \cdot 175 \equiv 35 \cdot 32 \equiv 1120 \equiv (143 \cdot 7 + 119) \equiv 119 \pmod{143} \end{aligned}$$

# Exemplo

- Fazendo o mesmo com os outros blocos

PC	14	30	99	102	2	24	99	22	102
C	53	134	33	119	128	106	33	22	119
PC	91	42	2	10	29	18	12	10	-
C	130	81	128	10	94	138	12	10	

- PC: Pré-codificado e C: codificado.
- 53 134 33 119 128 106 33 22 119 130 81 128  
10 94 138 12 10

# Decodificação

- Decodificamos bloco por bloco.

# Decodificação

- Decodificamos bloco por bloco.
- Usamos  $n$  e um número  $d$ , tal que  $d$  é o inverso de  $e$  mod  $\phi(n)$ .

# Decodificação

- Decodificamos bloco por bloco.
- Usamos  $n$  e um número  $d$ , tal que  $d$  é o inverso de  $e$  mod  $\phi(n)$ .
- $d \cdot e \equiv 1 \pmod{\phi(n)}$



# Decodificação

- Decodificamos bloco por bloco.
- Usamos  $n$  e um número  $d$ , tal que  $d$  é o inverso de  $e$  mod  $\phi(n)$ .
- $d \cdot e \equiv 1 \pmod{\phi(n)}$
- $(n, d) \longrightarrow$  chave de decodificação.

# Decodificação

- Decodificamos bloco por bloco.
- Usamos  $n$  e um número  $d$ , tal que  $d$  é o inverso de  $e$  mod  $\phi(n)$ .
- $d \cdot e \equiv 1 \pmod{\phi(n)}$
- $(n, d) \longrightarrow$  chave de decodificação.
- Seja  $a$  um bloco codificado e  $D(a)$  sua decodificação, então

$$D(a) \doteq \text{resto da divisão de } a^d \text{ por } n$$

# Decodificação

- Decodificamos bloco por bloco.
- Usamos  $n$  e um número  $d$ , tal que  $d$  é o inverso de  $e$  mod  $\phi(n)$ .
- $d \cdot e \equiv 1 \pmod{\phi(n)}$
- $(n, d) \longrightarrow$  chave de decodificação.
- Seja  $a$  um bloco codificado e  $D(a)$  sua decodificação, então

$$D(a) \doteq \text{resto da divisão de } a^d \text{ por } n$$

- $D(a)$  é a forma reduzida de  $a^d$  módulo  $n$ .

# Exemplo

■  $n = 143$ ,  $e = 7$  e  $\phi(143) = 120$

# Exemplo

- $n = 143$ ,  $e = 7$  e  $\phi(143) = 120$
- Pelo Algoritmo Euclidiano estendido:

$$120 = 7 \cdot 17 + 1$$

$$1 = 120 + (-17) \cdot 7$$

# Exemplo

- $n = 143$ ,  $e = 7$  e  $\phi(143) = 120$
- Pelo Algoritmo Euclidiano estendido:

$$120 = 7 \cdot 17 + 1$$

$$1 = 120 + (-17) \cdot 7$$

- $d = (-17) + 120 = 103$ .

# Exemplo

- $n = 143$ ,  $e = 7$  e  $\phi(143) = 120$
- Pelo Algoritmo Euclidiano estendido:

$$120 = 7 \cdot 17 + 1$$

$$1 = 120 + (-17) \cdot 7$$

- $d = (-17) + 120 = 103$ .
- Pois:

$$de \equiv 1 \pmod{\phi(n)}$$

$$de - 1 = k\phi(n), k \in \mathbb{Z}$$

$$1 = de + (-k)\phi(n)$$

# Exemplo

$$\blacksquare 119^d \pmod{n} \equiv 119^{103} \pmod{143} \equiv 102 \pmod{143}$$



# Exemplo

■  $119^d \pmod{n} \equiv 119^{103} \pmod{143} \equiv 102 \pmod{143}$

■

PC	14	30	99	102	2	24	99	22	102
C	53	134	33	119	128	106	33	22	119
PC	91	42	2	10	29	18	12	10	-
C	130	81	128	10	94	138	12	10	

# Resumo

- 1 Conversão de letras em números;
- 2 Escolha de  $n = p \cdot q$ ,  $p \neq q$  primos;
- 3 Mensagem em blocos menores que  $n$ ;
- 4 Escolha de  $e$  tal que,  $\text{mdc}(\phi(n), e) = 1$ ;
- 5  $(n, e) \longrightarrow$  chave de codificação;
- 6  $C(b)$  é a forma reduzida de  $b^e \bmod n$ ;
- 7 Escolha de  $d$  tal que,  $d$  é inverso de  $e \bmod \phi(n)$ ;
- 8  $(n, d) \longrightarrow$  chave de decodificação
- 9  $D(a)$  é a forma reduzida de  $a^d \bmod n$ .

# Por que funciona?

# Por que funciona?

- Queremos  $D(C(b)) = b$

## Por que funciona?

- Queremos  $D(C(b)) = b$ , ou seja,  $(b^e)^d = b^{ed} = b$

# Por que funciona?

- Queremos  $D(C(b)) = b$ , ou seja,  $(b^e)^d = b^{ed} = b$
- $b^{ed} \equiv b \pmod{n}$

# Por que funciona?

- Queremos  $D(C(b)) = b$ , ou seja,  $(b^e)^d = b^{ed} = b$
- $b^{ed} \equiv b \pmod{n}$
- Observamos que  $ed \equiv 1 \pmod{\phi(n)}$  implica em:

$$ed = 1 + k\phi(n), \quad k \in \mathbb{Z}$$

$$ed = 1 + k(p-1)(q-1)$$

$$\implies b^{ed} \equiv b \cdot b^{ed-1} \equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p}$$

## Por que funciona?

- Queremos  $D(C(b)) = b$ , ou seja,  $(b^e)^d = b^{ed} = b$
- $b^{ed} \equiv b \pmod{n}$
- Observamos que  $ed \equiv 1 \pmod{\phi(n)}$  implica em:

$$ed = 1 + k\phi(n), \quad k \in \mathbb{Z}$$

$$ed = 1 + k(p-1)(q-1)$$

$$\implies b^{ed} \equiv b \cdot b^{ed-1} \equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p}$$

- Se  $p$  não divide  $b$  temos  $b^{p-1} \equiv 1 \pmod{p}$  por Fermat



## Por que funciona?

- Queremos  $D(C(b)) = b$ , ou seja,  $(b^e)^d = b^{ed} = b$
- $b^{ed} \equiv b \pmod{n}$
- Observamos que  $ed \equiv 1 \pmod{\phi(n)}$  implica em:

$$ed = 1 + k\phi(n), \quad k \in \mathbb{Z}$$

$$ed = 1 + k(p-1)(q-1)$$

$$\implies b^{ed} \equiv b \cdot b^{ed-1} \equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p}$$

- Se  $p$  não divide  $b$  temos  $b^{p-1} \equiv 1 \pmod{p}$  por Fermat
- Se  $p$  divide  $b$  temos  $b \equiv 0 \pmod{p}$ , então  $b^{ed} \equiv b \pmod{p}$

# Por que funciona?

- Analogamente,  $b^{ed} \equiv b \pmod{q}$ ;

# Por que funciona?

- Analogamente,  $b^{ed} \equiv b \pmod{q}$ ;
- $b^{ed} - b$  é divisível por  $p$  e  $q$ ;

# Por que funciona?

- Analogamente,  $b^{ed} \equiv b \pmod{q}$ ;
- $b^{ed} - b$  é divisível por  $p$  e  $q$ ;
- Como  $\text{mdc}(p, q) = 1$ , segue que  $b^{ed} - b$  é divisível por  $pq \Rightarrow b^{ed} - b \equiv 0 \pmod{n}$  e por fim

$$b^{ed} \equiv b \pmod{n}.$$

# Implementação e problemas de segurança

- Para descriptografar é necessário saber  $(n, d)$ ;

# Implementação e problemas de segurança

- Para descriptografar é necessário saber  $(n, d)$ ;
- $de \equiv 1 \pmod{\phi(n)}$ ;

# Implementação e problemas de segurança

- Para descriptografar é necessário saber  $(n, d)$ ;
- $de \equiv 1 \pmod{\phi(n)}$ ;
- Primos grandes;

# Implementação e problemas de segurança

- Para descriptografar é necessário saber  $(n, d)$ ;
- $de \equiv 1 \pmod{\phi(n)}$ ;
- Primos grandes;
- $d$  pequeno;



# Implementação e problemas de segurança

- Para descriptografar é necessário saber  $(n, d)$ ;
- $de \equiv 1 \pmod{\phi(n)}$ ;
- Primos grandes;
- $d$  pequeno;
- $p, q$  grandes, mas  $|p - q|$  não;

# Implementação e problemas de segurança

- Para descriptografar é necessário saber  $(n, d)$ ;
- $de \equiv 1 \pmod{\phi(n)}$ ;
- Primos grandes;
- $d$  pequeno;
- $p, q$  grandes, mas  $|p - q|$  não;
- Teste de Miller.

# Assinatura Digital

- Empresa  $\leftrightarrow$  Banco;



# Assinatura Digital



- Empresa  $\leftrightarrow$  Banco;
- Quem recebe pode confirmar o remetente;

# Assinatura Digital



- Empresa  $\leftrightarrow$  Banco;
- Quem recebe pode confirmar o remetente;
- Usa-se  $e_e$ ,  $d_e$  para a empresa e  $e_b$ ,  $d_b$  para o banco;

# Assinatura Digital



- Empresa  $\leftrightarrow$  Banco;
- Quem recebe pode confirmar o remetente;
- Usa-se  $e_e$ ,  $d_e$  para a empresa e  $e_b$ ,  $d_b$  para o banco;
- Mensagem  $m$  da empresa;

# Assinatura Digital



- Empresa  $\leftrightarrow$  Banco;
- Quem recebe pode confirmar o remetente;
- Usa-se  $e_e$ ,  $d_e$  para a empresa e  $e_b$ ,  $d_b$  para o banco;
- Mensagem  $m$  da empresa;
- $C(m) = m^{e_b}$

# Assinatura Digital



- Empresa  $\leftrightarrow$  Banco;
- Quem recebe pode confirmar o remetente;
- Usa-se  $e_e$ ,  $d_e$  para a empresa e  $e_b$ ,  $d_b$  para o banco;
- Mensagem  $m$  da empresa;
- $C(m) = m^{e_b}$
- Empresa:  $m^{d_e} \longrightarrow s = (m^{d_e})^{e_b}$



# Assinatura Digital



- Empresa  $\leftrightarrow$  Banco;
- Quem recebe pode confirmar o remetente;
- Usa-se  $e_e$ ,  $d_e$  para a empresa e  $e_b$ ,  $d_b$  para o banco;
- Mensagem  $m$  da empresa;
- $C(m) = m^{e_b}$
- Empresa:  $m^{d_e} \longrightarrow s = (m^{d_e})^{e_b}$
- Banco:  $(s^{d_b})^{e_e}$

# Assinatura Digital



- Empresa  $\leftrightarrow$  Banco;
- Quem recebe pode confirmar o remetente;
- Usa-se  $e_e$ ,  $d_e$  para a empresa e  $e_b$ ,  $d_b$  para o banco;
- Mensagem  $m$  da empresa;
- $C(m) = m^{e_b}$
- Empresa:  $m^{d_e} \longrightarrow s = (m^{d_e})^{e_b}$
- Banco:  $(s^{d_b})^{e_e}$

$$\left( \left[ (m^{d_e})^{e_b} \right]^{d_b} \right)^{e_e} = m^{(e_e \cdot d_e)(e_b \cdot d_b)} = m$$

# Exercícios

- 1 Tomando  $p = 11$  e  $q = 3$ , siga os passos descritos no capítulo para codificar o seu nome. Lembre-se de usar a tabela para conversão de letras em números e ignore acentos. Além disso escolha um valor para  $e$  conveniente. Após a codificação, decodifique a mensagem e confira o resultado.
- 2 A mensagem 6355 - 5075 foi codificada pelo método RSA usando a senha  $n = 7597$  e  $e = 4947$ . Além disso, sabe-se que  $\phi(n) = 7420$ . Decodifique a mensagem.

# Ajudinha exercício 1

- 1 Conversão de letras em números;
- 2 Escolha de  $n = p \cdot q$ ,  $p \neq q$  primos;
- 3 Mensagem em blocos menores que  $n$ ;
- 4 Escolha de  $e$  tal que,  $\text{mdc}(\phi(n), e) = 1$ ;
- 5  $(n, e) \rightarrow$  chave de codificação;
- 6  $C(b)$  é a forma reduzida de  $b^e \text{ mod } n$ ;
- 7 Escolha de  $d$  tal que,  $d$  é inverso de  $e \text{ mod } \phi(n)$ ;
- 8  $(n, d) \rightarrow$  chave de decodificação
- 9  $D(a)$  é a forma reduzida de  $a^d \text{ mod } n$ .

$$p = 11, q = 3.$$

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

# Solução do exercício 1

VAMOS CODIFICAR: ZECA

Z	E	C	A
3	5	14	12
10			

↳ 35141210

Blocos: 3 5 14 12 10

$$\phi(n) = \phi(33) = \phi(11) \cdot \phi(3) = 10 \cdot 2 = 20$$

$$\Rightarrow \phi(n) = 20 = 2^2 \cdot 5$$

$$e = 3$$

CODIFICAÇÃO:

$$3^3 \equiv 27$$

$$5^3 \equiv 25 \cdot 5 \equiv (-8) \cdot 5 \equiv -40 \equiv 26$$

$$14^3 \equiv 14^2 \cdot 14 \equiv 196 \cdot 14 \equiv (33 \cdot 5 + 31) \cdot 14$$

$$\equiv 31 \cdot 14 \equiv (-2) \cdot 14 \equiv -28 \equiv 5$$

# Solução do exercício 1

$$12^3 \equiv 1728 \equiv 52 \cdot 33 + 12 \equiv \underline{12}$$

$$10^3 \equiv 1000 \equiv 30 \cdot 33 + 10 \equiv \underline{10}$$

Encontrar  $d$ :

Dividimos  $\phi(n)$  por  $e$

$$20 = 6 \cdot 3 + 2$$

$$20 = 6 \cdot 3 + (3-1)$$

$$20 = 7 \cdot (3) - 1$$

$$1 = \underset{\substack{\uparrow \\ d}}{7} \cdot \underset{\substack{\uparrow \\ e}}{3} + (-1) \cdot \underset{\substack{\uparrow \\ \phi(n)}}{20}$$

$$\Rightarrow d = 7$$

$$\begin{aligned} 5^7 &\equiv (5^2)^3 \cdot 5 \equiv (-8)^3 \cdot 5 \\ &\equiv (-8)^2 \cdot (-40) \equiv 64 \cdot (-40) \\ &\equiv (-2) \cdot (-7) \equiv \underline{14} \end{aligned}$$

# Referências

- [1] COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro, IMPA, 2014.
- [2] COMPARITECH. **What is RSA encryption and how does it work?**.
- [3] MARINHO, T. **Criptografia Assimétrica RSA**, 2017.

Muito Obrigado!



