



1) 1 1 1 1 1 1 1 1  
01000011<sup>C</sup> - 01010010<sup>R</sup> - 01001001<sup>I</sup> - 01010000<sup>P</sup>  
01010100<sup>T</sup> - 01001111<sup>G</sup> - 01000111<sup>S</sup> - 01010010<sup>R</sup>  
01000001<sup>A</sup> - 01000110<sup>F</sup> - 01001001<sup>I</sup> - 01000001<sup>A</sup>

Palavra traduzida: CRİPTOGRAFIA

2 3 2 1

2) 2432(m)

x 263(r)

50626

21555 +

5164

1046206

2 3 3 1 2  
3 4 4 2 3

3) 34524(6)

x 45(6)

1310312

231344 +

3024152

4) 4051(m) 436(m)

130

6



. .

7 11 10  
8 5

5)  $\frac{1}{2} \frac{1}{2}$  POLI (26)  
 $\times$  TEC (26)  
 1 TFCWQ  
 1 TFCWQ  
 HAJOGW +  
 HBOMQVMQ

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

7)  $23^{-2}$  mod 61

$61$	$23^2$	$15^2$	$8^2$	$7^2$
$15$	$8$	$7$	$1$	

$61 = 23 \cdot 2 + 15$   
 $23 = 15 \cdot 1 + 8$   
 $15 = 8 \cdot 1 + 7$   
 $8 = 7 \cdot 1 + 1$

$1 = 8 - 1 \cdot 7$   
 $1 = 8 - 1 \cdot (15 - 8 \cdot 1)$   
 $1 = 8 - 1 \cdot 15 + 8 \cdot 1$   
 $1 = 2 \cdot 8 - 1 \cdot 15$   
 $1 = 2 \cdot (23 - 1 \cdot 15) - 1 \cdot 15$

$1 = 2 \cdot 23 - 2 \cdot 15 - 1 \cdot 15$   
 $1 = 2 \cdot 23 + 3 \cdot 15$   
 $1 = 2 \cdot 23 + 3 \cdot (61 - 2 \cdot 23)$   
 $1 = 2 \cdot 23 + 3 \cdot 61 - 6 \cdot 23$   
 $1 = 18 \cdot 23 + 3 \cdot 61$

8) A diferença é que uma trabalha com números em restrição enquanto a outra trabalha com resto de divisões.

10)

F	437	19	393	3
	23	23	133	133
	1		1	

$$\text{mdc} = (437, 393) = 1$$

437	393 <sup>s</sup>	44 <sup>8</sup>	41 <sup>4</sup>	313	2 <sup>s</sup>
44	41	3	2	(1)	



15) Calcular  $1234^{-1} \pmod{4321}$

4321	1234 <sup>3</sup>	619 <sup>1</sup>	615 <sup>1</sup>	4 <sup>153</sup>	3 <sup>1</sup>
619	615	4	3	(1)	

$$1^a \text{ eq: } 4321 = 3 \cdot 1234 + 619$$

$$2^a \text{ eq: } 1234 = 1 \cdot 619 + 615$$

$$3^a \text{ eq: } 619 = 1 \cdot 615 + 4$$

$$4^a \text{ eq: } 615 = 153 \cdot 4 + 3$$

$$5^a \text{ eq: } 4 = 1 \cdot 3 + 1$$

$$1 = 4 - 1 \cdot 3$$

$$1 = 4 - 1 \cdot (615 - 153 \cdot 4)$$

$$1 = 4 - 1 \cdot 615 + 153 \cdot 4$$

$$1 = 154 \cdot 4 - 1 \cdot 615$$

$$1 = 154 \cdot (619 - 1 \cdot 615) - 1 \cdot 615$$

$$1 = 154 \cdot 619 - 154 \cdot 615 - 1 \cdot 615$$

$$1 = 154 \cdot 619 - 155 \cdot 615$$



16) b)  $6x \equiv 4 \pmod{13}$

para isso  
pelo inverso

$$x \equiv 4 \cdot 6^{-1} \pmod{13}$$

↳ calcular a inversa  $6^{-1} \pmod{13}$

$$\begin{array}{r|l} 13 & 6^2 \\ \hline 11 & 1 \end{array}$$

$$1^a \text{ eq: } 13 = 2 \cdot 6 + 1$$

$$1 = 13 - 2 \cdot 6$$

$$\text{logo: } 6^{-1} \pmod{13} = -2$$

$$+ 13$$

$$11$$

$$x \equiv 4 \cdot 11 \pmod{13}$$

$$x \equiv 44 \pmod{13} \Rightarrow \boxed{5}$$

01)  $12x \equiv 10 \pmod{23}$

$$x \equiv 10 \cdot 12^{-1} \pmod{23}$$

$$\begin{array}{r|l} 23 & 12^2 \\ \hline 11 & 1 \end{array}$$

$$1^a \text{ eq: } 23 = 1 \cdot 12 + 11 \rightarrow 23 - 1 \cdot 12 = 11$$

$$2^a \text{ eq: } 12 = 1 \cdot 11 + 1$$



$$1 = 12 - 1 \cdot 11$$

$$1 = 12 - 1 \cdot (23 - 1 \cdot 12)$$

$$1 = \underline{12} - 1 \cdot 23 + \underline{1 \cdot 12}$$

$$1 = \underline{2 \cdot 12} - \underline{1 \cdot 23}$$

$$1 = 2 \cdot 12 \pmod{23} \Rightarrow 12^{-1} = 2$$

$$x \equiv 10 \cdot 2 \pmod{23}$$

$$x \equiv 20 \pmod{23} = \boxed{20}$$