# Matemática Discreta

## Licenciatura em Segurança Informática em Redes de Computadores
## Licenciatura em Engenharia Informática
## **Teoria dos Números - Criptografia**

Eliana Costa e Silva – eos@estg.ipp.pt
Aldina Correia – aic@estg.ipp.pt

P.PORTO ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Felgueiras, maio de 2022

# Exemplos da utilização da Teoria dos Números na Criptografia

## Cifra de César

A **Cifra de César** é um método de escrita de mensagens proposto por César que consistia em transladar cada letra do alfabeto para três "casas" mais adiante:

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

### Encriptar

Substituímos cada letra por um número inteiro de $0$ até $25$, baseado na sua posição no alfabeto, onde $A \leftrightarrow 0, \ldots, Z \leftrightarrow 25$.

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

Portanto, o método de César é definido pela função $f$ que aplica cada número inteiro $n$, $0 \leq n \leq 26$, no inteiro $f(n) = (n+3) \bmod 26$.

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

Por exemplo, $X \leftrightarrow 23 \longrightarrow f(23) = 27 \bmod 23 = 1 \leftrightarrow B$.

## Exercício

Encripte a mensagem "DISCRETA" usando a cifra de César.

$D \leftrightarrow 3 \longrightarrow f(3) = (3+3) \bmod 26 = 6 \leftrightarrow G$
$I \leftrightarrow 8 \longrightarrow f(8) = (8+3) \bmod 26 = 11 \leftrightarrow L$.
$S \leftrightarrow 18 \longrightarrow f(18) = (18+3) \bmod 26 = 21 \leftrightarrow V$.
...

## Recuperar a mensagem original

Para recuperar a mensagem original a partir da mensagem encriptada pela Cifra de César basta considerar a **função inversa** $f^{-1}$ que transforma um número inteiro $n$, com $0 \leq n \leq 25$, no número inteiro localizado 3 posições antes, i.e.

$$f^{-1}(n) = (n-3) \bmod 26.$$

### Generalizar a cifra de César

Podemos generalizar a cifra de César transladando $b$ casas em vez de 3 da seguinte forma:

$$f(n) = (n+b) \bmod 26$$

Este é um método muito simples e muito pouco seguro!

## Generalizar e "melhorar" a cifra de César

Pode definir-se

$$f(n) = (an+b) \bmod 26,$$

com $a$ e $b$ inteiros escolhidos de modo a garantir que $f$ é uma bijeção (**Porquê?**)

## Exercício

Considere a função de encriptação definida por $f(n) = (25n + 1) \bmod 29$ e considere as seguintes correspondências:

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | * | + | $ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |

1. Encripte a mensagem "BLOB".
2. Defina a expressão da função de desencriptação, $f^{-1}$
3. Desencripte a mensagem "TDQ".

# Criptografia – O sistema RSA de chave pública[1]

Suponhamos que a Ana pretende enviar uma **mensagem** $x$ ao Bruno, pedindo-lhe que gere uma chave pública $u$ (conhecida por toda a gente) e uma chave privada $v$ (conhecida apenas pelo Bruno).
O protocolo funciona do seguinte modo:

**[1]** A Ana envia a mensagem $u(x)$ ao Bruno pelo canal público.

**[2]** O Bruno recupera a mensagem original $x$ aplicando $v$ a $u(x)$.

As chaves $u$ e $v$ são aplicações do espaço das mensagens para o espaço das mensagens. Para que o sistema funcione bem e permita manter o secretismo na comunicação, devem ter as seguintes propriedades:

(P1) $v(u(x)) = x$ para qualquer mensagem $x$.

(P2) deve ser difícil obter $x$ conhecendo $u(x)$ e não conhecendo $v$.

Ao definirmos um sistema criptográfico deveremos explicitar o espaço das mensagens bem como as aplicações $u$ e $v$.

[1] desenvolvido em 1976 por Rivest, Shamir e Adleman.

# Criptografia – O sistema RSA de chave pública

Os sistemas criptográficos do tipo RSA são definidos do seguinte modo:

- $Z_m = \{0, 1, 2, \ldots, m-1\}$, onde $m = p \times q$ para algum par de números primos $p$ e $q$ é o espaço de mensagens;
- $u(x) = x^a \bmod m$, para qualquer $x \in \mathbb{Z}_m$;
- $v(y) = y^b \bmod m$, para qualquer $y \in \mathbb{Z}_m$;

  onde $a$ e $b$ são tais que

$$a \times b \bmod [(p-1) \times (q-1)] = 1$$

Este sistema permite enviar mensagens encriptadas por uma chave pública $a$, mas para que o recetor seja capaz de desencriptar a mensagem precisa de ter uma chave privada $b$, apenas do seu conhecimento.

**Proposicao**

Sejam $p$ e $q$ números primos distintos. Sejam ainda $m = p\,q$ e $n = (p-1)(q-1)$. Se $a$ e $b$ são números inteiros tais que $ab \equiv 1 \bmod n$, então

$v(u(x)) = x$ para qualquer número inteiro $x < p\,q$.

## Procedimento de encriptação

Sejam $p$ e $q$ dois números primos, $m = p\,q$, $n = (p-1)(q-1)$, $a$ tal que $\text{mdc}(a, n) = 1$ e $b$ a solução da congruência $ab \equiv 1 \bmod n$.

No sistema RSA, podemos começar por traduzir as mensagens (sequências de letras) em sequências de números inteiros (tal como fizemos na cifra de César).

O número inteiro $x$ daí resultante é depois transformado, com a ajuda da chave pública $a$, num número inteiro fazendo:

$$u(x) = x^a \bmod m$$

## Procedimento de desencriptação

O recetor quando recebe a mensagem desencripta-a com a ajuda da chave privada $b$ que apenas ele conhece, fazendo:

$$v(u(x)) = u(x)^b \bmod m$$

## Exemplo

Encripte a mensagem "STOP" usando o sistema RSA com $m$ =2537 e $a = 13$.

Note que $2537 = 43 \times 59$, $p = 43, q = 59$ e mdc$(13, (43-1)(59-1)) =$ mdc$(13, 42 \times 58) = 1$.

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

Para encriptar começamos por traduzir STOP no seu equivalente numérico. De seguida agrupamos esses números em blocos de quatro dígitos (pois $2525 < 2537 < 252525$). Obtemos,

$$1819 \quad 1415$$

De seguida encriptamos cada bloco de quatro dígitos:

$u(x) = x^a \bmod m$, com $m = p \times q = 2537$ e $a = 13$.

$u(1819) = 1819^{13} \bmod 2537 = 2081$

e

$u(1415) = 1415^{13} \bmod 2537 = 2182$

A mensagem encriptada é $2081 \quad 2182$.

```
--> aux =
pmodulo(1819,2537);
--> for k=1:(13-1)
> aux =
pmodulo(aux*1819,2537);
> end
--> aux
aux =
2081.
```

## Exemplo

Encripte a mensagem "SOS" usando o sistema RSA com com $m$ =2537 e $a = 13$..

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

Temos S $\rightarrow$ 18 e O $\rightarrow$ 14.

**Encriptação**:

$$u(x) = x^a \bmod m, \text{ com } m = p \times q = 2537 \text{ e } a = 13.$$

Assim,

$$u(\text{“}S\text{”}) = u(18) = 18^{13} \bmod (2537) = 2222$$
$$u(\text{“}OS\text{”}) = u(1418) = 1418^{13} \bmod (2537) = 1289$$

A mensagem "SOS" encriptada é:

$$2222 \quad 1289$$

## Exemplo

Desencripte a mensagem 2081 2182, encriptada usando o sistema RSA do exemplo anterior ($p = 43, q = 59$ e $a = 13$).

**Desencriptação**:

$$v(u(x)) = u(x)^b \bmod m.$$

Temos que começar por determinar $b$ resolvendo a congruência $ab \equiv 1 \bmod n$. Como $n = (p-1)(q-1) = 42 \times 58 = 2436$, a congruência a resolver é

$$13b \equiv 1 \bmod 2436$$

Portanto, é necessário calcular o inverso de $13 \bmod 2436$.

Usando o algoritmo de Euclides:

$$\begin{aligned}
2436 &= 187 \times 13 + 5 && \rightarrow && 5 &= 2436 - 187 \times 13 \\
13 &= 5 \times 2 + 3 && \rightarrow && 3 &= 13 - 5 \times 2 \\
5 &= 3 \times 1 + 2 && \rightarrow && 2 &= 5 - 3 \times 1 \\
3 &= 2 \times 1 + 1 && \rightarrow && 1 &= 3 - 2 \times 1
\end{aligned}$$

Temos que mdc(2436,13)=1, donde existe o inverso de 13 modulo 2436.

Assim,

$$\begin{aligned}
\text{mdc}(2436, 13) &= 1 \\
&= 3 - 2 \times 1 \\
&= 3 - (5 - 3 \times 1) \times 1 \\
&= 2 \times 3 - 1 \times 5 \\
&= 2 \times (13 - 5 \times 2) - 1 \times 5 \\
&= 2 \times 13 - 5 \times 4 - 1 \times 5 \\
&= 2 \times 13 - 5 \times 5 \\
&= 2 \times 13 - 5 \times (2436 - 187 \times 13) \\
&= 2 \times 13 - 5 \times 2436 + 935 \times 13 \\
&= \mathbf{937} \times 13 - 5 \times 2436
\end{aligned}$$

Logo, o inverso de 13 modulo 2436 é **937** e

$$13b \equiv 1 \bmod 2436 \Leftrightarrow 937 \times 13 \times b \equiv 937 \times 1 \bmod 2436 \Leftrightarrow b \equiv 937 \bmod 2436$$

Podemos então desencriptar a mensagem fazendo:

$$v(u(x)) = u(x)^b \bmod m$$

$$v(2081) = 2081^{937} \bmod (2537) = 1819$$

No Scilab fazemos:

```
aux=pmodulo(2081,2537)
for k=1:(937-1)
 aux=pmodulo(aux*2081,2537);
end
```

$$v(2182) = 2182^{937} \bmod (2537) = 1415$$

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

Como

$$18 \to \text{S},\ 19 \to \text{T},\ 14 \to \text{O e } 15 \to \text{P}.$$

A mensagem original é “STOP”.

Como se desenrola na realidade o processo de troca de mensagens secretas entre a Ana e o Bruno?

O recetor, o Bruno:

1. escolhe dois números primos $p$ e $q$
   que pode ser difícil quando se procuram números $p$ e $q$ muito grandes;
2. calcula os produtos $m = pq$ e $n = (p-1)(q-1)$
   é muito fácil!
3. escolhe $a \in \mathbb{Z}_n$ (a chave pública) tal que $\text{mdc}(a, n) = 1$
   é fácil se conhecemos um algoritmo eficaz para calcular o mdc de 2 números!
4. usando o algoritmo de Euclides, determina $b \in \mathbb{Z}_n$ (a chave privada) tal que $ab \equiv 1 \bmod n$
   é fácil se conhecemos um algoritmo eficaz para calcular o inverso de um elemento em $\mathbb{Z}_n$!
5. envia os valores de $m$ e $a$ para a Ana, mantendo a chave privada $b$ apenas do seu conhecimento
   não havendo garantias de segurança no canal de comunicação, os valores de $m$ e $a$ passam a ser eventualmente públicos!

A Ana tem agora os elementos para encriptar as suas mensagens com a função $u$ e enviá-las ao Bruno. Como apenas o Bruno conhece o valor de $b$, apenas ele poderá decifrar a mensagem aplicando a função $v$.

E que trabalho tem que fazer uma terceira pessoa mal intencionada, que conhece apenas a função de encriptação, para desencriptar uma mensagem?

1. fatorizar o número $m$ para recuperar os primos $p$ e $q$
   o que pode ser muito difícil quando $m$ é muito grande;
2. usando o algoritmo de Euclides, determinar $b \in \mathbb{Z}_n$ (a chave privada) tal que $ab \equiv 1 \bmod n$
   o que será fácil se conhecemos um algoritmo eficaz para calcular o inverso de um elemento em $\mathbb{Z}_n$.

Portanto,

- para criar o código é preciso encontrar dois números primos $p$ e $q$;
- para decifrar o código é preciso fatorizar o produto $n = p\,q$.

**Exercícios**: 118 ao 126.