Introdução à Criptografia

Master in Mathematics and Applications
Universidade Agostinho Neto, Luanda, Angola

Doutor Pedro Quaresma
Departamento de Matemática
Universidade de Coimbra, Portugal

26 de Julho a 13 de Agosto, 2021

Bibliografia

- Douglas Stinson, *Cryptography: Theory and Practice*, CRC, 2006.
- A. Menezes, P. van Oorschot, S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. (Fifth Printing, August 2001)
- Johannes Buchmann, *Introduction to Cryptography*, Springer, 2000.
- Richard Spillman. *Classical and Contemporary Cryptology*. Prentice Hall, 2005.
- Viktoria Tkotz. *CRIPTOGRAFIA - Segredos Embalados para Viagem*. NOVATEC Editora, São Paulo, Brasil, 2005.
- Jones, G.A. e Jones J.M., Elementary Number Theory, Springer-Verlag, 1998.
- J.F. Queiró, *Teoria dos Números* (notas), Departamento de Matemática, FCTUC, 2008.

Programa

- Introdução à Criptografia e Criptoanálise
  - Criptografia: Definição e Objectivos
  - Notas históricas
- Criptografia e Criptoanálise Clássicas
  - Mono-alfabéticas: deslocamento simples e linear
  - Poli-alfabéticas: Vigenère
  - Procura Exaustiva
  - Análise de Frequências
- Cifras Fieira
  - Cifra de Vernam
- Cifras por Blocos de Chaves Simétricas
  - Modos de Operação
  - Cifras Produto
  - Cifras Feistel
  - Cifra FEAL
  - Outras cifras de chaves simétricas: AES
  - Criptoanálise Linear e Criptoanálise Diferencial
- Cifras por Blocos de Chave Pública
  - Funções Unidireccionais e Unidireccionais com Escapatória
  - Autenticação e manutenção de chaves públicas
  - RSA
  - Criptoanálise da Cifra RSA
  - ElGamal
  - Criptoanálise da Cifra ElGamal
- Cifras Quânticas, breves notas

Informação

Segurança

Criptografia

Kryptós – oculto; graph – escrever

4000 a.C.	Egipto (encontrados em túmulos)
600 a 500 a.C.	O Livro de Jeremias e as Cifras Hebraicas atbah, atbash, albam (substituição simples)
487 a.C.	Tucídides (Esparta) e o Bastão de Licurgo (transposição)
50 a.C.	O Código de Júlio César (substituição simples)
801 a 873	al-Kindi e a Criptoanálise

Substituição Poli-alfabética

1466	Leon Battista Alberti (inventor da substituição poli-alfabética)
1553	Giovanni Battista Bellaso (substituição poli-alfabética com palavra-chave)
1558	Philibert Babou (substituição homofónica)
1586	Blaise de Vigenère (substituição poli-alfabética com palavra-chave)
1854	Charles Babbage e as Máquinas de Diferenças Cifra Playfair (substituição poli-alfabética em bloco bigrâmico)

Máquinas Cifrantes

1918	Arthur Scherbius - Máquina Enigma

Aplicações

487 a.C. — . . . Militares

- Segredos Nacionais
- Estratégias
- planos; datas; tropas; . . .

A proliferação das telecomunicações levou a criptografia para um "palco" diferente.

1960 – . . . Aplicações Civis

- Empresas, informação interna
- troca de informação entre diferentes delegações

O advento da Internet "globalizou" a criptografia.

1969 — . . . Aplicações Pessoais

- Correio electrónico
- Redes sem fios
- Comunicações entre dispositivos electrónicos

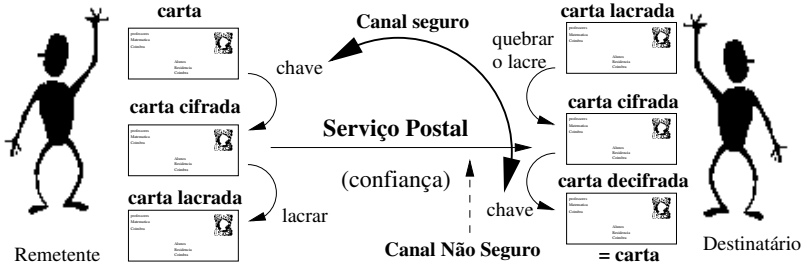
Algumas Datas (Recentes) Relevantes

1977	**D**ata **E**ncryption **S**tandard
1976	Diffie & Hellman, *New Directions in Cryptography* - Sistemas de Chave Pública (logaritmo discreto, sem aplicação computacional)
1978	**R**ivest, **S**hamir, **A**delman, sistema de chave pública, factorização de números primos
1985	ElGamal, sistema de chave pública, logaritmo discreto.
1994	Algoritmo de Factorização de Shor (computação quântica)
2001	**A**dvanced **E**ncryption **S**tandard

Troca de Informação de Forma Segura

- Questões de Confiança
- Protocolos

Meios Físicos + Meios Computacionais + Conjunto de Protocolos + Lei



Criptografia

Definição (Criptografia)

Criptografia é o estudo das técnicas matemáticas relacionadas com os aspectos de segurança da informação tais como: confidencialidade, integridade da informação, autenticação de entidades e da origem da informação.

Criptografia — conjunto de técnicas para providenciar uma troca de informação segura.

Objectivos da Criptografia

Confidencialidade manter o conteúdo da informação secreto para todos excepto para o (correcto) destinatário da mesma.

Integridade da Informação assegurar que não há alteração da informação por pessoas não autorizadas.

Autenticação

- das entidades que comunicam entre si;
- da informação (origem, conteúdo, data de envio, . . .)

Não repudiação o produtor da informação não poder negar a autoria da mesma.

Esquema de Encriptação (Cifra)

Uma primeira definição informal.

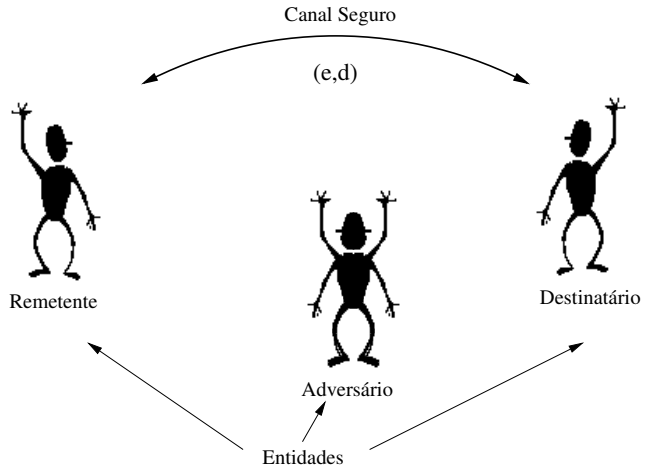
Definição (Esquema de Encriptação (ou cifra))

Um esquema de encriptação *consiste de um conjunto de transformações de encriptação e um conjunto correspondente de transformações de desencriptação com a propriedade de que o processo desencriptação é o inverso da encriptação.*

Um esquema de encriptação e usualmente designado por cifra.

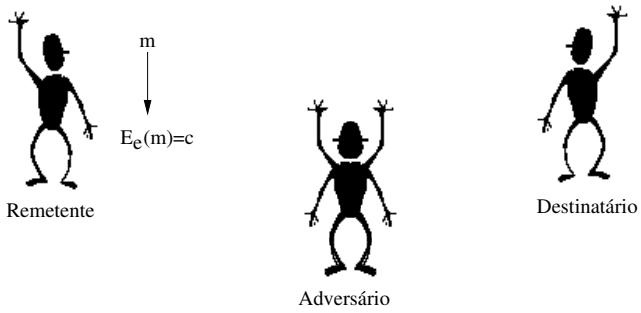
Uma utilização de uma Cifra de Chaves Simétricas

1 – João e José escolhem (secretamente) um par de chaves



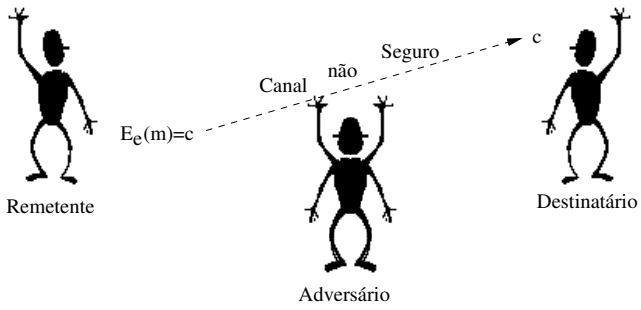
Uma utilização de uma Cifra (Chaves Simétricas)

2 – João decide enviar uma mensagem, $m \in \mathcal{M}$, a José. Calcula $c = E_e(m)$ e envia o texto resultante.



Uma utilização de uma Cifra (Chaves Simétricas)

2 – João decide enviar uma mensagem, $m \in \mathcal{M}$, a José. Calcula $c = E_e(m)$ e envia o texto resultante.

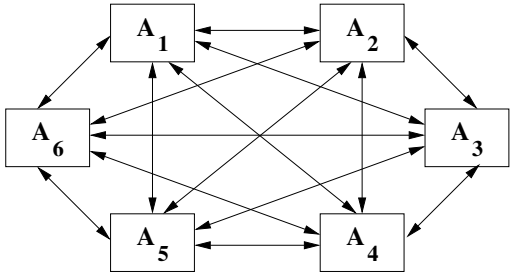


Uma utilização de uma Cifra (Chaves Simétricas)

3 – Ao receber a mensagem o José calcula $D_d(c) = m$ recuperando deste modo a mensagem original.

Estabelecer e Manter Chaves Simétricas

Se num sistema de chaves simétricas (secretas) se pretender que cada duas entidades distintas partilhem uma chave secreta, então temos que o número de chaves secretas necessárias é $\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$.



É fácil de ver que o manter das chaves é problemático numa situação como esta, $\binom{6}{2} = \frac{6\times5}{2} = 15$.

Vantagens e Desvantagens

Vantagens das Cifras de Chaves Simétricas

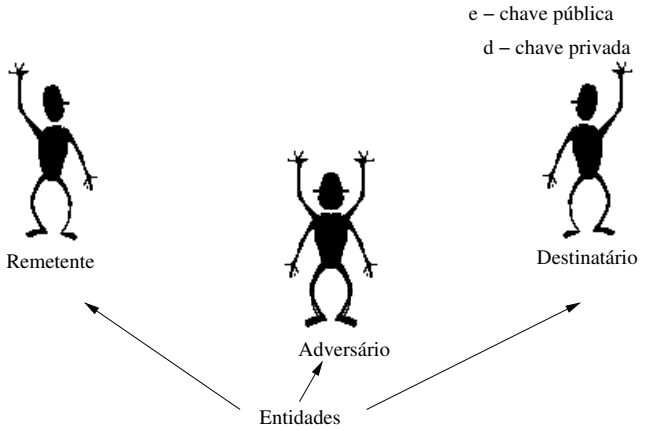
1. Podem ser concebidas para terem uma velocidade de processamento de dados elevada.
2. As chaves são relativamente pequenas.
3. Cifras deste tipo podem ser usadas como primitivas em vários tipos de ferramentas criptográficas
4. São facilmente componíveis de forma a construir sistemas criptográficos mais seguros.
5. Têm um largo historial, e como tal já foram muito, e extensivamente, estudadas.

Desvantagens das Cifras de Chaves Simétricas

1. As chaves entre todas as entidades envolvidas numa comunicação têm de ser mantidas secretas.
2. Se o número de entidades envolvidas for elevado o número de pares de chaves a considerar é também elevado.
3. As chaves têm de ser mudadas muito frequentemente.

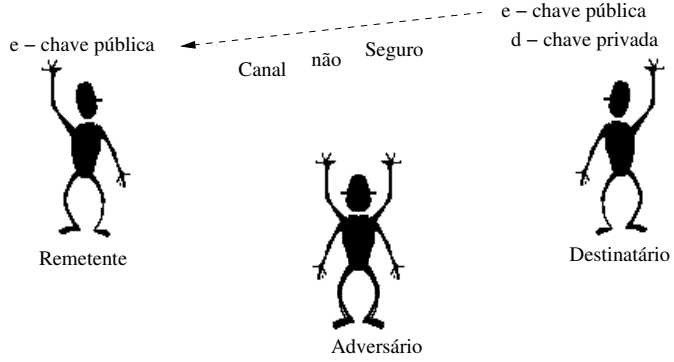
Uma utilização de uma Cifra de Chave Pública

1 – O José escolhe um par de chaves: publicita a chave de encriptação e, mantém secreta a chave de desencriptação d.



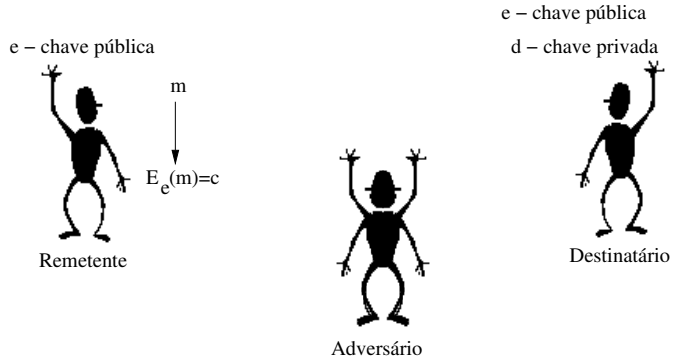
Uma utilização de uma Cifra (Chave Pública)

2 – João decide enviar uma mensagem, $m \in \mathcal{M}$, a José. Obtém a chave pública do José e e calcula $c = E_e(m)$. Depois envia o texto resultante.



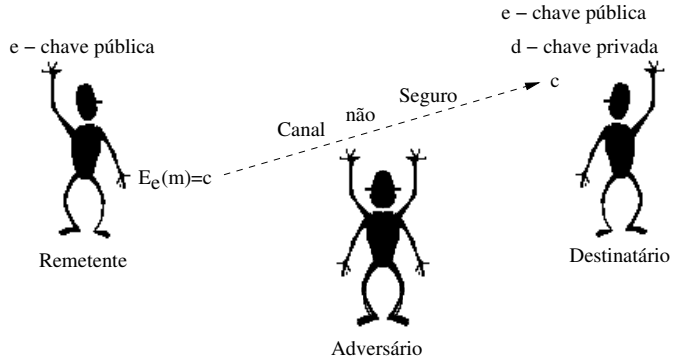
Uma utilização de uma Cifra (Chave Pública)

2a – João decide enviar uma mensagem, $m \in \mathcal{M}$, a José. Calcula $c = E_e(m)$ e envia o texto resultante.



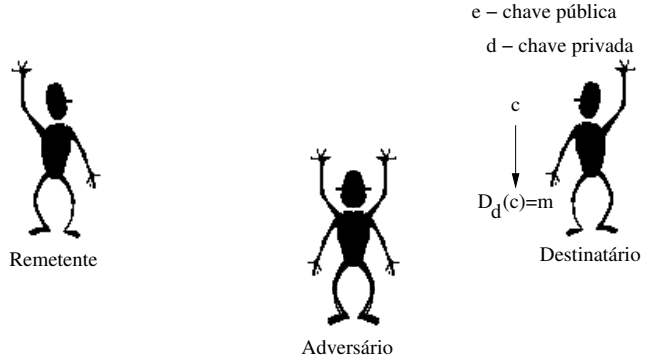
Uma utilização de uma Cifra (Chave Pública)

2b – João decide enviar uma mensagem, $m \in \mathcal{M}$, a José. Calcula $c = E_e(m)$ e envia o texto resultante.



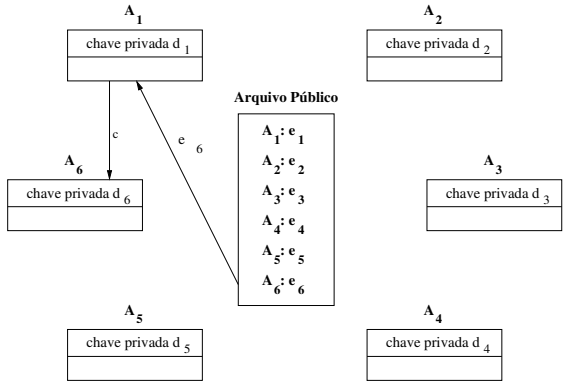
Uma utilização de uma Cifra (Chave Pública)

3 – Ao receber a mensagem o José calcula $D_d(c) = m$ recuperando deste modo a mensagem original.



Estabelecer e Manter Chaves Públicas

Numa rede de chaves públicas cada entidade tem um par (chave pública,chave privada). Para assegurar um mecanismo de estabelecimento e manutenção de chaves basta criar um repositório de chaves, usualmente designado por *Arquivo Público*.



Vantagens e Desvantagens

Vantagens das Cifras de Chaves Públicas

1. Só a chave privada deve permanecer secreta.
2. As chaves podem ser mantidas por largos períodos de tempo.
3. Mesmo que o número de entidades envolvidas seja elevado o número de chaves permanece baixo (comparado com as chaves simétricas).

Desvantagens das Cifras de Chaves Públicas

1. A autenticidade das chaves públicas tem de ser, de alguma forma, assegurado.
2. São consideravelmente mais lentos que os sistemas de chaves simétricas no que diz respeito ao processamento da informação.
3. O comprimento das chaves é em geral bastante maior do que nos sistemas de chaves simétricas.
4. A segurança destes sistemas é baseada em assumpções (ainda não demonstradas) sobre dificuldade computacional de certo tipo de problemas.
5. O seu historial é recente (década de 1970).

Avaliação de Ferramentas Criptográficas

Nível de Segurança número de operações requeridas pelo melhor método conhecido para quebrar o código (difícil de quantificar).

Funcionalidade quais são as primitivas mais eficientes para um dado objectivo.

Métodos de Operação o comportamento das primitivas depende da forma como são aplicadas e de quais os valores que lhe são fornecidos.

Performance eficiência em termos de tempo e/ou espaço que uma ferramenta tem num dado modo de operação.

Facilidade de Implementação a possibilidade que se tem de implementar uma dada ferramenta num dado sistema computacional.

Criptoanálise

Definição (Criptoanálise)

Criptoanálise *é o estudo dos procedimentos necessários para tentar comprometer as técnicas criptográficas, e mais genericamente, os serviços de segurança da informação.*

Definição (Criptoanalista)

Um criptoanalista *é alguém que se dedica à criptoanálise.*

Criptoanálise

Uma cifra diz-se:

- **quebrada totalmente** se é possível obter a chave.
- **quebrada parcialmente** se é possível (de forma sistemática) obter parte do texto claro, mas não a chave.

Ao avaliar-se uma cifra é usual assumir que:

1. o adversário tem acesso a toda a informação transmitida através do canal de comunicação de texto cifrados;
2. o adversário conhece todos os detalhes da cifra à excepção da chave (princípio de Kerckhoff, slide 28).

Em conclusão: uma cifra tem de resistir a um ataque por procura exaustiva no espaço das chaves, para poder ser considerada segura.

Desiderato de Kerckhoff (1883)

1. O sistema deve ser, se não formalmente inquebrável, inquebrável em termos práticos.
2. A quebra do detalhes do sistema não deve implicar os correspondentes.
3. As chaves devem ser facilmente memorizáveis e fáceis de mudar.
4. A mensagem cifrada deve poder ser enviada telegraficamente.
5. Os mecanismos de cifragem devem ser transportáveis e devem poder ser operados por uma só pessoa.
6. O sistema deve ser simples de usar, não requerendo uma longa lista de regras ou um raciocínio complicado.

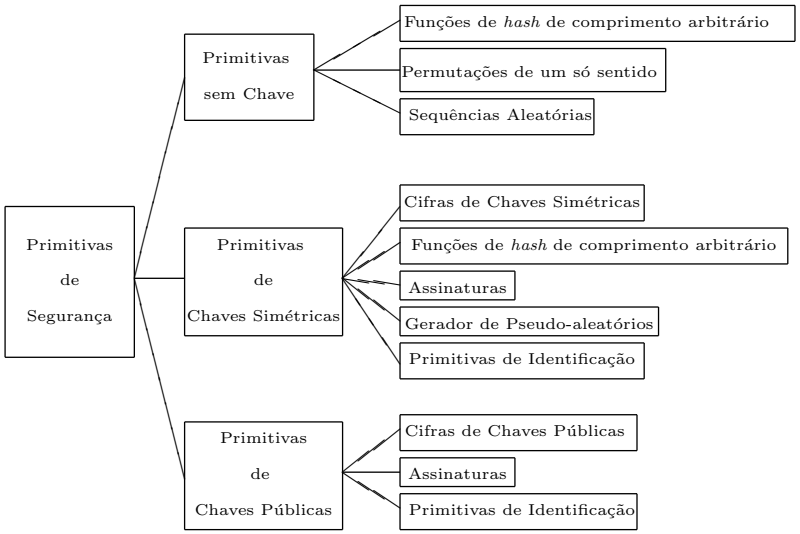
Definição (Princípio de Kerckhoff)

Os algoritmos de encriptação devem ser do conhecimento público. A segurança do sistema só se deve basear na chave escolhida.

Ferramentas Criptográficas

- Esquemas de encriptação
- Funções de dispersão («hash»).
- Esquemas de assinaturas digitais.
- Sequências Aleatórias.
- Primitivas de Identificação.

Taxonomia



Terminologia Básica

Definição (Alfabeto de Definição)

$\mathcal{A}$ denota um conjunto finito de símbolos designado por alfabeto de definição.

Definição (Espaço das Mensagens)

$\mathcal{M}$ denota um conjunto designado o espaço das mensagens. *$\mathcal{M}$ consiste de sequências de elementos de um alfabeto de definição («strings»). Um elemento de M é designado por* mensagem de texto claro (não cifrado).

Definição (Espaço das Mensagens Cifradas)

$\mathcal{C}$ denota um conjunto designado por espaço das mensagens cifradas. *$\mathcal{C}$ consiste de sequências de elementos de um dado alfabeto de definição, o qual pode diferir do usado em $\mathcal{M}$. Um elemento de $\mathcal{C}$ é designado por um texto cifrado.*

Terminologia Básica

Definição (Espaço das Chaves)

$\mathcal{K}$ denota um conjunto designado por espaço das chaves. *Um elemento de $\mathcal{K}$ é designado por* chave.

Definição (Função de Encriptação)

Cada elemento $e \in \mathcal{K}$ determina, de forma única, uma bijecção de $calM$ para $\mathcal{C}$, designada por E_e. A bijecção E_e é designada por função de encriptação, *ou* transformação de encriptação.

Definição (Função de Desencriptação)

para cada $d \in \mathcal{K}$, D_d denota a bijecção de C para M. D_d é designada por função de desencriptação, *ou* transformação de desencriptação.

$$D_d(E_e(m)) = m$$

Encriptação

Definição (Encriptação)

O processo de aplicar a transformação E_e a uma mensagem $m \in \mathcal{M}$ é usualmente designado por encriptar m, *ou a* encriptação de m.

Definição (Desencriptação)

O processo de aplicar a transformação D_d a um texto cifrado $c \in \mathcal{C}$ é usualmente designado por desencriptar c, *ou a* desencriptação de c.

Definição (Par de Chaves)

As chaves e e d na definição anterior são designadas por par de chaves, *e usualmente denotadas por (e, d). Note-se que as chaves podem ser iguais.*

Esquema de Encriptação (Cifra)

Em ordem a construir um esquema de encriptação é então necessário seleccionar:

- um alfabeto (finito) de definição, $\mathcal{A}$;
- um espaço de mensagens $\mathcal{M}$;
- um espaço das mensagens cifradas $\mathcal{C}$;
- um espaço de chaves $\mathcal{K}$;
- um conjunto de transformações de encriptação $\{E_e : e \in \mathcal{K}\}$;
- um correspondente conjunto $\{D_d : d \in \mathcal{K}\}$ de transformações de desencriptação.

Esquema de Encriptação (Cifra)

Definição (Esquema de Encriptação (ou cifra))

Um esquema de encriptação *consiste de um conjunto $\{E_e : e \in \mathcal{K}\}$ de transformações de encriptação e um conjunto correspondente $\{D_d : d \in \mathcal{K}\}$ de transformações de desencriptação com a propriedade de que para todo o $e \in \mathcal{K}$ existe uma chave única $d \in \mathcal{K}$ tal que $D_d = E_e^{-1}$; isto é, $D_d(E_e(m)) = m$ para todo o $m \in \mathcal{M}$.*

Um esquema de encriptação e usualmente designado por *cifra*.

Divisibilidade — Definição

Definição (Divisibilidade)

Dados $a, b \in \mathbb{Z}$, com $a \neq 0$, diz-se que, a **divide** *b, e escreve-se $a|b$, se existe $q \in \mathbb{Z}$ tal que $b = aq$.*

Convenção: Quando se escreve $a|b$ está implícito que a $a \neq 0$.

Se $a|b$ também se diz que a **é um divisor de** b, que b **é um múltiplo de** a ou que b **é divisível por** a.

Se a não divide b, escreve-se $a \nmid b$.

Exemplos:

- $-25|225$ porque $225 = -25 \times (-9)$ e $-9 \in \mathbb{Z}$;
- $8 \nmid 36$ porque não existe $q \in \mathbb{Z}$ tal que $36 = 8q$.

Propriedades

Para quaisquer $a, b, c \in \mathbb{Z}$ tem-se:

1. $a|0$, $1|a$ e $a|a$;
2. $a|b \Leftrightarrow a| - b \Leftrightarrow -a|b$;
3. $a|b \wedge b|c \Rightarrow a|c$ (Transitividade);
4. Para quaisquer $x, y \in \mathbb{Z}$, $a|b \wedge a|c \Rightarrow a|bx + cy$;
5. $a|1 \Leftrightarrow a = \pm 1$;
6. $a|b \wedge b|a \Leftrightarrow a = \pm b$;
7. $a, b \in \mathbb{N} \wedge a|b \Rightarrow a \leq b$;
8. Um inteiro não nulo tem um número finito de divisores.

Algoritmo da Divisão Inteira

Teorema (Algoritmo da divisão inteira)

Dados $a, b \in \mathbb{Z}$, com $a \neq 0$, existem $q, r \in \mathbb{Z}$, únicos, tais que

$$b = aq + r \quad \text{e} \quad 0 \leq r < |a|$$

q e r são, respectivamente, o quociente e o resto da divisão inteira de b por a.

Observações:

- $a|b$ se e só se o resto da divisão inteira de b por a é zero.
- Em *C/C++*, os operadores «/» e «%» dão-nos o quociente e o resto da divisão inteira (desde que o divisor e o dividendo sejam inteiros).

Congruência $(\mathrm{mod}\ m)$

Definição (Congruência $(\mathrm{mod}\ m)$)

Para $m \in \mathbb{N}$ a relação de congruência módulo m é a relação definida em $\mathbb{Z}$ por

$$a \equiv b (\mathrm{mod}\ m) \Leftrightarrow m|a - b, \quad a, b \in \mathbb{Z}$$

Se $a \equiv b (\mathrm{mod}\ m)$ diz-se que a é congruente módulo m com b.

Observe-se que $a \equiv b (\mathrm{mod}\ m)$ se e só se a e b têm o mesmo resto quando divididos por m.

Exemplos:

- $25 \equiv 47 (\mathrm{mod}\ 11)$ porque $11|47 - 25$.
- $43 \not\equiv 62 (\mathrm{mod}\ 7)$ porque $7 \nmid 43 - 62$.

Propriedades

Para quaisquer $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{N}$ tem-se:

1. $a \equiv a (\mathrm{mod}\ m)$ (Reflexividade);
2. $a \equiv b (\mathrm{mod}\ m) \Rightarrow b \equiv a (\mathrm{mod}\ m)$ (Simetria);
3. $\left\{ \begin{array}{l} a \equiv b (\mathrm{mod}\ m) \\ b \equiv c (\mathrm{mod}\ m) \end{array} \right. \Rightarrow a \equiv c (\mathrm{mod}\ m)$ (Transitividade);
4. $\left\{ \begin{array}{l} a \equiv b (\mathrm{mod}\ m) \\ c \equiv d (\mathrm{mod}\ m) \end{array} \right. \Rightarrow a + c \equiv b + d (\mathrm{mod}\ m)$;
5. $\left\{ \begin{array}{l} a \equiv b (\mathrm{mod}\ m) \\ c \equiv d (\mathrm{mod}\ m) \end{array} \right. \Rightarrow ac \equiv bd (\mathrm{mod}\ m)$;
6. $a \equiv b (\mathrm{mod}\ m) \Rightarrow \mathrm{mdc}(a, m) = \mathrm{mdc}(b, m)$;
7. $ab \equiv ac (\mathrm{mod}\ m) \Leftrightarrow b \equiv c \left(\mathrm{mod}\ \frac{m}{\mathrm{mdc}(a,m)}\right)$.

Classes de Congruência

Das propriedades 1, 2 e 3 resulta que, para $m \in \mathbb{N}$, a relação de congruência módulo m é uma relação de equivalência em $\mathbb{Z}$.

Às classes de equivalência desta relação de equivalência chamam-se classes de congruência módulo m.

A classe de congruência módulo m a que pertence $a \in \mathbb{Z}$ é representada por $[a]_m$ ou $\overline{a}$.

$$[a]_m = \{b \in \mathbb{Z} : a \equiv b (\mathrm{mod}\ m)\} = \{a + qm : q \in \mathbb{Z}\}.$$

Uma vez que $a \in \mathbb{Z}$ é congruente módulo m com o resto da sua divisão inteira por m, e os m restos possíveis são $0, 1, \ldots, m-2$ e $m-1$, conclui-se que há m classes de congruência módulo m: $[0]_m, [1]_m, \ldots, [m-1]_m$. Assim,

$$\mathbb{Z} = [0]_m \cup [1]_m \cup \cdots \cup [m-1]_m.$$

$(\mathbb{Z}_m, +)$ é um Grupo Abeliano

Para $m \in \mathbb{N}$, por $\mathbb{Z}_m$ representa-se o conjunto das classes de congruência módulo m, isto é,

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Uma vez que

$$\begin{cases} a \equiv c (\mathrm{mod}\ m) \\ b \equiv d (\mathrm{mod}\ m) \end{cases} \Rightarrow a + b \equiv c + d (\mathrm{mod}\ m),$$

pode definir-se uma operação em $\mathbb{Z}_m$ (adição de classes de congruência) por $[a]_m + [b]_m = [a+b]_m$.

$(\mathbb{Z}_m, +)$ é um grupo abeliano.

Neste grupo o elemento neutro é $[0]_m$ e o simétrico de $[a]_m$ é $[-a]_m = [m-a]_m$.

Congruência $(\mathrm{mod}\ m)$ em *C*

A definição de classes de congruência $(\mathrm{mod}\ m)$ pode ser replicada numa linguagem de programação através da operação de divisão inteira, mais concretamente pelo resto da divisão inteira.

No caso de uma linguagem de programação o foco não está na demonstração de que dois inteiros são congruentes mas no obter, dado um inteiro, a classe de congruência $(\mathrm{mod}\ m)$ a que ele pertence, recorrendo ao resultado do resto da divisão inteira.

Temos então que ao escrever

$$a = b (\mathrm{mod}\ m)$$

que em *C* seria, `a = b % m;`, obtêm-se a, o representante da classe de congruência $(\mathrm{mod}\ m)$ de b.

Programação

Programação Imperativa (C)

> *Programas = Algoritmos + Estruturas de Dados*
> *Niklaus Wirth*

Programação Orientada para os Objectos (C++)

Classes $\leftrightarrow$ Estrutura de Dados + Operações Internas

> *Programas = Classes (de Objectos) + Relações entre Classes*

Ambiente de Trabalho

- Linguagem de Programa C++
- Ambiente de Trabalho Geany (`https://www.geany.org/`).
- Makefiles — para automatizar o processo de compilação de projectos.

C++: Bibliografia

POO Booch, Grady. 1994. *Object Oriented Design, with Applications*. Redwood City, USA: The Bejamin/Cummings Publishing Company, Inc.

C++ Stroustrup, Bjarne. 1997. *The C++ Programming Language*. Addison Wesley Longman, Inc.

C++ Stroustrup, Bjarne. 2009. *Programming: Principles and Practice Using C++*. Addison Wesley Longman, Inc.

C++ Rodrigues, Pimenta, Pereira, Pedro, & Sousa, Manuela. 1998. *Programação em C++*. 2 edn. FCA, Editora de Informática LDA.

C Kernighan, Brian, & Ritchie, Dennis. 1988. *The C Programming Language*. 2nd edn. Prentice Hall.

Pedro Quaresma, *Programação Orientada para os Objectos*, Departamento de Matemática, Universidade de Coimbra, 2021.[1]

[1] `http://www.mat.uc.pt/~pedro/lectivos/ProgramacaoOrientadaObjectos/apontamentosPOO.pdf`

C++: Páginas de Referência

C++ Standard Library cplusplus.com, `http://www.cplusplus.com/`.

C++ STL C++ STL (Standard Template Library) Tutorial and Examples, `http://www.yolinux.com/TUTORIALS/LinuxTutorialC++STL.html`.

C++: Ficheiros hpp/cpp

A construção de uma biblioteca criptográfica deve-se organizar em torno de um conjunto de classes, especificadas em ficheiros `hpp` e implementadas em ficheiros cpp.

Ficheiros `hpp` Os *Header Files* são ficheiros em que as classes são especificadas, isto é, as estruturas de dados são definidas e aridades dos operadores definida (cabeçalhos (headers) das funções).

Ficheiros cpp Os ficheiros de extensão cpp irão conter o código *C++* que implementa os métodos (funções).

Ambiente de Trabalho — Geany

Geany: multi-plataform; grátis; simples de usar; genérico, mas bem adaptado para o C/C++. `https://www.geany.org/`.

Running Geany on Windows
`https://wiki.geany.org/howtos/win32/running`

Para o descarregar do Geany tem-se
`https://www.geany.org/download/releases/`

Para instalar o compilador *C++* (TDM-GCC)
`http://tdm-gcc.tdragon.net/download`

Makefile

Processo de automatização do procedimento de compilação

Tutorial: Aprenda a criar seu próprio makefile, Darcamo (editado), ver página da disciplina.

```
CC     = g++
FLAGS = -lm

.PHONY: clean all

all: encriptarDS desencriptarDS

clean:
        -rm *.o encriptarDS desencriptarDS

encriptarDS: encriptarDS.cpp cifrasDeslocamento.o
        ${CC} -o $@ $@.cpp  cifrasDeslocamento.o

desencriptarDS: desencriptarDS.cpp cifrasDeslocamento.o
        ${CC} -o $@ $@.cpp cifrasDeslocamento.o
```


Exercícios Práticos, em *C++*

1. Escrever «Olá Mundo».
2. Ler dois inteiros e escreve o valor da sua soma.
3. Implemente em C++ uma classe apropriada para representar os números racionais. Deverá ser possível:
   - declarar (criar) números racionais. Assim como a operação inversa de os «destruir».
   - as operações elementares com números racionais.
   - obter as componentes numerador e denominador de um número racional.
   - simplificar um número racional para a sua versão irredutível.
   - os operadores relacionais de igualdade e de desigualdade
   - Elabore um programa para escrever os primeiros n termos de uma sucessão associada à série harmónica:
   $$H = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$
   sob a forma de fracção.

Criptografia Clássica

Designam-se por *cifras clássicas* as cifras pré-computacionais, isto é, cifras desenvolvidas e utilizadas tendo por base processos mecânicos, ou mesmo manuais.

São, em geral, *cifras fracas*, se se tiver em conta os actuais meios criptoanalíticos à nossa disposição.

- Stinson, Douglas, *Cryptography: Theory and Practice*, CRC, 2006.
- Richard Spillman. *Classical and Contemporary Cryptology*. Prentice Hall, 2005.
- Viktoria Tkotz. *CRIPTOGRAFIA - Segredos Embalados para Viagem*. NOVATEC Editora, São Paulo, Brasil, 2005.