

# Códigos e Criptografia

Cristina Caldeira & Pedro Quaresma

Departamento de Matemática  
Faculdade de Ciências e Tecnologia  
Universidade de Coimbra

2012/2013

1 / 245

## Bibliografia

- Stinson, Douglas, *Cryptography: Theory and Practice*, CRC, 2006.
- A. Meneses, P. van Oorschot, S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- Dominic Welsh, *Codes and Cryptography*, Clarendon Press, 1988.
- Buchman, Johannes, *Introduction to Cryptography*, Springer, 2000.
- Paul Garrett, *The Mathematics of Coding Theory*, Pearson, Prentice Hall, 2004.
- Richard Spillman. *Classical and Contemporary Cryptology*. Prentice Hall, 2005.
- Viktoria Tkotz. *CRIPTOGRAFIA - Segredos Embalados para Viagem*. NOVATEC Editora, São Paulo, Brasil, 2005.

2 / 245

## Programa

- **Introdução aos Códigos e à Criptografia**
  - 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**
- **Cifras por Blocos Simétricas: Criptografia e Criptoanálise**
  - Modos de Operação
  - Cifras Produto
  - Cifras Feistel
  - Cifra FEAL
  - Outras cifras de chave simétrica: DES; IDEA.
  - Criptoanálise Linear e Criptoanálise Diferencial
- **Cifras por Blocos de Chave Pública**
  - Funções Unidireccionais e Unidireccionais com Escapatória
  - RSA
  - Criptoanálise da Cifra RSA
  - Outras cifras de chave pública: ElGamal; Knapsack; Goldwasser-Micali
- **Funções de Dispersão**
- **Códigos**

3 / 245

## Informação

## Segurança

## Criptografia

4 / 245

# Kryptós – oculto; graph – escrever

- 4000 a.C. Egípto (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 Civas

- 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 computadores pessoais.

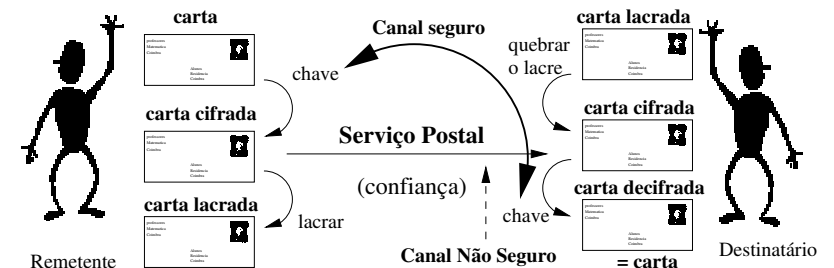
# Algumas Datas (Recentes) Relevantes

- 1977 **Data Encryption Standard**
- 1976 Diffie & Hellman, *New Directions in Cryptography* - Sistemas de Chave Pública (logaritmo discreto, sem aplicação computacional)
- 1978 **Rivest, Shamir, Adelman**, sistema de chave pública, factorização de números primos
- 1985 ElGamal, sistema de chave pública, logaritmo discreto.

# 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 repudição** o produtor da informação não poder negar a autoria da mesma.

## Esquema de Encriptação (Cifra)

Uma primeira definição informal.

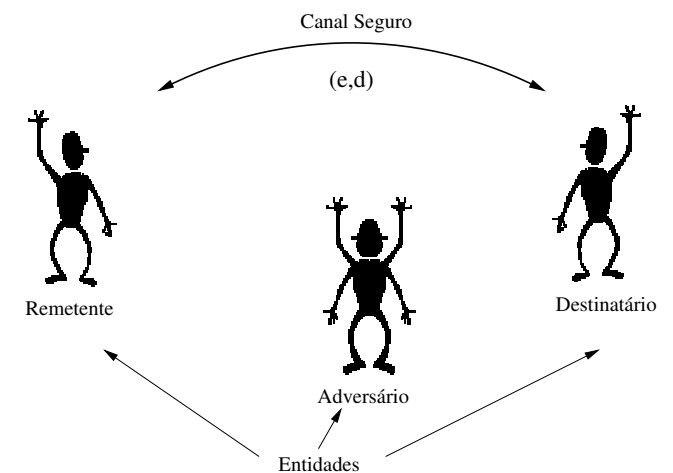
### Definição (Esquema de Encriptação (ou cifra))

*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 é usualmente designado por cifra.*

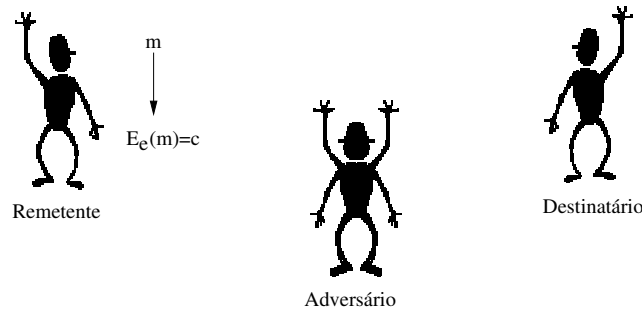
## Uma utilização de uma Cifra de Chaves Simétricas

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



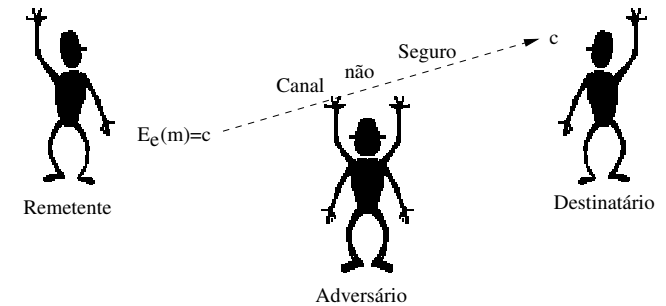
## Uma utilização de uma Cifra (Chaves Simétricas)

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



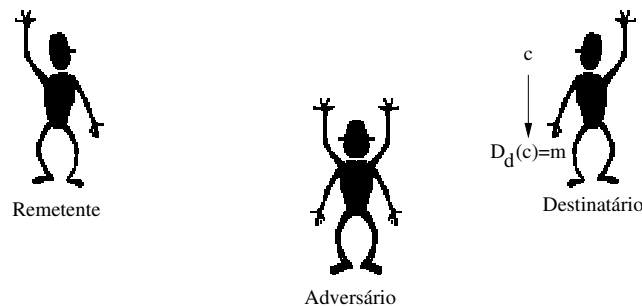
## Uma utilização de uma Cifra (Chaves Simétricas)

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



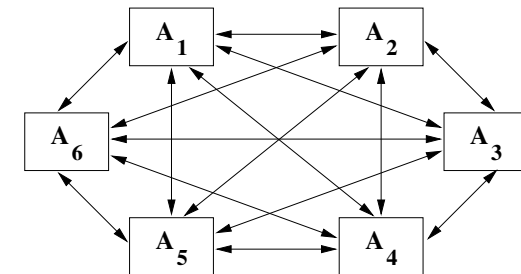
## Uma utilização de uma Cifra (Chaves Simétricas)

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  
 $\binom{n}{2} = \frac{n(n-1)}{2}$ .



É fácil de ver que o manter das chaves é problemático numa  
situação como esta.

## Vantagens e Desvantagens

### Vantagens das Cifras de Chaves Simétricas

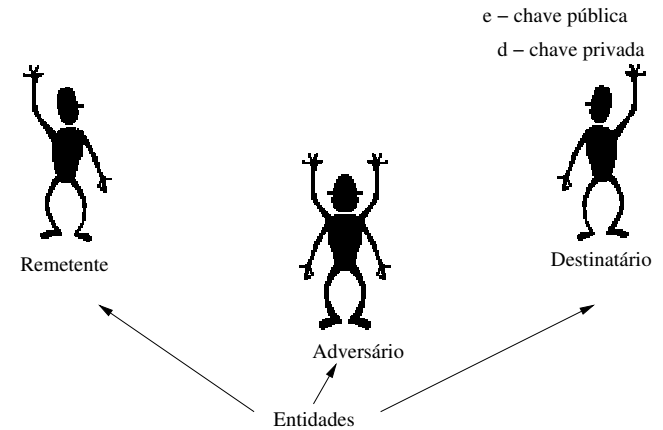
- 1 Podem ser concebidas para terem uma velocidade de processamento de dados elevada.
- 2 As chaves são relativamente pequenas.
- 3 Cifras deste tipo podem ser usadas como primitivas em vários tipos de ferramentas criptográficas
- 4 São facilmente componíveis de forma a construir sistemas criptográficos 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.

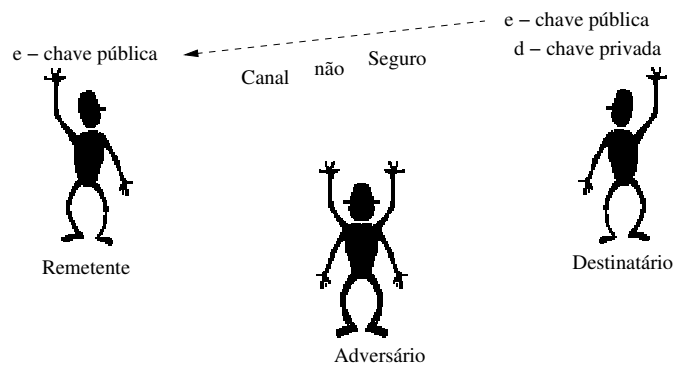
## Uma utilização de uma Cifra de Chave Pública

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



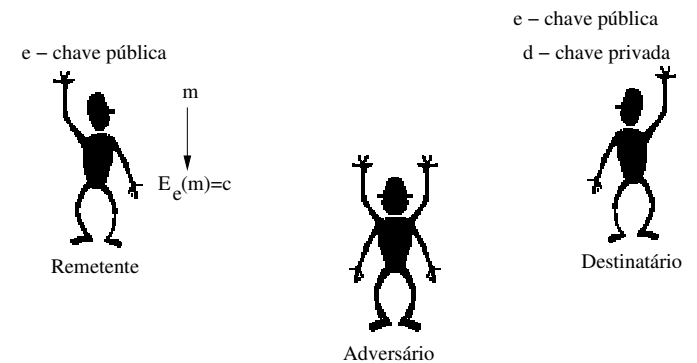
## Uma utilização de uma Cifra (Chave Pública)

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.



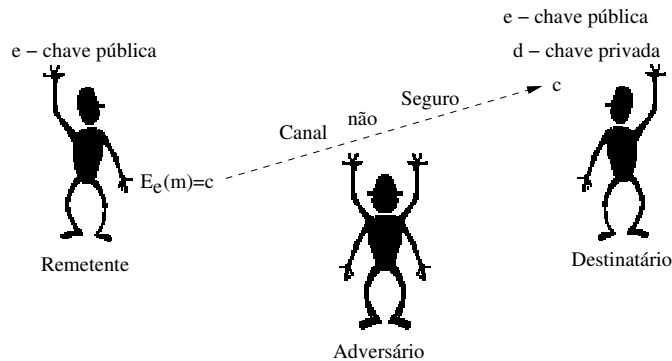
## Uma utilização de uma Cifra (Chave Pública)

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)

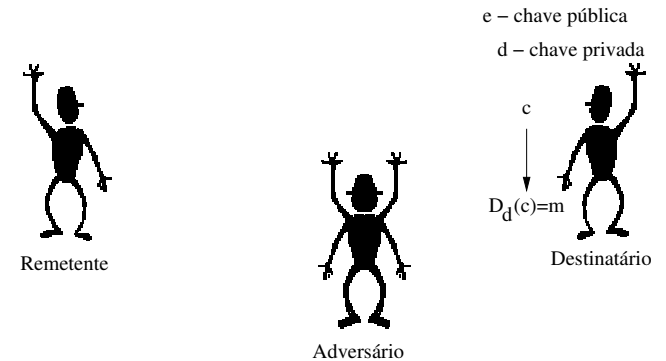
2b – João decide enviar uma mensagem,  $m \in \mathcal{M}$ , a José.  
Calcula  $c = E_e(m)$  e envia o texto resultante.



21 / 245

## Uma utilização de uma Cifra (Chave Pública)

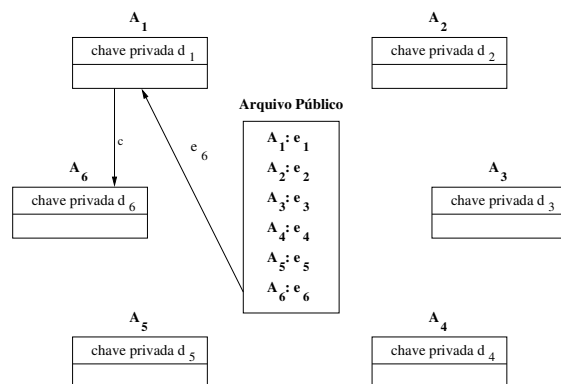
3 – Ao receber a mensagem o José calcula  $D_d(c) = m$   
recuperando deste modo a mensagem original.



22 / 245

## 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*.



23 / 245

## 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 suposições, não demonstradas, de dificuldade computacional de certo tipo de problemas.
- 5 O seu historial é recente (década de 1970).

24 / 245

## 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).

**Em conclusão:** uma cifra tem de resistir a um ataque por procura exhaustiva 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.

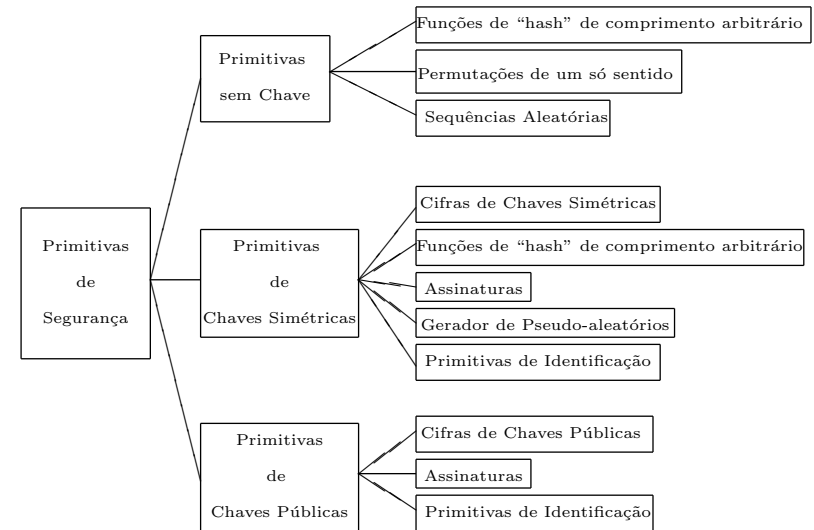
### Definição (Princípio de Kerckhoff)

*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 "hash".
- Esquemas de assinaturas digitais.
- Sequências Aleatórias.
- Primitivas de Identificação.

## Taxonomia



## Terminologia Básica

### Definição (Alfabeto de Definição)

*A* denota um conjunto finito de símbolos designado por alfabeto de definição.

### Definição (Espaço das Mensagens)

*M* denota um conjunto designado o espaço das mensagens. *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)

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

## Terminologia Básica

### Definição (Espaço das Chaves)

*K* denota um conjunto designado por espaço das chaves. Um elemento de *K* é designado por chave.

### Definição (Função de Encriptação)

Cada elemento  $e \in K$  determina, de forma única, uma bijecção de *M* para *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  $d \in K$ ,  $D_d$  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)

### 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  $e \in \mathcal{K}$  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 é usualmente designado por cifra.

## Esquema de Encriptação (Cifra)

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

- um alfabeto (finito) de definição;
- 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.

## 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.