

# Mestrado em Engenharia Informática (MEI)

# Mestrado Integrado em Engenharia Informática

## (MiEI)

Perfil de Especialização **CSI** : Criptografia e Segurança da Informação

Engenharia de Segurança



# Tópicos

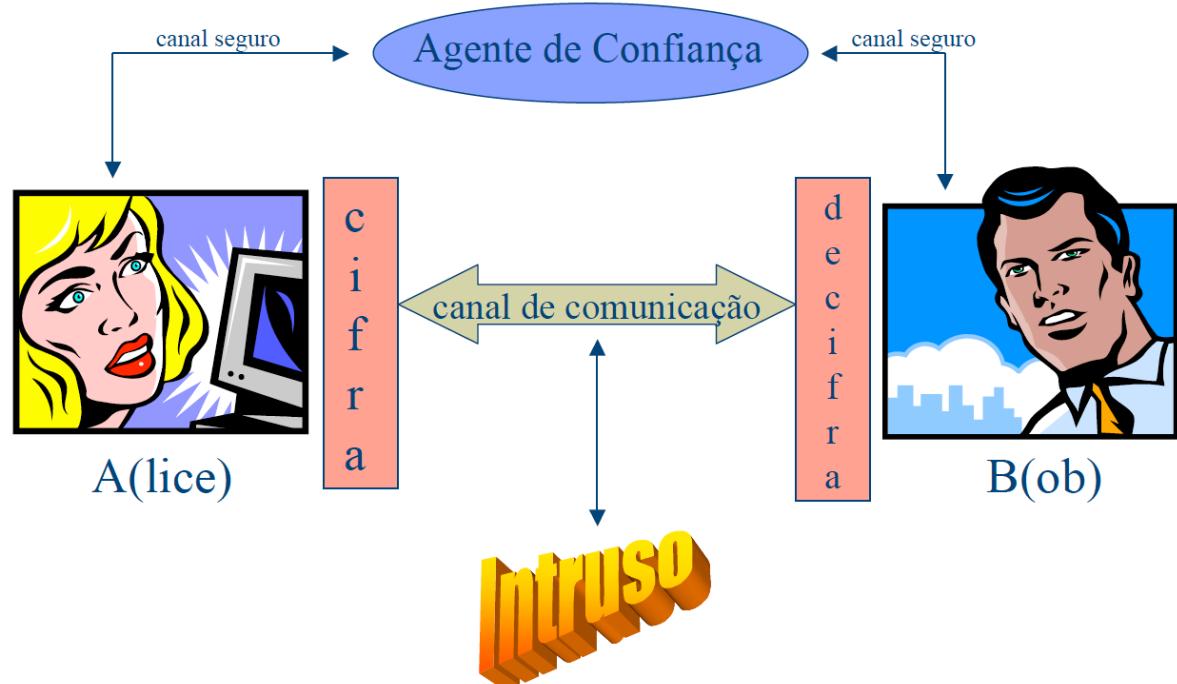
- **Parte I: Criptografia – conceitos básicos**
- Parte II: Exemplos de Cifras Clássicas

Nota: Apontamentos baseados nos slides de “Tecnologia Criptográfica” do Professor José Bacelar Almeida (com permissão do mesmo)



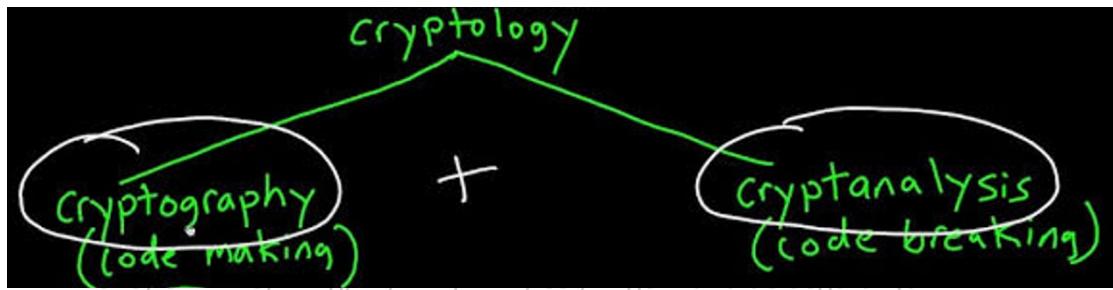
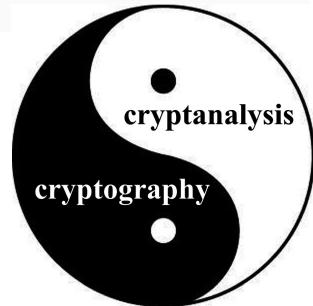
# O que é a criptografia?

- Historicamente, a **Criptografia** consiste no estudo de técnicas que procuram tornar possível a comunicação secreta entre duas partes sobre um canal aberto.
- Objetivos da criptografia:
  - Confidencialidade** ;
  - Integridade**;
  - Autenticação**;
  - Não repúdio**;
  - Controlo de acesso**.



# Criptoanálise

- Em oposição, a **Criptoanálise** tenta gorar os objetivos da Criptografia.
- Quando se tem sucesso ao comprometer (atacar) os objetivos de uma técnica criptográfica, dizemos que essa técnica foi quebrada.
- Conjuntamente, a Criptografia e a Criptoanálise formam uma área a que chamamos de **Criptologia**.
- Como área científica, a Criptologia tem profundos pontos de contacto com a Matemática e as Ciências da Computação.



# Criptografia Moderna

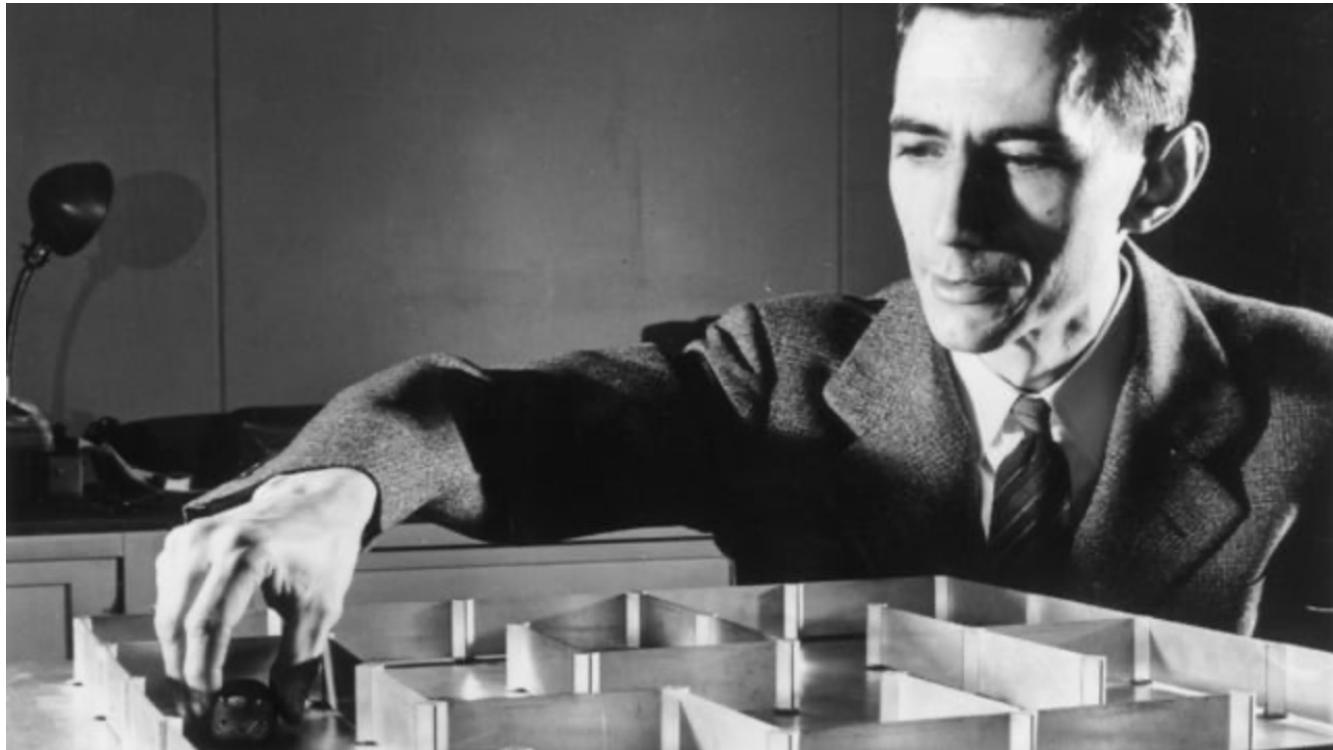
- A Criptografia existe desde a antiguidade, normalmente associada a actividades militares e diplomáticas.
- A segurança dependia, em grande parte, do secretismo que rodeava as técnicas utilizadas (o que, historicamente, se revelou “catastrófico”).
- Esta tendência fez-se notar ainda no Século XX, durante as 1<sup>a</sup> e 2<sup>a</sup> Guerras Mundiais e prolongou-se durante as primeiras décadas da Guerra Fria.
- Só no princípio dos anos 70 surgiu como área de investigação académica de reconhecimento generalizado.
- Hoje é reconhecida a importância de eliminar o secretismo como factor na segurança dos sistemas criptográficos.



**IT security should be your  
number one priority.  
Security through obscurity  
is not security at all.**

# Alguns marcos na história da Criptografia Moderna

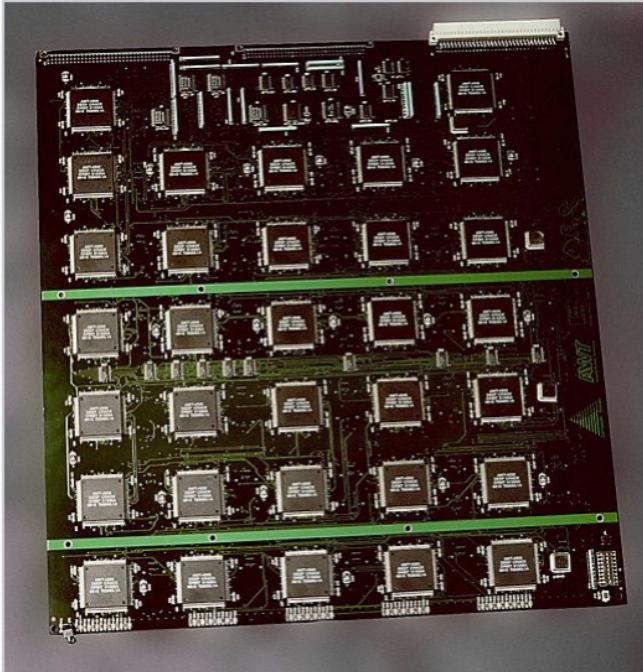
- **1948-1949** – *Claude Shannon* desenvolve a Teoria da Informação que permite formalizar noções de segurança, dando início ao estudo da Criptografia como uma área científica.



Video de <https://thebitplayer.com>

# Alguns marcos na história da Criptografia Moderna

- **1970-1977** – Desenvolvimento e estandardização do *Data Encryption Standard (DES)*.



The EFF's US\$250,000 DES cracking (1998) machine contained 1,856 custom chips and could **brute force** a DES key in a matter of days — the photo shows a two-sided DES Cracker circuit board fitted with 64 Deep Crack chips



The EFF's DES cracker "Deep Crack" custom microchip

Imagens de [https://en.wikipedia.org/wiki/EFF\\_DES\\_cracker](https://en.wikipedia.org/wiki/EFF_DES_cracker)

# Alguns marcos na história da Criptografia Moderna

- **1976** – Artigo científico de (*Diffie & Hellmann*) definindo os princípios da criptografia de chave pública.

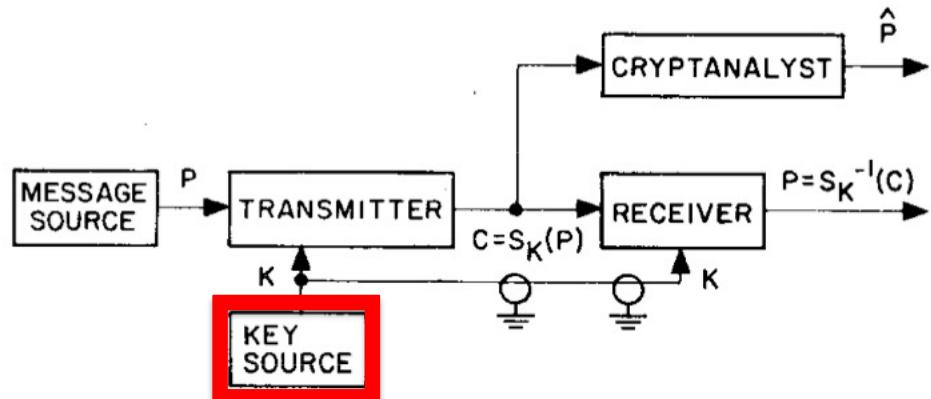


Fig. 1. Flow of information in conventional cryptographic system.

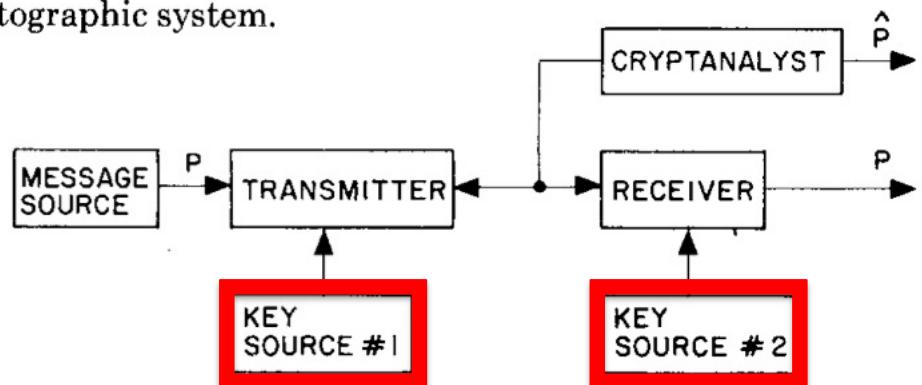


Fig. 2. Flow of information in public key system.

Imagens de <https://ee.stanford.edu/~hellman/publications/24.pdf>

# Alguns marcos na história da Criptografia Moderna

- **1978 – Rivest, Shamir e Adleman** “descobrem” a primeira cifra assimétrica: o RSA.

## Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be “signed” using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in “electronic mail” and “electronic funds transfer” systems.

A message is encrypted by representing it as a number  $M$ , raising  $M$  to a publicly specified power  $e$ , and then taking the remainder when the result is divided by the publicly specified product,  $n$ , of two large secret prime numbers  $p$  and  $q$ . Decryption is similar; only a different, secret, power  $d$  is used, where  $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$ . The security of the system rests in part on the difficulty of factoring the published divisor,  $n$ .

Imagens de <https://people.csail.mit.edu/rivest/Rsapaper.pdf>



# Alguns marcos na história da Criptografia Moderna

- 1985 – “Descoberta” da cifra assimétrica *El Gamal*.

**Abstract—A new signature scheme is proposed, together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.**

Imagen de <https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf>

# Alguns marcos na história da Criptografia Moderna

- **1985** – É mencionada a utilização das curvas elípticas na criptografia (por Neal Koblitz e Victor S. Miller, de forma independente), mas que só passam a ser utilizadas (em larga escala) a partir de 2004.

## Elliptic Curve Cryptosystems

By Neal Koblitz

*This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday*

**Abstract.** We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over  $GF(2^n)$ . We discuss the question of primitive points on an elliptic curve modulo  $p$ , and give a theorem on nonsmoothness of the order of the cyclic subgroup generated by a global point.

Imagen de <https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf>

### Use of Elliptic Curves in Cryptography

Victor S. Miller

Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598

#### ABSTRACT

We discuss the use of elliptic curves in cryptography. In particular, we propose an analogue of the Diffie-Hellmann key exchange protocol which appears to be immune from attacks of the style of Western, Miller, and Adleman. With the current bounds for infeasible attack, it appears to be about 20% faster than the Diffie-Hellmann scheme over  $GF(p)$ . As computational power grows, this disparity should get rapidly bigger.

Imagen de [https://link.springer.com/content/pdf/10.1007%2F3-540-39799-X\\_31.pdf](https://link.springer.com/content/pdf/10.1007%2F3-540-39799-X_31.pdf)

# Alguns marcos na história da Criptografia Moderna

- **2001** – Escolha do substituto do DES: *Advanced Encryption Standard (AES)*.

Federal Information  
Processing Standards Publication 197

November 26, 2001

## Announcing the ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS PUB 197).
2. **Category of Standard.** Computer Security Standard, Cryptography.
3. **Explanation.** The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

# Alguns marcos na história da Criptografia Moderna

- **2016 – Report on Post-Quantum Cryptography, NIST.**
  - Criptografia pós-quântica é o estudo de modelos/algoritmos criptográficos a serem utilizados contra adversários que tenham acesso a um computador quântico, já que muitos dos algoritmos utilizados atualmente podem ser quebrados num computador quântico.

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-----	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

*It is unclear when scalable quantum computers will be available. However, in the past year or so, researchers working on building a quantum computer have estimated that it is likely that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030 for a budget of about a billion dollars [11]. This is a serious long-term threat to the cryptosystems currently standardized by NIST.*

*It is useful to compare the above predictions with the cost of breaking these cryptosystems using classical computers. Cryptosystems offering 80 bits of security or less, which were phased out in 2011-2013, are at the greatest risk: they can be broken now at a cost ranging from tens of thousands to hundreds of millions of dollars [12, 13, 14, 15]. Cryptosystems offering 112 bits of security are likely to remain secure for some time: they may be breakable for a budget of a billion dollars in 30 to 40 years<sup>3</sup> (using classical computers).*

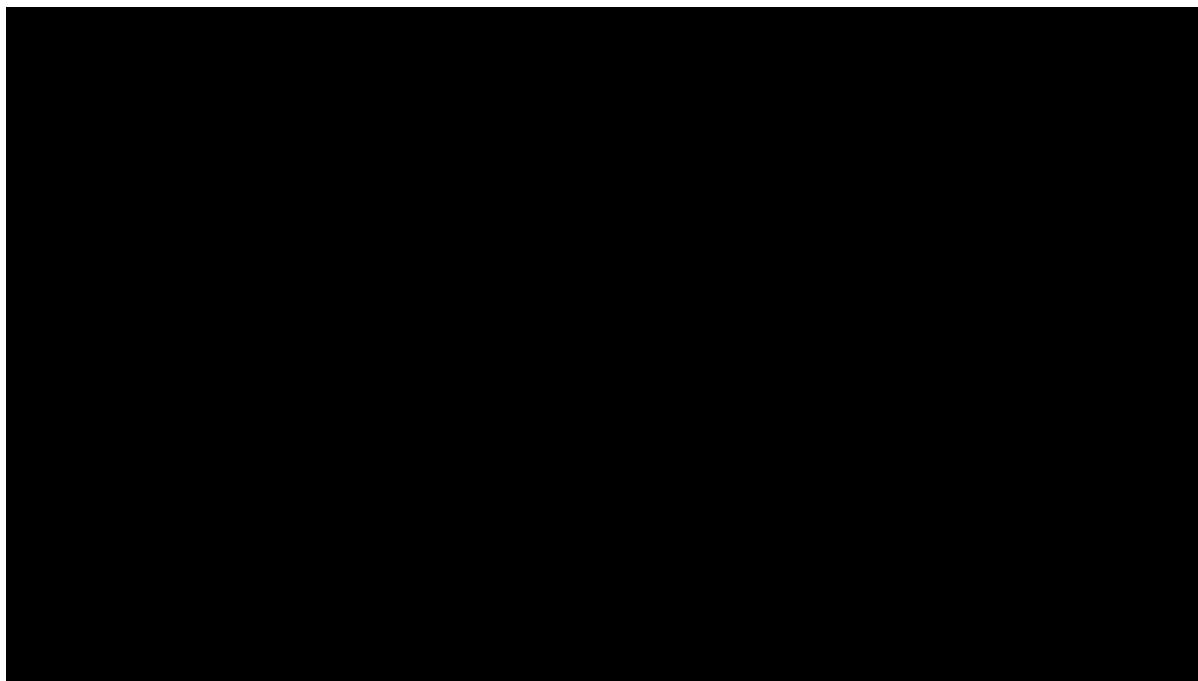
Thus, transitioning from 112 to 128 (or higher) bits of security is perhaps less urgent than transitioning from existing cryptosystems to post-quantum cryptosystems. This post-quantum transition raises many fundamental challenges.

Imagens de <https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf>



# Alguns marcos na história da Criptografia Moderna

- **2016 - 2024 – Post-Quantum Cryptography Standardization, NIST.**
  - Processo para estandardização de um ou mais *quantum-resistant public-key cryptographic algorithms*.
  - Atualmente na fase 3 (encontrados os algoritmos finalistas) do processo de estandardização (<https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions>).



Video de <https://www.nist.gov/video/post-quantum-cryptography-good-bad-and-powerful>

# Princípios de Kerckhoff (1883)

Um sistema criptográfico deve ser seguro mesmo quando todo o sistema é de conhecimento público, à exceção da **chave**.

- 1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
- 2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvenient tomber entre les mains de l'ennemi ;
- 3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
- 4° Il faut qu'il soit applicable à la correspondance télégraphique ;
- 5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
- 6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

**La cryptographie militaire**, Auguste Kerckhoffs, *Journal des sciences militaires*, vol. IX, pp. 5–38, Janvier 1883 ([https://www.petitcolas.net/kerckhoffs/crypto\\_militaire\\_1\\_b.pdf](https://www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf))

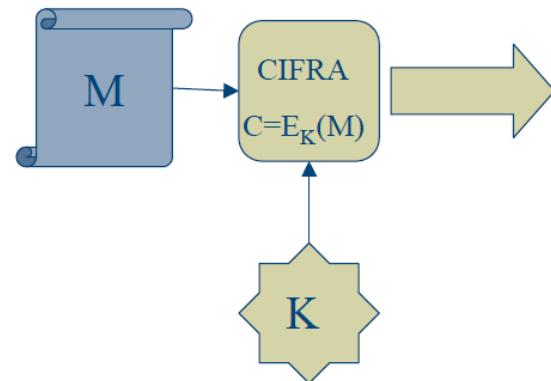


# Princípio de Kerckhoff (1883)

Um sistema criptográfico deve ser seguro mesmo quando todo o sistema é de conhecimento público, à exceção da **chave**.

**Corolário:** a segurança da cifra é assegurada por um parâmetro explícito – a chave ( $K$ ).

$$C = \text{enc}_K(M)$$



# Alguma Terminologia

- **texto limpo (cleartext/plaintext)**: mensagem a transmitir.
- **cifra**: operação que transforma o texto limpo numa mensagem “com significado obscurecido” (**texto cifrado**).
- **chave**: parâmetro de segurança da operação de cifra.
- **texto cifrado (ciphertext)** ou **criptograma**: texto resultante da aplicação da **cifra** e determinada **chave** ao **texto limpo**.
- **decifragem**: operação que transforma o **texto cifrado** no **texto limpo**.
- **sistema criptográfico**: especificação das operações de “inicialização”; “cifra” e “decifragem”.
- **ataque**: comprometimento dos objetivos da técnica criptográfica (e.g. obtenção do texto limpo sem conhecimento da chave; descobrir a chave utilizada; etc.).
- **intruso/adversário/inimigo/spy**: entidade que personifica quem pretende comprometer os objetivos da técnica criptográfica.

# Adversários

- A natureza hostil do *ambiente* onde a técnica criptográfica será executada é personificada pelo **adversário** (também designado por intruso, spy, Eve, ...).
- Se o objetivo da técnica for comprometido, diz-se que esta foi objeto de um **ataque** (com sucesso).
- Distinguem-se dois tipos de ataques, dependendo das faculdades atribuídas ao adversário:
  - **Passivo**: o adversário dispõe unicamente da capacidade de escutar o canal de comunicação (i.e. de observar todo o tráfego que circula do canal).
  - **Ativo**: atribui-se adicionalmente capacidade para manipular a informação que circula no canal de comunicação (alterar/bloquear/injectar ou repetir mensagens).

# Definição de Segurança

Uma **técnica criptográfica** diz-se **segura** se nenhum atacante puder ter sucesso a atacá-la.

- Na prática, interessa distinguir os adversários de acordo com a sua capacidade computacional. Dependendo das capacidades que lhe são atribuídas, obtêm-se assim diferentes noções de segurança:
  - **Segurança Absoluta** – quando a segurança é estabelecida perante um adversário sem limitações computacionais (*attackers with high attack potential*).
  - **Segurança Computacional** – quando se considera que o adversário dispõe de limitações do poder computacional “realistas” (e.g., tempo de processamento, capacidade de memória, etc.).
- Como se pode “demonstrar” a segurança ??
  - Métodos matemáticos formais;
  - Investigação teórica nas componentes matemáticas da técnica criptográfica.

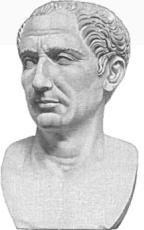
# Tópicos

- Parte I: Criptografia – conceitos básicos
- **Parte II: Exemplos de Cifras Clássicas**

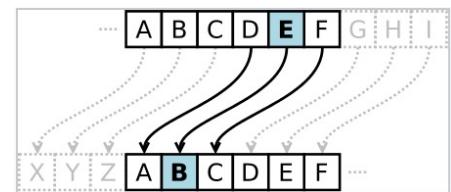
Nota: Apontamentos baseados nos slides de “Tecnologia Criptográfica” do Professor José Bacelar Almeida (com permissão do mesmo)

# Cifra de César

- Cifra conhecida desde a antiguidade clássica.
- Diz-se que terá sido utilizada por Júlio César na campanha da Gália.
- Operação de cifra consiste em realizar um “deslocamento” das letras do alfabeto.



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



- Representação matemática utilizando aritmética modular:
  - Cifra:  $E_n(x) = (x + n) \pmod{26}$ , com letra  $x$  e deslocamento/chave  $n$ .
  - Decifra:  $D_n(x) = (x - n) \pmod{26}$ .
- Exemplo: cifrar a mensagem OsLusitanosNaoSeRendem com chave  $n = 23$  resulta em LPIRPFQXKLPKXLPBOBKABJ.
- Número total de chaves possíveis é de 26 (porquê?).
  - Uma das chaves é muito fraca. Porquê?



# Cifra de César

- Ex.:

- <https://cryptii.com/pipes/caesar-cipher>
- <http://practicalcryptography.com/ciphers/caesar-cipher/>
- <https://www.xarg.org/tools/caesar-cipher/>

# Cifra de César – exemplo de ataque

- Considere-se o criptograma *FXLNTQCLOPNPDLC*.
- Baixo número de chaves permite uma busca exaustiva sobre todas as possíveis chaves:

Criptograma:	F	X	L	N	T	Q	C	L	O	P	N	P	D	L	C
$K^{-1} = +1$ :	G	Y	M	O	U	R	D	M	P	Q	O	Q	E	M	D
...										...					
$K^{-1} = +15$ :	U	M	A	C	I	F	R	A	D	E	C	E	S	A	R
...										...					

- A chave utilizada deve então ter sido  $K = 26 - 15 = 11$ .
- Análise de frequências permite ataques muito mais eficientes... (porquê?)
- E.g.: alta frequência da letra *L* sugere chave  $K = L - A = 11$ .

# Ataque por força bruta (*Brute Force Attack*)

- O ataque apresentado designa-se por **ataque por força bruta** (ataque por busca exaustiva sobre todas as possíveis chaves).
- Esse ataque caracteriza-se por o adversário percorrer todo o espaço de chaves na expectativa de encontrar o texto limpo original.
- É normalmente tido como um ataque que é sempre passível de ser aplicado a uma cifra.
- ... mas cuja *viabilidade* se encontra condicionada pelo tempo que demora percorrer todo o espaço de chaves!!!
- Pode, portanto, ser ultrapassado adotando tamanhos razoáveis para as chaves.

# Ataque por força bruta (*Brute Force Attack*)

- O que é que se considera como tamanho razoável para as chaves?
  - Nota: questão só faz sentido se considerarmos adversários limitados computacionalmente.
- Note que a dimensão do espaço de chaves é exponencial em relação ao tamanho da chave. Um incremento de um bit no tamanho da chave duplica o espaço de chaves disponível.
- Exemplos de tempos de execução (sem utilização de computadores quânticos):

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at $10^6$ decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8 \text{ minutes}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142 \text{ years}$	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$	$5.4 \times 10^{18} \text{ years}$
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$	$5.9 \times 10^{30} \text{ years}$
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$	$6.4 \times 10^6 \text{ years}$

- Considera-se que chaves com tamanho de 112 bits (espaço de chaves de  $2^{112}$ ) permanecerão seguras por mais algum tempo (sem utilização de computadores quânticos)

classical computers. Cryptosystems offering 80 bits of security or less, which were phased out in 2011-2013, are at the greatest risk: they can be broken now at a cost ranging from tens of thousands to hundreds of millions of dollars [12, 13, 14, 15]. Cryptosystems offering 112 bits of security are likely to remain secure for some time: they may be breakable for a budget of a billion dollars in 30 to 40 years<sup>3</sup> (using classical computers).

Fonte: <https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf>

# Cifra por substituição mono-alfabética

- Generaliza a cifra de César permitindo “deslocamentos” diferentes para as diferentes letras do alfabeto.
- Por exemplo:

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

Imagen de [https://www.tutorialspoint.com/cryptography/traditional\\_ciphers.htm](https://www.tutorialspoint.com/cryptography/traditional_ciphers.htm)

- Como atacar?
  - Ataque por força bruta desaconselhado, já que o espaço de chaves é bastante elevado:  $26! = 17,5 * 10^{24}$ .
  - Sabendo qual a língua da mensagem, a análise de frequências das letras permite ataques muito mais eficientes.

# Ataque a uma cifra por substituição mono-alfabética

Considere que numa cifra por substituição mono-alfabética se interceptou o seguinte texto cifrado (e sabe-se que a mensagem transmitida é em texto português):

FPGFBNBVPKFBDMSBEMDMGUCDKDGUGDMUSPMMDBEFLEFEQDCPPGIDEXDCBKPMDDHKPMPFQBUGPSUGHKEGPFBMPXPKSESEB  
SURBHKBHBMEQBFUFSDSBGHKPPFCECPHDKQPDHDKQPFDBADVEDFDCDDCEZPKLDZEDGMPPMNDKPMGDVPEMPDNUPFQDVDMPC  
CPZGEFUQBMCPUGMEOPFSEBHPFBMBFBUDUNPCDPXSEQSDBCBUQBFBCPMUKNEKDUGDMHPKMBFDNPFCPBKENPGBIMSUKD  
SBGJUPGPFKPQEVPBSFSEOEDIUOBMPGKPMQDUKDFQPMPXSPFQKESBMPMMPMQKDZEDGUGDHPKNUFQDQPKKEVPOBJUPPJUPV  
DEMUSPCPKPMHBFCEOAPMJUPFDBMDIEDPPOPMBOADKGHDHKDBHQDQBSBGEFJUEPQDSDB

# Ataque a uma cifra por substituição mono-alfabética

Como proceder à criptoanálise desta cifra?

1. Explora-se o facto de, em Português, existirem diferentes probabilidades de ocorrência de letras nos textos.

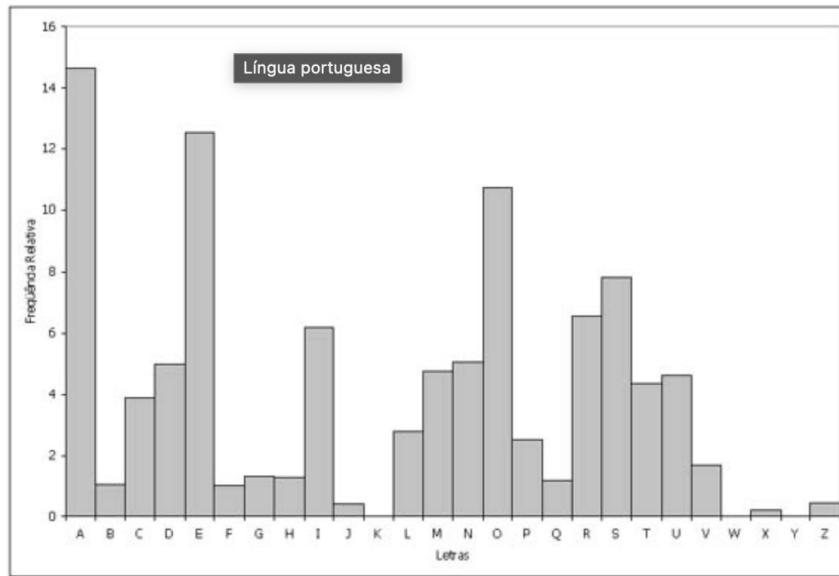


Imagen de [https://pt.wikipedia.org/wiki/Análise\\_de\\_frequência](https://pt.wikipedia.org/wiki/Análise_de_frequência)

- Por outro lado, também são distintas as probabilidades com que estas se agrupam (e.g. “as”, “os”, “es”, “que”, “nao”, ...).

# Ataque a uma cifra por substituição mono-alfabética

Como proceder à criptoanálise desta cifra?

- Note que a probabilidade de ocorrência de letras nos textos difere consoante a língua analisada.

Letra	Francês [9]	Alemão [10]	Espanhol [11]	Português [12]	Esperanto [13]	Italiano <sup>[14]</sup>	Turco	Sueco <sup>[15]</sup>	Polonês <sup>[16]</sup>	Toki Pona [17]	Holandês [18]
a	7.636%	6.51%	12.53%	14.63%	12.12%	11.74%	11.68%	9.3%	8.0%	17.2%	7.49%
b	0.901%	1.89%	1.42%	1.04%	0.98%	0.92%	2.95%	1.3%	1.3%	0.0%	1.58%
c	3.260%	3.06%	4.68%	3.88%	0.78%	4.5%	0.97%	1.3%	3.8%	0.0%	1.24%
d	3.669%	5.08%	5.86%	4.99%	3.04%	3.73%	4.87%	4.5%	3.0%	0.0%	5.93%
e	14.715%	17.40%	13.68%	12.57%	8.99%	11.79%	9.01%	9.9%	6.9%	7.4%	18.91%
f	1.066%	1.66%	0.69%	1.02%	1.03%	0.95%	0.44%	2.0%	0.1%	0.0%	0.81%
g	0.866%	3.01%	1.01%	1.30%	1.17%	1.64%	1.34%	3.3%	1.0%	0.0%	3.40%
h	0.737%	4.76%	0.70%	1.28%	0.38%	1.54%	1.14%	2.1%	1.0%	0.0%	2.38%
i	7.529%	7.55%	6.25%	6.18%	10.01%	11.28%	8.27%*	5.1%	7.0%	14.8%	6.50%
j	0.545%	0.27%	0.44%	0.40%	3.50%	0.00%	0.01%	0.7%	1.9%	3.0%	1.46%
k	0.049%	1.21%	0.01%	0.02%	4.16%	0.00%	4.71%	3.2%	2.7%	5.1%	2.25%
l	5.456%	3.44%	4.97%	2.78%	6.14%	6.51%	5.75%	5.2%	3.1%	10.2%	3.57%
m	2.968%	2.53%	3.15%	4.74%	2.99%	2.51%	3.74%	3.5%	2.4%	4.4%	2.21%
n	7.095%	9.78%	6.71%	5.05%	7.96%	6.88%	7.23%	8.8%	4.7%	11.6%	10.03%
o	5.378%	2.51%	8.68%	10.73%	8.78%	9.83%	2.45%	4.1%	7.1%	7.7%	6.06%
p	3.021%	0.79%	2.51%	2.52%	2.74%	3.05%	0.79%	1.7%	2.4%	3.7%	1.57%
q	1.362%	0.02%	0.88%	1.20%	0.00%	0.51%	0	0.007%	-	0.0%	0.009%
r	6.553%	7.00%	6.87%	6.53%	5.91%	6.37%	6.95%	8.3%	3.5%	0.0%	6.41%
s	7.948%	7.27%	7.98%	7.81%	6.09%	4.98%	2.95%	6.3%	3.8%	4.1%	3.73%
t	7.244%	6.15%	4.63%	4.34%	5.27%	5.62%	3.09%	8.7%	2.4%	4.6%	6.79%
u	6.311%	4.35%	3.93%	4.63%	3.18%	3.01%	3.43%	1.8%	1.8%	3.2%	1.99%
v	1.628%	0.67%	0.90%	1.67%	1.90%	2.10%	0.98%	2.4%	-	0.0%	2.85%
w	0.114%	1.89%	0.02%	0.01%	0.00%	0.00%	0	0.03%	3.6%	2.8%	1.52%
x	0.387%	0.03%	0.22%	0.21%	0.00%	0.00%	0	0.1%	-	0.0%	0.04%
y	0.308%	0.04%	0.90%	0.01%	0.00%	0.00%	3.37%	0.6%	3.2%	0.0%	0.035%
z	0.136%	1.13%	0.52%	0.47%	0.50%	0.49%	1.50%	0.02%	5.1%	0.0%	1.39%

Imagen de  
[https://pt.wikipedia.org/  
 wiki/Frequ%C3%Aancia\\_de\\_letra  
 S](https://pt.wikipedia.org/wiki/Frequ%C3%Aancia_de_letra_S)



# Ataque a uma cifra por substituição mono-alfabética

Como proceder à criptoanálise desta cifra?

2. Realiza-se a análise de frequência de letras no texto cifrado

		% calculated   % expected
P	62x	14.06% ■■■■■
D	54x	12.24% ■■■■■
B	40x	9.07% ■■■■
M	35x	7.94% ■■■
E	31x	7.03% ■■■■■
K	30x	6.8% ■■■
F	28x	6.35% ■■■■
U	25x	5.67% ■■■
G	23x	5.22% ■■■
Q	20x	4.54% ■■
S	20x	4.54% ■■
C	15x	3.4% ■
H	13x	2.95% ■■
N	8x	1.81% ■
O	7x	1.59% ■■
V	7x	1.59% ■
J	5x	1.13% ■
Z	4x	0.91% ■
X	4x	0.91% ■
I	4x	0.91% ■■
A	3x	0.68% ■■■
L	2x	0.45% ■■
R	1x	0.23% ■

Obtido utilizando <https://www.dcode.fr/frequency-analysis>

# Ataque a uma cifra por substituição mono-alfabética

Como proceder à criptoanálise desta cifra?

3. Podemos prosseguir por “palpites”: as letras P, D e B deverão corresponder ao A, E e O. Por outro lado, a existência de várias ocorrências dos pares PM, PF, MP, JUP, ... sugerem-nos a seguinte decifragem parcial:

ME-MO-O-E-MOAS-O-SAS-U-A-A-U-ASU-ESSAO-M--M--A-EE--A--A-O-ESA--ESEM-OU-E-U----EM-OSE-E----O-U-O--O-OS--OMUM-A-O--EEM---E-A--EA-A--EMAO-A--AMA-AA---E--A--A-SEES-A-ESA-A-E-SEA-UEM-A-ASE-E---MU-OS-EU-S--EM--O-EMOSOMOAU-E-AE---A-AO-OOU-OMO-ESU---A-U-AS-E-SOMA-EMS-EO---E-O-S-U-A-O-QUE-EM--E---E-OM---A-U-OSE--ES-AU-AM-ESE--EM---OSESSES--A-A-U-A-E--UM-A-E---E-OQUEEQUE-A-SUE-E--ES-OM---ESQUEMAOSA--AEE-ESO--A-A--A-AO--A-O-O--MQU-E-A-AO

- ... que não parece fazer muito sentido!!! :-(

# Ataque a uma cifra por substituição mono-alfabética

Como proceder à criptoanálise desta cifra?

- Voltando atrás e tentando outra alternativa, obtemos:

NE-NO-O-ERNOAS-O-SAS-U-ARA-U-ASU-ESSAO-N--N-TA-EE--A--A-ORESA-RESENTOU-E-U--R--ENTOSE-ER---O-U-O-RO-OS-TONUN-A-  
O--REEN---E-ARTEA-ARTENAO-A--ANA-AA---ER-A--ASEES-ARESA-A-E-SEA-UENTA-ASE-E---NUTOS-EU-S--EN--O-ENOSONOAU-E-AE---  
TA-AOOOUTONO-ESUR--RA-U-AS-ERSONA-ENS-EOR--E-O-S-URA-O-QUE-ENTRET--E-ON---A-U-OSERESTAURANTESE--  
ENTR--OSESSESTRA--A-U-A-ER-UNTATERR--E-OQUEEQUE-A-SU-E-ERRES-ON---ESQUENAOSA--AEE-ESO--ARA--ARAO-RATO-O--NQU-  
ETA-AO

- que finalmente nos conduz a:

NEMNOGOVERNOASCOISASMUDARAMUMASUCESSAOINFINITADEEMBAIXADORESAPRESENTOUMECUMPRIMENTOSEEXERCICIOCUJO  
PROPOSITONUNCACOMPREENDIDEPARTEAPARTENAOHAVIANADAADIZERFAZIAMSEESGARESAMAVEISEAGUENTAVASEDEZMINUTOS  
DEUMSILENCIOPENOSONO AUGEDAEXCITACAODOOUTONODESURGIRAMUMAPERSONAGENSDEORIGEMOBSCURACOMQUEMENTR  
ETIVECONCILIABULOSEMRESTAURANTESEXCENTRICOSSESSESTRAZIAMUMAPERGUNTATERRIVELOQUEEQUEVAISUCEDERRESPONDILH  
ESQUENAOSABIAELESOLHARAMPARAOPRATOCOMINQUIETACAO

Nota: Texto original de Vasco Pulido Valente, *Às avessas*, Assírio & Alvim, Lisboa 1991  
(conforme <https://crestomatiadequarta.wordpress.com/tag/espioes-e-diplomatas/>)

# Cifra por substituição mono-alfabética

- Ex.:

- <https://www.dcode.fr/monoalphabetic-substitution>
- <https://www.dcode.fr/frequency-analysis>
- <https://www.101computing.net/mono-alphabetic-substitution-cipher/>

# Cifra de Vigenère (substituição poli-alfabética)

- Inventada por Blaise Vigenère (finais sec. XVI). Conhecida como “*le chiffre indéchiffrable*”.
- Intercala múltiplas cifras de César.
- Quebrada no final do sec. XIX por Charles Babbage e Friedrich Kasiski.
- Descrição da cifra:
  - Chave é uma “frase” em que cada letra determina uma substituição
  - Cada substituição é um simples deslocamento (cf. cifra de César) determinado pelo caracter respetivo da chave.
  - Tamanho da chave determina número de substituições utilizadas.
- Representação matemática utilizando aritmética modular (para um alfabeto de tamanho  $\ell$ , e uma chave de tamanho  $m$ ):
  - Cifra:  $C_i = E_K(M_i) = (M_i + K_{(i \bmod m)}) \bmod \ell$ ,
  - Decifra:  $M_i = D_K(C_i) = (C_i - K_{(i \bmod m)}) \bmod \ell$ .



# Cifra de Vigenère (substituição poli-alfabética)

## Exemplo de utilização

- Pretende-se cifrar a mensagem  $M = \text{Cifralndecifravel}$  com a chave  $K = BACO$ .
- Tabela de Vigenère (*tabula recta*):

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

- Operação de cifra:*

Chave:	B	A	C	O	B	A	C	O	B	A	C	O	B	A	C	O	B	A	C	O	B
Texto limpo	C	I	F	R	A	I	N	D	E	C	I	F	R	A	V	E	L				
Criptograma	D	I	H	F	B	I	P	R	F	C	K	J	S	A	X	S	M				

- Observações:
  - A mesma letra não é sempre cifrada da mesma forma;
  - mas se o texto limpo for muito maior do que a chave, os padrões no texto limpo vão-se repercutir no criptograma.
  - As técnicas de criptoanálise desenvolvidas dispõem já de um nível de sofisticação considerável...

# Cifra de Vigenère (substituição poli-alfabética)

- Ex.:
  - <https://www.dcode.fr/vigenere-cipher>
  - <https://cryptii.com/pipes/vigenere-cipher>
- Nota: Tabela de Vigenère (*tabula recta*)

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

# Cifra One-Time-Pad

- Generaliza a cifra de Vigenère com:
  - comprimento da chave é o mesmo (ou maior) da mensagem a cifrar;
  - a chave é completamente aleatória (distribuição uniforme e independente do texto limpo) – originada num gerador de números aleatórios;
  - a chave não pode ser reutilizada em parte ou na sua totalidade;
  - a chave tem de ser mantida em completo segredo pelas partes comunicantes.
- Cifra demonstrada incondicionalmente segura por Claude Shannon (1949).
  - Communication Theory of Secrecy Systems, Claude Shannon  
(<https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>)
- É normalmente descrita operando sobre um alfabeto binário:
  - Operações de cifra/decifragem são simplesmente o *XOR* com a chave.

$$C_i = T_i \oplus K_i \quad M_i = C_i \oplus K_i$$

- Segurança da cifra resulta do facto de o conhecimento do criptograma não resultar na diminuição de incerteza relativa ao conhecimento do texto limpo.
- Os problemas inerentes à geração e distribuição da chave, assim como a necessidade de utilizar um “verdadeiro” gerador de números aleatórios, tornam (na prática) a cifra inviável.

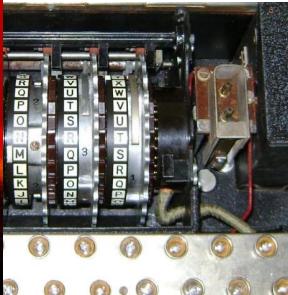
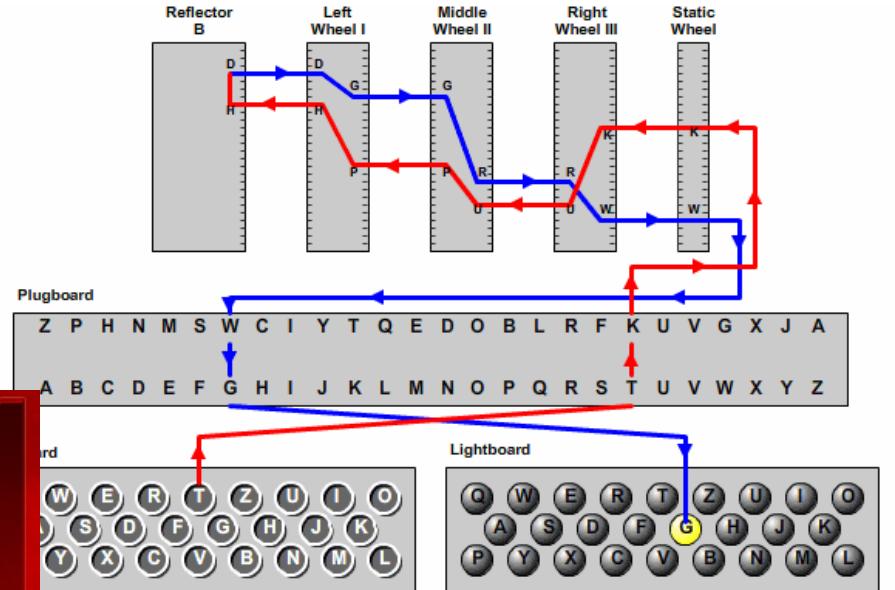
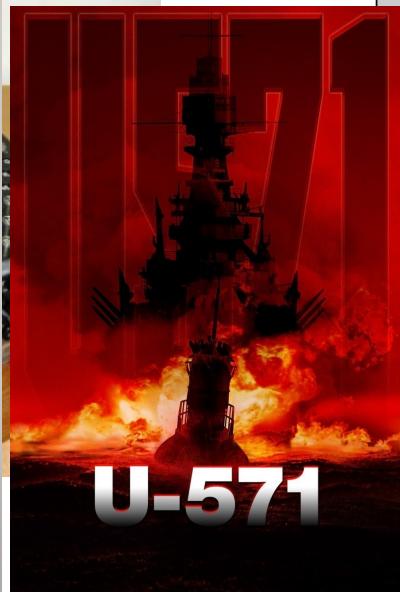
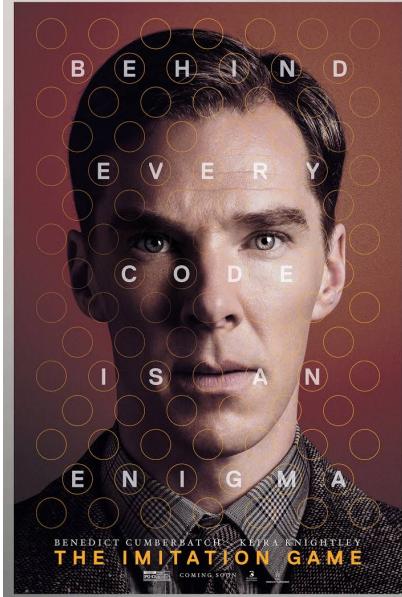
# Cifra One-Time-Pad

- Ex.:

- <https://www.dcode.fr/vernam-cipher>
- [https://www.mobilefish.com/services/one\\_time\\_pad/one\\_time\\_pad.php](https://www.mobilefish.com/services/one_time_pad/one_time_pad.php)

# Mecanização

- Desde 1844, a mecanização simplificou a utilização das cifras de substituição
  - Ex.: Enigma (WWII)



# Mecanização

- Enigma Machine (I/II)

Numberphile



Disponível em [https://www.youtube.com/embed/G2\\_Q9FoD-oQ](https://www.youtube.com/embed/G2_Q9FoD-oQ)

# Mecanização

- Enigma Machine (II/II)



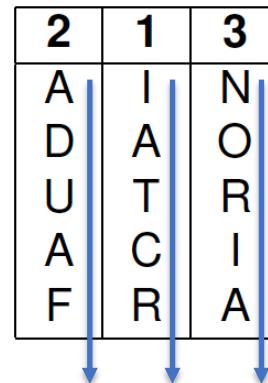
Disponível em <https://www.youtube.com/embed/V4V2bpZlqx8>

# Cifras por Transposição

- O mecanismo de cifra pode afectar as posições dos caracteres, em vez de manipular esses mesmos caracteres.
- E.g. considere-se a **permutação**:  

1	2	3
2	1	3
- Operação de cifra:
  - Para cifrar: AINDAOUTRACIFRA
  - organiza-se a mensagem numa matriz
  - lê-se a matriz seguindo a ordem da chave... (escreve-se por linhas e lê-se por colunas)
  - ...resultando em: IATCRADUAFNORIA

2	1	3
A	I	N
D	A	O
U	T	R
A	C	I
F	R	A



# Cifras por Transposição

- O mecanismo de cifra pode afectar as posições dos caracteres, em vez de manipular esses mesmos caracteres.

- E.g. considere-se a **permutação**:

1	2	3
2	1	3

- Operação de decifra:

- Para decifrar: IATCRADUAFNORIA

- Obter o tamanho da coluna, dividindo o tamanho da mensagem pelo tamanho da chave (permutação), i.e.  $15 / 3 = 5$

- Escrever a mensagem por colunas IATCR ADUAF NORIA, reordenando as colunas de acordo com a permutação

1            2            3

2	1	3
A	I	N
D	A	O
U	T	R
A	C	I
F	R	A

# Cifras por Transposição

- Ex.:
  - <https://www.dcode.fr/transposition-cipher>
  - <https://crypto.interactive-maths.com/simple-transposition-ciphers.html>



Imagen de <https://en.wikipedia.org/wiki/Scytale>

# Combinação de Cifras

- Tendo visto diferentes *cifras simples*...
- ...fará sentido construir uma *cifra complicada* combinando várias dessas cifras mais simples?
- Em particular, será que é legítimo dizer que a segurança dessa nova cifra é maior?
- **Depende!!!**
  - pode acontecer de não trazer valor acrescentado nenhum (e.g. combinando duas cifras por substituição)
  - mas há padrões de combinação que podem ser vantajosos (e.g. intercalando substituições com permutações)

# Em resumo

- Na criptoanálise, explora-se toda a informação disponível, como sejam:
  - a natureza na mensagem transmitida;
  - informação parcial dessa mensagem;
  - histórico sobre a utilização da cifra (e.g. existência de mensagens cifradas com a mesma cifra/chave);
  - possíveis vícios de utilização da cifra (e.g. deficiências na escolha das chaves, etc.).
- Mesmo se existem técnicas incondicionalmente seguras, elas impõem normalmente requisitos de tal maneira fortes à sua utilização que se tornam impraticáveis.
- Por isso, a generalidade das técnicas criptográficas utilizadas atualmente baseiam-se numa noção de segurança onde se limitam as capacidades computacionais do adversário: segurança computacional.
- O *tamanho de chave recomendado* para uma determinada cifra deve ser definido com base no **nível de segurança** pretendido (e.g.  $2^{112}$ ) e de qual a percentagem do tamanho de chave consumida pelas técnicas de criptoanálise conhecidas.

# Bibliografia referenciada

- **La cryptographie militaire**, Auguste Kerckhoffs, *Journal des sciences militaires*, vol. IX, pp. 5–38, Janvier 1883 ([https://www.petitcolas.net/kerckhoffs/crypto\\_militaire\\_1\\_b.pdf](https://www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf))
- **How Claude Shannon Invented the Future** (<https://www.quantamagazine.org/how-claude-shannons-information-theory-invented-the-future-20201222/>)
- **Claude Shannon: Prophet of Information** (<https://thebitplayer.com>)
- **Communication Theory of Secrecy Systems**, Claude Shannon (<https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>)
- **New directions in Cryptography**, Diffie & Hellman (<https://ee.stanford.edu/~hellman/publications/24.pdf>)
- **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**, R.L. Rivest, A. Shamir, and L. Adleman (<https://people.csail.mit.edu/rivest/Rsapaper.pdf>)
- **A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms**, Taher ElGamal (<https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf>)
- **Elliptic Curve Cryptosystems**, Neal Koblitz (<https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf>)
- **Use of Elliptic Curves in Cryptography**, Victor. S. Miller ([https://link.springer.com/content/pdf/10.1007%2F3-540-39799-X\\_31.pdf](https://link.springer.com/content/pdf/10.1007%2F3-540-39799-X_31.pdf))
- **NISTIR 8105 - Report on Post-Quantum Cryptography**, NIST (<https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf>)