

$$\begin{aligned}
& \int f(x) dx = \left( \sum_{j=1}^m a_j y_j(x) \right)' = \sum_{j=1}^m a_j y_j'(x) = \sum_{j=1}^m a_j u_j'(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \rightarrow 0} \frac{\sum_{j=1}^m a_j u_j(x+h) - \sum_{j=1}^m a_j u_j(x)}{h} = \lim_{h \rightarrow 0} \frac{\sum_{j=1}^m a_j u_j(x+h) - \sum_{j=1}^m a_j u_j(x)}{h} = \lim_{h \rightarrow 0} \frac{\sum_{j=1}^m a_j u_j(x+h) - \sum_{j=1}^m a_j u_j(x)}{h} = \\
& F(x) = F(x_0 + \Delta x_0) - F(x_0), \quad I_1 = \int_{x_0}^{x_0 + \Delta x_0} x \rightarrow a, \quad x \rightarrow b, \quad \Delta F = F(x_b + \Delta x_b) - F(x_b), \quad I_2 = \int_{x_b}^{x_b + \Delta x_b} x \rightarrow a, \quad x \rightarrow b, \\
& x_0 \pm y_{n+1} \} (\sqrt{n+2})^2 - (\sqrt{n})^2 \sum_{k=1}^n a_k z_k^2 \lim_{h \rightarrow 0} (\sqrt{n+2} - \sqrt{n}) = \lim_{h \rightarrow 0} \frac{(\sqrt{n+2})^2 - (\sqrt{n})^2}{h} \sum_{k=1}^n a_k z_k^2 \lim_{h \rightarrow 0} (\sqrt{n+2} - \sqrt{n}) = \\
& \left( 1 + \frac{1}{n} \right)^{n+1} < \left( 1 + \frac{1}{n} \right)^n, \quad a = \psi \left( \frac{1}{n} \right) = \left[ \psi \left( \frac{1}{n} \right) \right]^n \left( 1 + \frac{1}{n} \right)^{n+1} < \left( 1 + \frac{1}{n} \right)^n, \quad a = \psi \left( \frac{1}{n} \right) = \left[ \psi \left( \frac{1}{n} \right) \right]^n, \\
& \int \pi f''(x) dx = \int \pi \left( \frac{f'(x)}{h} \right) dx = \int_{h^2}^{h^2+1} x^2 dx \int [u_n(x) + u_{n+1}(x) + \dots + u_m(x)] dx = \int \pi f''(x) dx = \int \pi \left( \frac{f'(x)}{h} \right) dx = \int_{h^2}^{h^2+1} x^2 dx \int [u_n(x) + u_{n+1}(x) + \dots + u_m(x)] dx = \\
& x^3 \left[ \frac{1}{3} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \right] \dots P_n(z_0) = \sum_{k=1}^n a_k z_k^2 \times 0 / \lim_{h \rightarrow 0} f'(x) = \sum_{k=1}^n a_k z_k^2 \left[ \frac{1}{3} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \right] \dots P_n(z_0) = \sum_{k=1}^n a_k z_k^2 \times 0 / \lim_{h \rightarrow 0} f'(x) = \\
& \int f_j(x) dx + C = \sum_{k=1}^n C_k a_k z_k^2 x^k \int \left( \sum_{j=1}^n A_j f_j(x) \right) dx = \sum_{j=1}^n \int f_j(x) dx + C = \sum_{k=1}^n C_k a_k z_k^2 x^k \int \left( \sum_{j=1}^n A_j f_j(x) \right) dx = \sum_{k=1}^n a_k z_k^2 x^k - a_k = (z-a)/z^{m+1} \sum_{k=1}^n a_k z^{k-1} - a_k = (z-a)/z^{m+1} \\
& a_k = a_k z^k - a_k z^k (a_k z^0), \quad P_n(z) = a_k a_k z^k - P_n(z) = a_k a_k z^k - a_k z^k = \sum_{k=1}^n a_k z^k (a_k z^0), \quad P_n(z) = a_k a_k z^k - P_n(z) = \\
& a_k = \psi \left( \frac{1}{n} \right) \quad (a_k a_k z^k)' = \lim_{h \rightarrow 0} \frac{a_k(a_k z^k + h) - a_k(a_k z^k)}{h} = \quad a = \psi \left( \frac{1}{n} \right) \quad (a_k a_k z^k)' = \lim_{h \rightarrow 0} \frac{a_k(a_k z^k + h) - a_k(a_k z^k)}{h} = \\
& \lim_{h \rightarrow 0} a_k \left( \frac{a_k z^k + h}{a_k z^k} \right)^{1/n} = \lim_{h \rightarrow 0} a_k \left( 1 + \frac{h}{a_k z^k} \right)^{1/n} = \lim_{h \rightarrow 0} a_k \left( 1 + \frac{h}{a_k z^k} \right)^{1/n} = \lim_{h \rightarrow 0} a_k \left( 1 + \frac{h}{a_k z^k} \right)^{1/n} = \lim_{h \rightarrow 0} a_k \left( 1 + \frac{h}{a_k z^k} \right)^{1/n} = \\
& y_j(x) = \sum_{k=1}^n a_k z_k^k \times 0, \quad I_1 = \int_{z_0}^{z_0 + \Delta z_0} \frac{1}{z} dz, \quad I_2 = \int_{z_0}^{z_0 + \Delta z_0} \frac{1}{z} dz, \quad P_n(z_0) = \sum_{k=1}^n a_k z_k^k \times 0, \quad I_1 = \int_{z_0}^{z_0 + \Delta z_0} \frac{1}{z} dz, \quad I_2 = \int_{z_0}^{z_0 + \Delta z_0} \frac{1}{z} dz,
\end{aligned}$$

Hello.

Epiphany is upon you. Your pilgrimage has begun. Enlightenment awaits.



Good luck.

3301

# Criptografia

Anna Rio • FIB • 2016



# EL PRESENT



# EL PASSAT

- Criptografia recreativa



- Criptografia clàssica



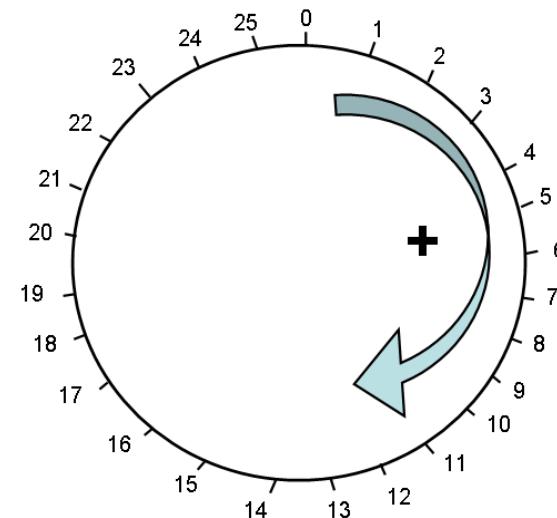
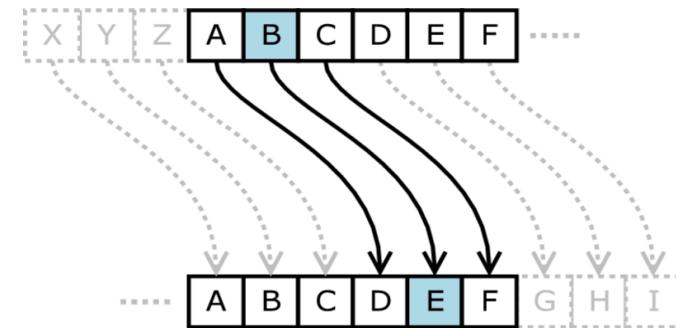
# HISTÒRIA DE LA CRIPTOGRAFIA



# XIFRAT DE CÈSAR

Juli Cèsar (segle I a.C.)

Cada lletra es substitueix per una altra, la que ocupa **k** posicions més enllà en l'alfabet, considerat cíclicament



<http://tools.zenverse.net/caesar-cipher/>

# CRIPTOGRAFIA CLÀSSICA

- Anterior a l'aparició dels ordinadors
- Té com a únic objectiu la confidencialitat
- Usos militars i diplomàtics
- Generalment usa l'alfabet {A, B, C, D, ....} (26 caràcters)
- Les transformacions bàsiques que utilitza són:

**Substitució:** cada lletra del missatge es substitueix per una altra, segons una determinada permutació de l'alfabet

Hi ha mètodes de substitució *polialfabètica*, considerant dígrafs, trígrafs...

**Transposició:** les mateixes lletres del missatge es col.loquen en un ordre diferent; es permuten, doncs, les posicions

# CRIPTOANÀLISI

- **Objectiu:** realització de transformacions criptogràfiques, de xifrat o desxifrat, sense disposar de la clau (trencar el sistema)
- **Hipòtesi:** el criptoanalista (l'atacant) coneix l'algoritme criptogràfic.
  - COA: Ciphertext Only Attack
  - KPA: Known Plaintext Attack
  - CPA: Chosen Plaintext Attack
  - ACPA: Adaptive Chosen Plaintext Attack
  - CCA: Chosen Ciphertext Attack

# LA CERCA EXHAUSTIVA

- Permutacions de 26 símbols ( ... i cicles?)

$26! = 403291461126605635584000000$

- És de l'ordre de  $10^{27}$   $O(2^{89})$

Fent un milió de proves per segon

trigaríem uns  $10^{13}$  anys

(l'edat estimada de l'univers és  $10^{10}$  anys...)

- La potència de càlcul actual es situa per sota de  $2^{80}$  operacions !!



# PERÒ ÒBVIAMENT...

Un **nombre de claus** *gran* no és suficient per fer segur un criptosistema

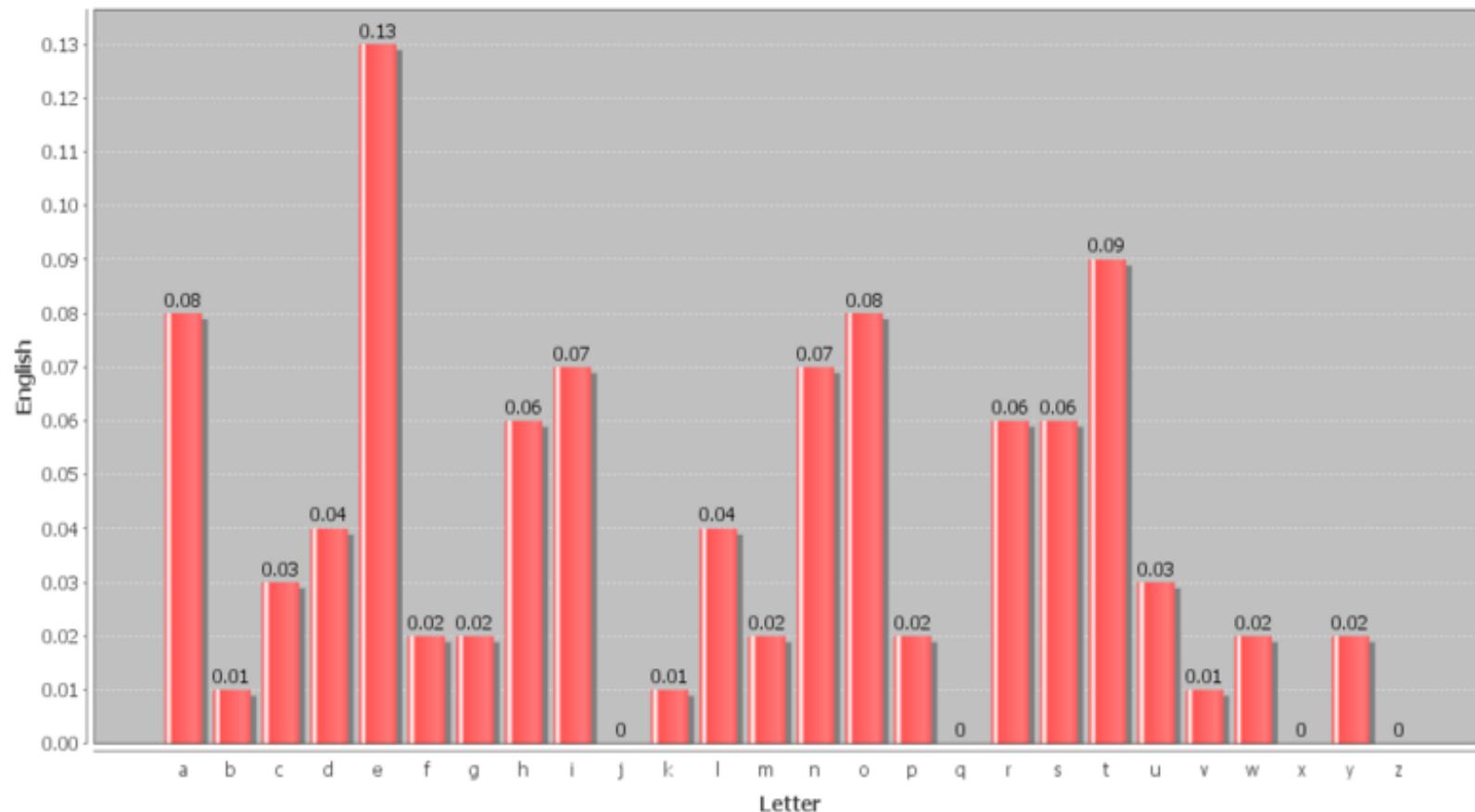
El teu oponent sempre utilitzarà la seva millor estratègia per vèncer, no l'estratègia que tu vulguis que utilitzi

La seguretat d'un criptosistema sempre dependrà del **millor mètode conegit** per trencar-lo

Mentre es desenvolupin nous i millors mètodes, el nivell de seguretat només pot fer que **empitjorar**, mai millorar

# ANÀLISI ESTADÍSTIC

English Language Letter Frequency Histogram

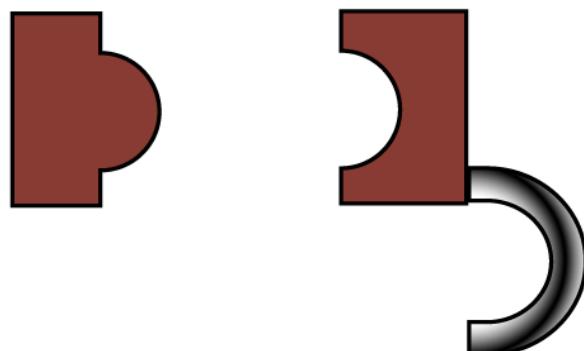


Mètodes de substitució: **repeticions** en el criptograma provenen de repetitions en el missatge

# DOS MÈTODES ACTUALS



Private key      Public key



## Criptografia de clau secreta (**Symmetric Ciphers**)

Hi ha una única clau (secreta) que **comparteixen** emissor i receptor. La seguretat del sistema rau en mantenir en secret aquesta clau

## Criptografia de clau pública (**Asymmetric ciphers**)

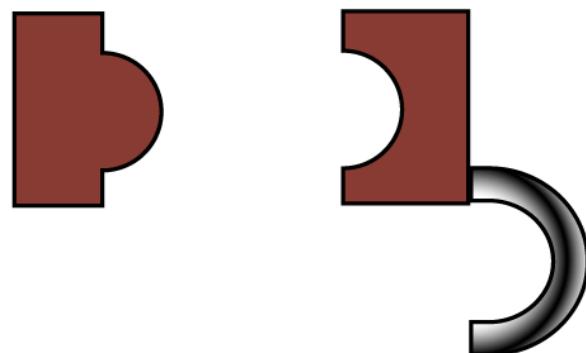
Cada usuari té un parell de **claus**, una **privada** i una altra **pública**. La seguretat del sistema rau en la **dificultat computacional** d'obtenir la clau privada a partir de la pública

# DOS MÈTODES ACTUALS



Principis de confusió i  
difusió

Private key      Public key



Complexitat  
computacional

# DEFINICIÓ DE CRIPTOSISTEMA

Un criptosistema és una 5-tupla  $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

- $\mathcal{M}$  conjunt finit de possibles missatges
- $\mathcal{C}$  conjunt finit de possibles criptogrames
- $\mathcal{K}$  conjunt finit de possibles claus
- $\mathcal{E}$  conjunt de regles de xifrat

$$E : \mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{C}$$

- $\mathcal{D}$  conjunt de regles de desxifrat

$$D : \mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{M}$$

$$D( E(x, k), k ) = x$$

# CRIPTOSISTEMA

(Algoritme) Xifrar amb clau k:  $e_k(m)=E(m,k)$

(Algoritme) Desxifrar amb clau k:  $d_k(c)=D(c,k)$

$$d_k(e_k(m))=m$$

➤  $e_k$  funció injectiva: entrades diferents, sortides diferents

**Principi de Kerchoff:** La seguretat d'un criptosistema ha de dependre únicament del secret de la clau, no del secret de l'algoritme de xifrar

# CRIPTOSISTEMA

- Per a cada clau  $k$ , els algoritmes  $e_k$  i  $d_k$  han de ser **eficients**
- Conegut un criptograma  $c$ , calcular  $d_k(c)$  sense conèixer  $k$  ha de ser un **problema difícil**
- Altres condicions segons el tipus d'atac
- Atac sempre possible: **força bruta (cerca exhaustiva)**

**condiciona el tamany de l'espai de claus**

# ALFABETS, CODIS...

Missatges i criptogrames poden estar escrits en alfabets qualssevol

Un **codi** és un criptosistema de clau fixa, un sistema de transcripció

En general, els codis s'utilitzen per passar de l'alfabet corrent a un altre més en consonància amb les màquines: codi Morse, **codi ASCII**,...

- Per al tractament informàtic, podem suposar que la **informació** està **digitalitzada**. Un missatge, text, document, dada, i qualsevol tipus d'informació és una cadena de símbols de l'alfabet binari

$$\mathcal{M} = \mathcal{C} = \{0, 1\}^*$$

**String**    Informació!

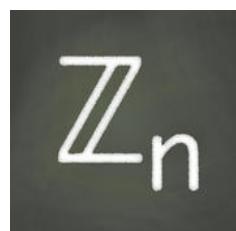
**Ascii**    73, 110, 102, 111, 114, 109, 97, 99, 105, 243, 33

**Binari**    01001001 01101110 01100110 01101111 01110010 ...



# MATEMÀTIQUES DE LA CRIPTOGRAFIA

- Operem amb cadenes de bits (**codificació**)
- Operem amb **nombres enters** (en base 2)
- Hem de fer **ARITMÈTICA**
- Els nombres dels ordenadors són finits
- Hem de fer **ARITMÈTICA MODULAR**



# EXEMPLE 1

$$R = \mathbb{Z}/26\mathbb{Z}$$

Xifrat de Cèsar:  $\mathcal{M} = \mathcal{C} = \mathcal{K} = R$

$$E(x, k) = x + k$$

$$D(y, k) = y - k$$

+ i - són les operacions de  $R$ , és a dir,

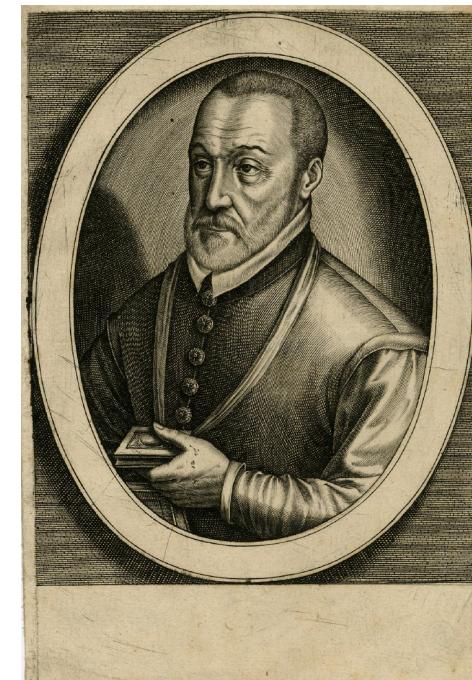
són la suma i la diferència **mòdul 26**

# EXAMPLE 2

**Vigenère (1586)** Es fixa una paraula clau, es repeteix fins igualar la longitud del missatge i després es suma amb el missatge

miss: ATACAR AVUI A LES TRES  
clau: SOLSOL SOLS O LSO LSOL

crip: SHLUOC SJFA O WWG EJSD



# EXEMPLES DE CRIPTOSISTMES

	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

cipher      V V V R B A C P

key            C O V E R C O V E R ...

plaintext    T H A N K Y O U

In encrypting plaintext, the cipher letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter. To decrypt ciphertext, the plaintext letter is found at the head of the column determined by the diagonal containing the cipher letter and the row containing the key letter.

© 2002 Encyclopædia Britannica, Inc.

Trencat pel Major de la infanteria prussiana **F. W. Kasiski**  
(1805-1881)

## EXAMPLE 2

$$\begin{array}{r} (12 \quad 8 \quad 18 \quad 18 \quad 0) \quad (19 \quad 6 \quad 18 \quad 4 \quad 2) \quad (17 \quad 4 \quad 19 \\ (2 \quad 11 \quad 0 \quad 21 \quad 4) \quad (2 \quad 11 \quad 0 \quad 21 \quad 4) \quad (2 \quad 11 \quad 0 \\ \hline 14 \quad 19 \quad 18 \quad 13 \quad 4 \quad 21 \quad 17 \quad 18 \quad 25 \quad 6 \quad 19 \quad 15 \quad 19 \end{array}$$

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n$$

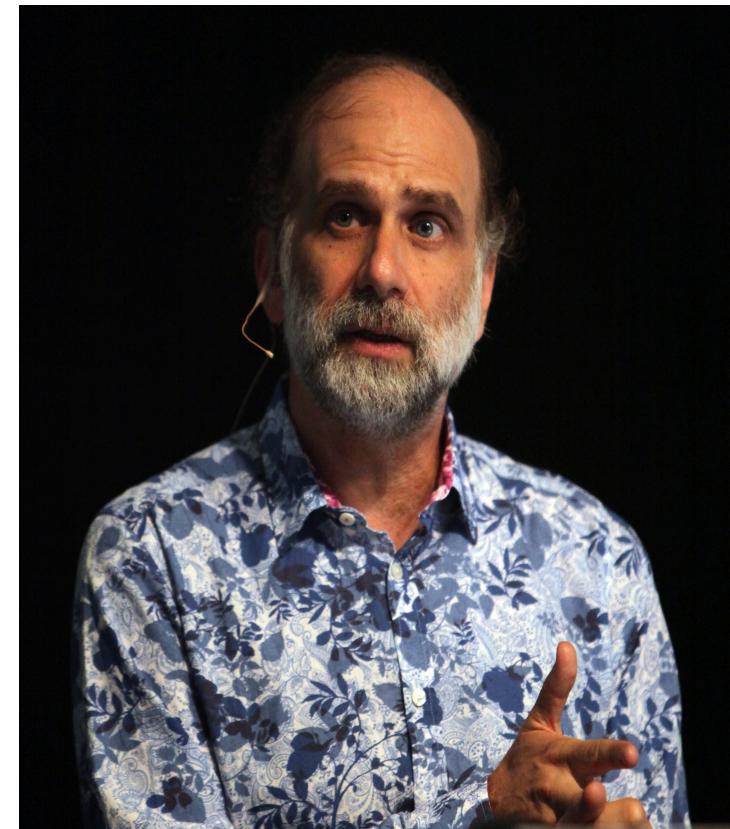
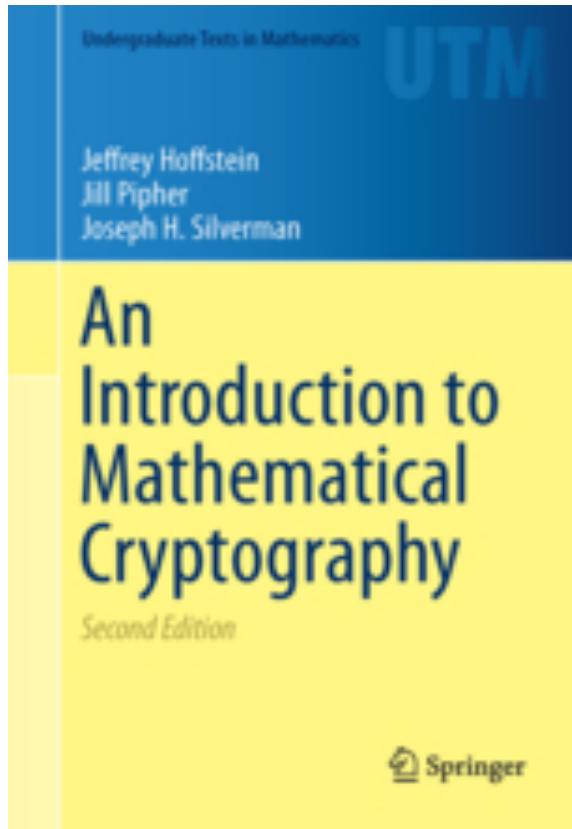
$$E(m, k) = m + k$$

$$D(c, k) = c - k$$

# ARITMÈTICA

- $x^k \text{ mòdul } n$  Operació RSA
- $65537 = 2^{16} + 1$  és primer
- $x^{p-1} = 1 \pmod p$  Test de primalitat
- Generar primers és fàcil
- Factoritzar nombres enters és difícil
- El grup multiplicatiu d'un cos finit és cíclic
- ....

# UN LLIBRE I UN GURÚ



Bruce Schneier  
[schneier.com](http://schneier.com)