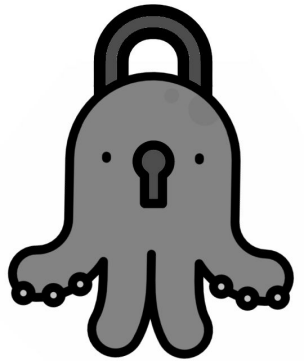
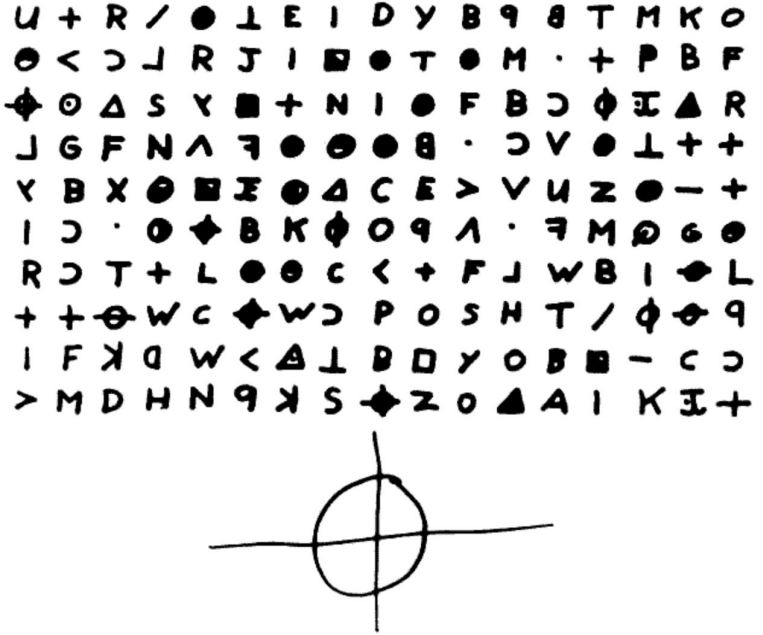
Histoire de la Cryptographie

IFT 3275



Cryptographie: L’art de créer et briser des codes secrets.

Cryptographie Moderne: L’étude des techniques mathématiques pour sécuriser les informations numériques, les systèmes et les calculs distribués contre les attaques adverses (Katz et Lindell 2007).

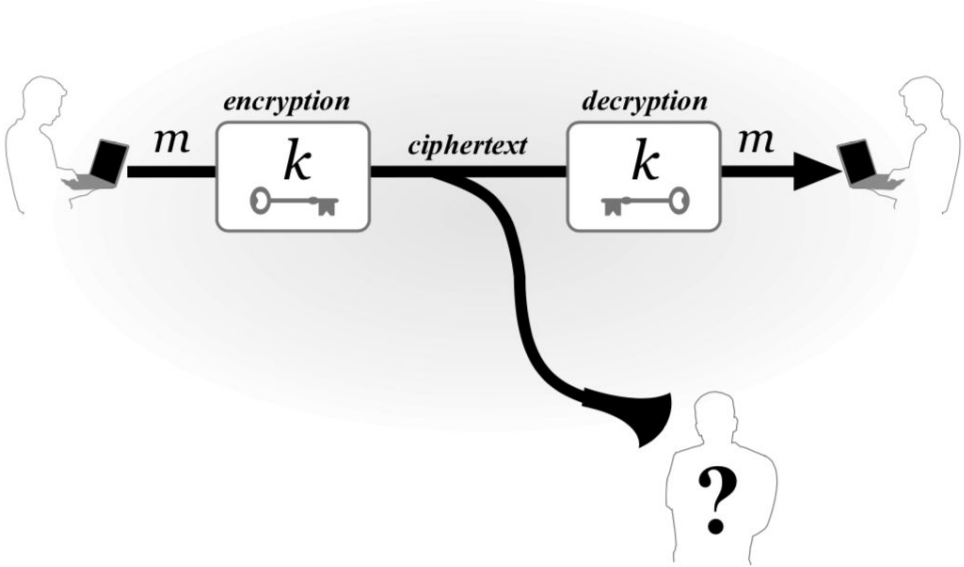


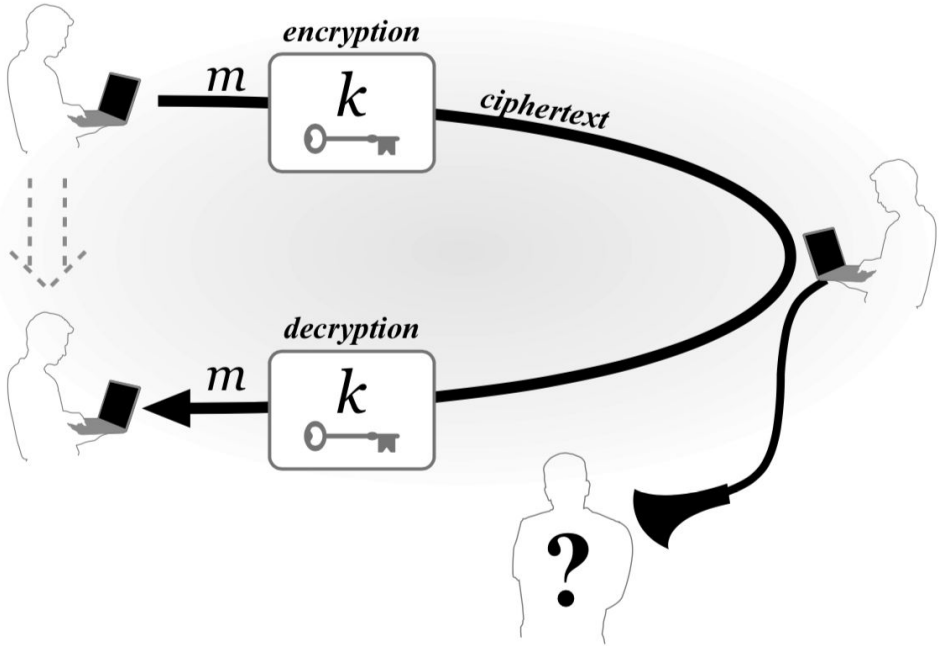
$$ENC_k(m) = c$$

$$DEC_k(c) = m$$

$$DEC_k(ENC_k(m)) = m$$

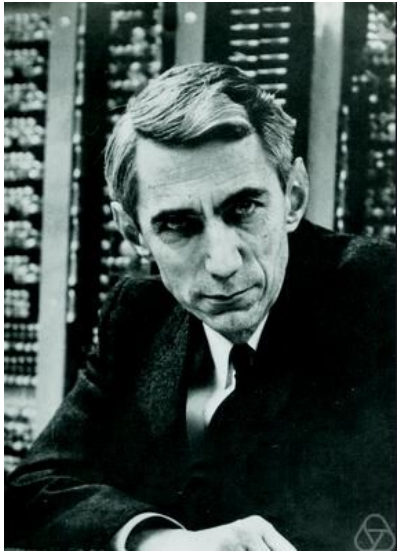
Cryptographie à clef privée

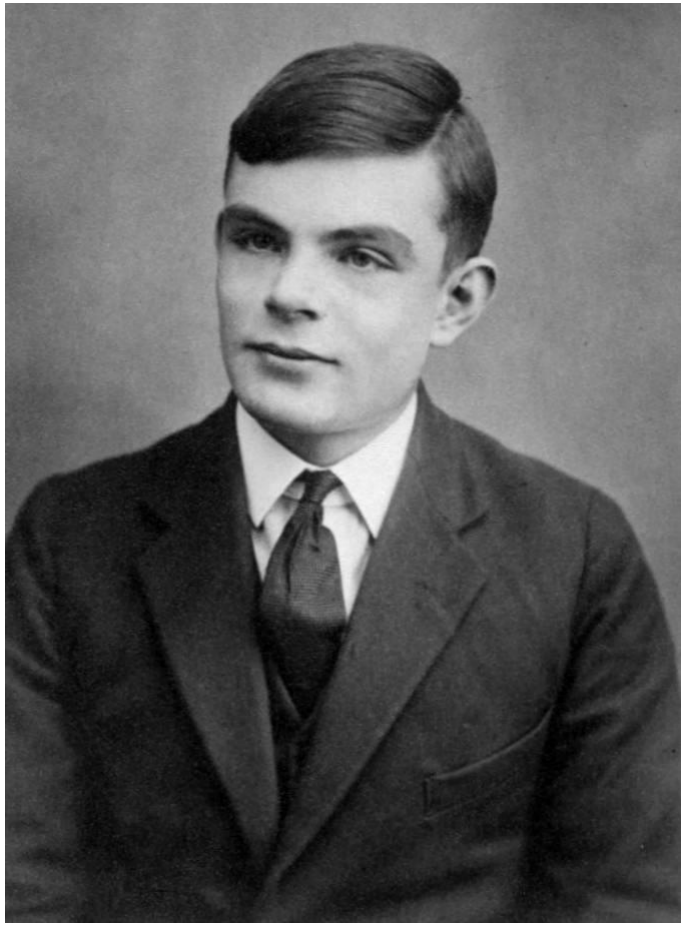


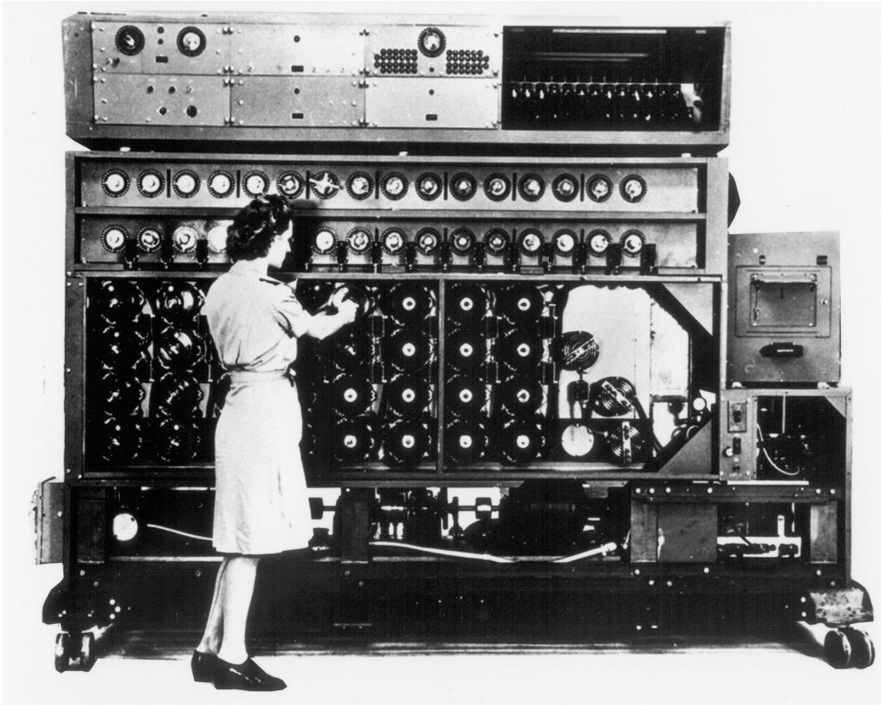

encryption
m
k
ciphertext
decryption
m
k
?

Principe de Kerckhoffs: La sécurité offerte par un cryptosystème doit reposer seulement sur le secret de la clef. “Il faut qu’il n’exige pas le secret, et qu’il puisse sans inconvénient tomber entre les mains de l’ennemi.”

Claude Shannon: “L'adversaire connaît le système.”







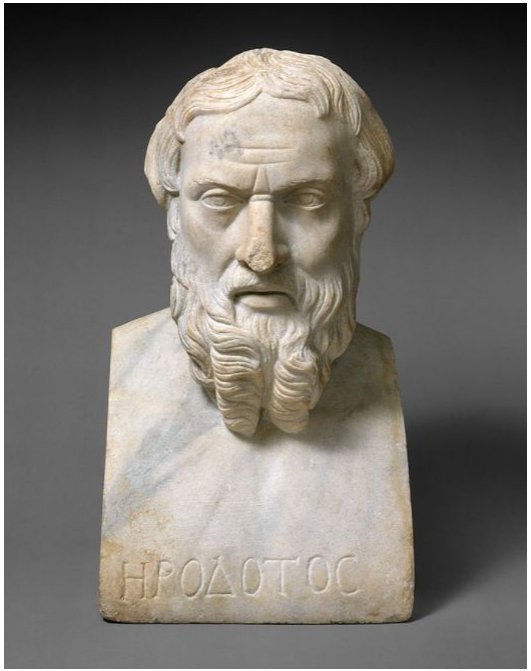
Pourquoi?

Il est plus facile de garder une clef secrète qu'un cryptosystème.

Il est facile d'inventer une nouvelle clef, mais pas un cryptosystème.

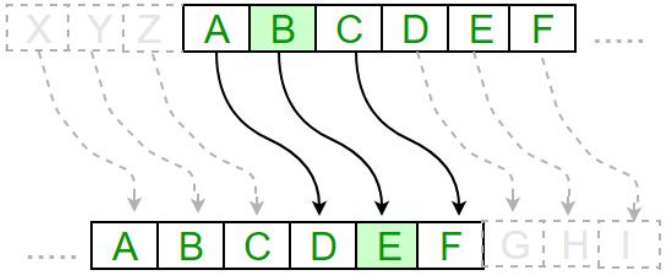
Un cryptosystème secret ne peut pas être standardisé.

Stéganographie: l'art de la dissimulation et non l’art du secret.



Hérodote

Chiffrement par décalage:



$$\mathsf{Enc}_k(m_1 \cdots m_\ell) = c_1 \cdots c_\ell, \quad \text{where } c_i = [(m_i + k) \bmod 26].$$

$$\mathsf{Dec}_k(c_1 \cdots c_\ell) = m_1 \cdots m_\ell, \quad \text{where } m_i = [(c_i - k) \bmod 26].$$

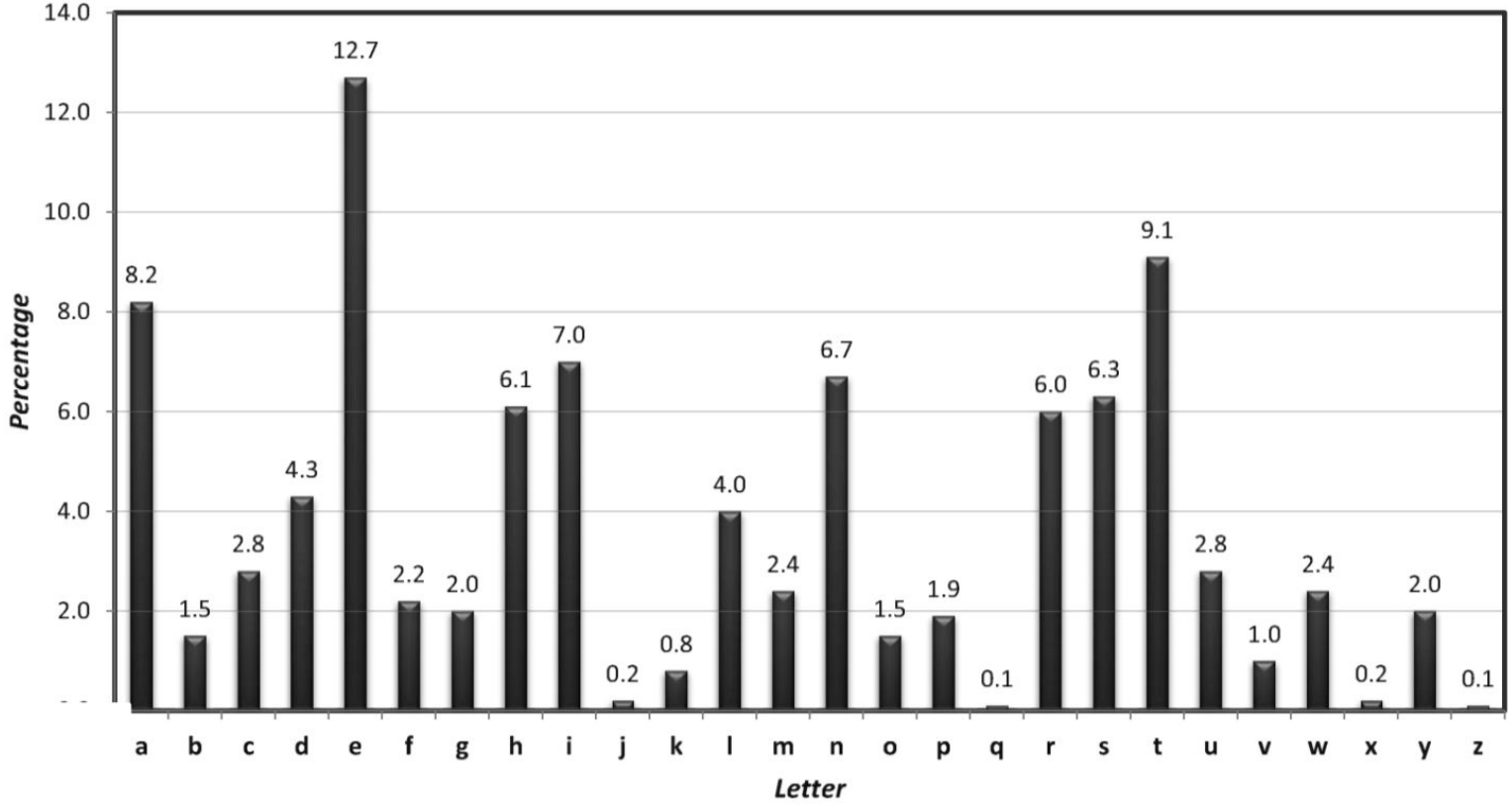
Si k = 3, nous avons le chiffre de césar. ROT-13 est utilisé de nos jours.

Chiffre mono-alphabétique:

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

m = The magic Words are Squeamish Ossifrage
c = gkd cxbvu ifhaw xhd wyldxcvwk fwwvnhxbd

Briser le chiffre mono-alphabétique:



Chiffre de Vigenère (poly-alphabétique):

Clef = ABC

```
The magic Words are Squeamish Ossifrage
ABC ABCAB CABCA ACB ABCACBACB ACBACBACB
tig mbiid yosfs bte tsufcmjuh pusjhrbie
```

Chiffrement parfait?

Si nous utilisons une clef de k lettres, le chiffre est composé de k sous-ensembles qui sont des chiffres par décalage!

Briser le chiffre de Vigenère: Comment automatiser une attaque?

$$\sum_{i=0}^{25} p_i^2 \approx 0.065.$$

$$\sum_{i=0}^{n-1} f_i^2 = \sum_{i=0}^{n-1} \left(\frac{1}{n}\right)^2 = n\left(\frac{1}{n}\right)^2 = \frac{1}{n} = f_i$$

$$I_j \stackrel{\text{def}}{=} \sum_{i=0}^{25} p_i \cdot q_{i+j}$$

$$k = k_1 \cdots k_t \qquad c_j, c_{j+t}, c_{j+2t}, \cdots \qquad j \in \{1, \ldots, t\}$$

$$c_1, c_{1+t}, c_{1+2t}, \cdots$$

$$\sum_{i=0}^{25} q_i^2 \approx \sum_{i=0}^{25} p_i^2 \approx 0.065.$$

$$\sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 \approx 0.038.$$

Types d’attaques:

- **Attaque sur texte chiffré seul (*ciphertext-only* en anglais) : le cryptanalyste possède des exemplaires chiffrés des messages, il peut faire des hypothèses sur les messages originaux qu'il ne possède pas. La cryptanalyse est plus ardue de par le manque d'informations à disposition.**

- **Attaque à texte clair connu (*known-plaintext attack* en anglais) : le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.**

- **Attaque à texte clair choisi (*chosen-plaintext attack* en anglais) : le cryptanalyste possède des messages en clair, il peut créer les versions chiffrées de ces messages avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.**

- **Attaque à texte chiffré choisi (*chosen-ciphertext attack* en anglais) : le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque.**

Masque Jetable:

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = k \oplus k \oplus m = m$$

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

Notre ami le OU-Exclusif:

Input		output
A	B	$C = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

$$a \oplus a = 0$$

$$a \oplus 0 = a$$

$$[1, 2, 3, 4, 3, 1, 2] \implies 4$$

$$|\mathcal{K}| \geq |\mathcal{M}|$$

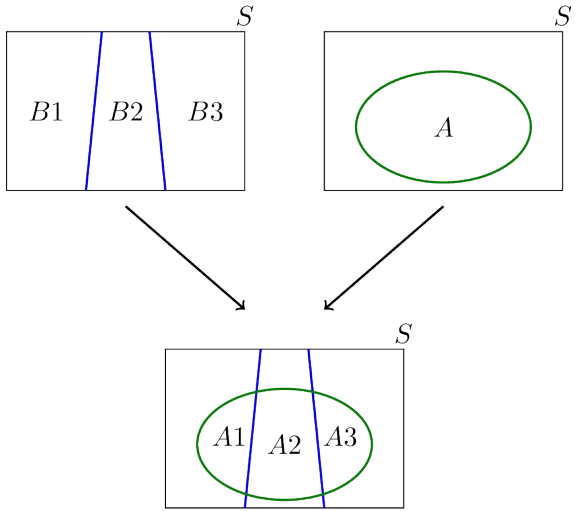
$$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'$$

Sécurité Inconditionnelle (perfect secrecy): un attaquant ne récupère aucune information sur le texte clair à partir du texte chiffré.

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Masque Jetable:

$$\begin{aligned}\Pr[C = c \mid M = m'] = \Pr[\mathsf{Enc}_K(m') = c] &= \Pr[m' \oplus K = c] \\ &= \Pr[K = m' \oplus c] \\ &= 2^{-\ell},\end{aligned}$$



$$\begin{aligned}\Pr[C = c] &= \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \\ &= 2^{-\ell} \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m'] \\ &= 2^{-\ell},\end{aligned}$$

$$P(A|B) = \frac{P(B|A)\ P(A)}{P(B)}$$

$$\begin{aligned}
\Pr[M = m \mid C = c] &= \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} \\
&= \frac{2^{-\ell} \cdot \Pr[M = m]}{2^{-\ell}} \\
&= \Pr[M = m].
\end{aligned}$$