



# Session 1

## Histoire de la Cryptographie

Introduction à la Cryptographie

Nadim Kobeissi



# Objectifs du cours

---

- Apprendre comment marchent les primitifs cryptographiques.
- Apprendre un instinct de raisonnement a propos de la sécurité.
- Trouver le secret de la vie heureuse.

# La Cryptographie Est Partout

---

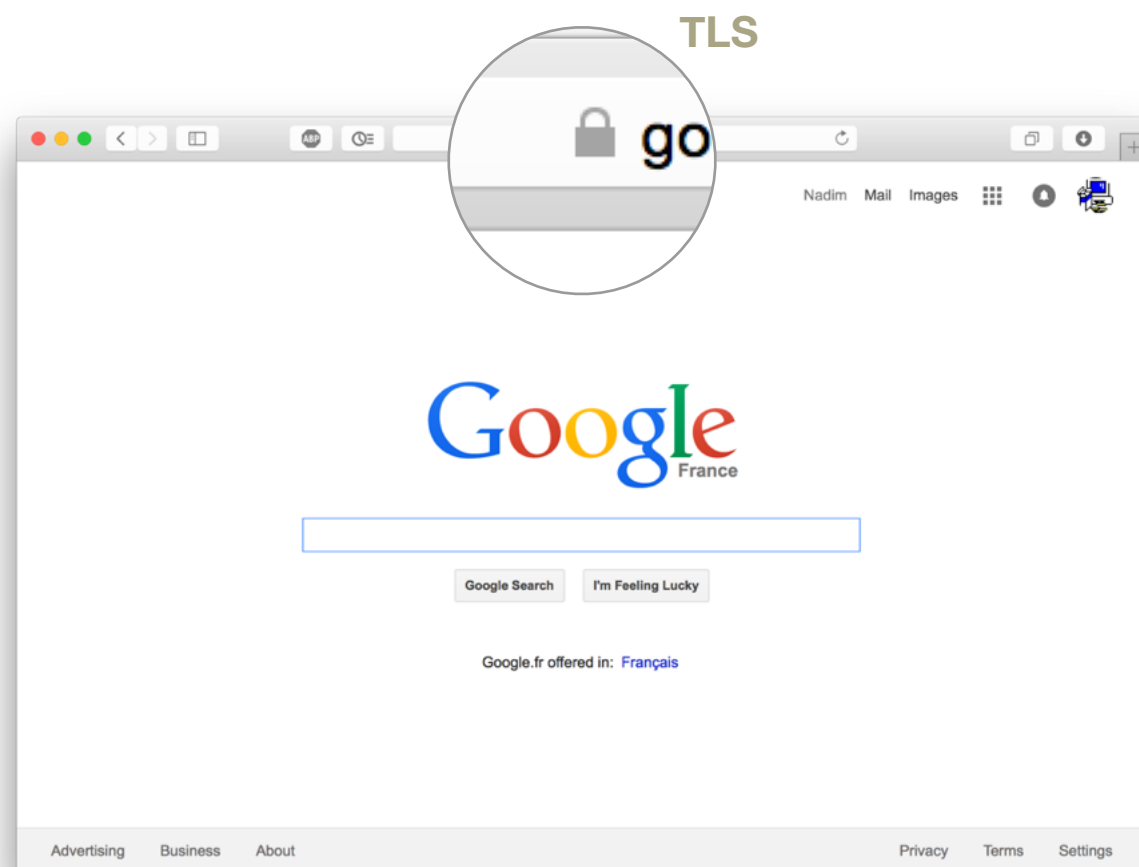
- **Communication Sécurisée:**
  - **Web:** HTTPS, TLS.
  - **Sans-fil:** WPA2, WEP, GSM, Bluetooth.
- **Chiffrement des Fichiers:** EFS, TrueCrypt.
- **Protection des Droits Intellectuels:** CCS, AACCS.
- **Authentication des Utilisateurs**, *et bien encore plus!*

# Des Utilisations Innovantes et Exotiques

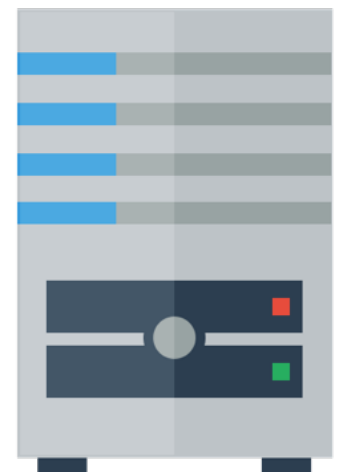
---

- **Connexions anonymes:** Tor.
- **Monnaie numérique:** Bitcoin.
- **Messagerie et Chat:** Cryptocat, Signal.
- **Partage de Fichiers:** BitTorrent.

# Communication Sécurisée



Pas d'espionnage,  
Pas d'alteration.



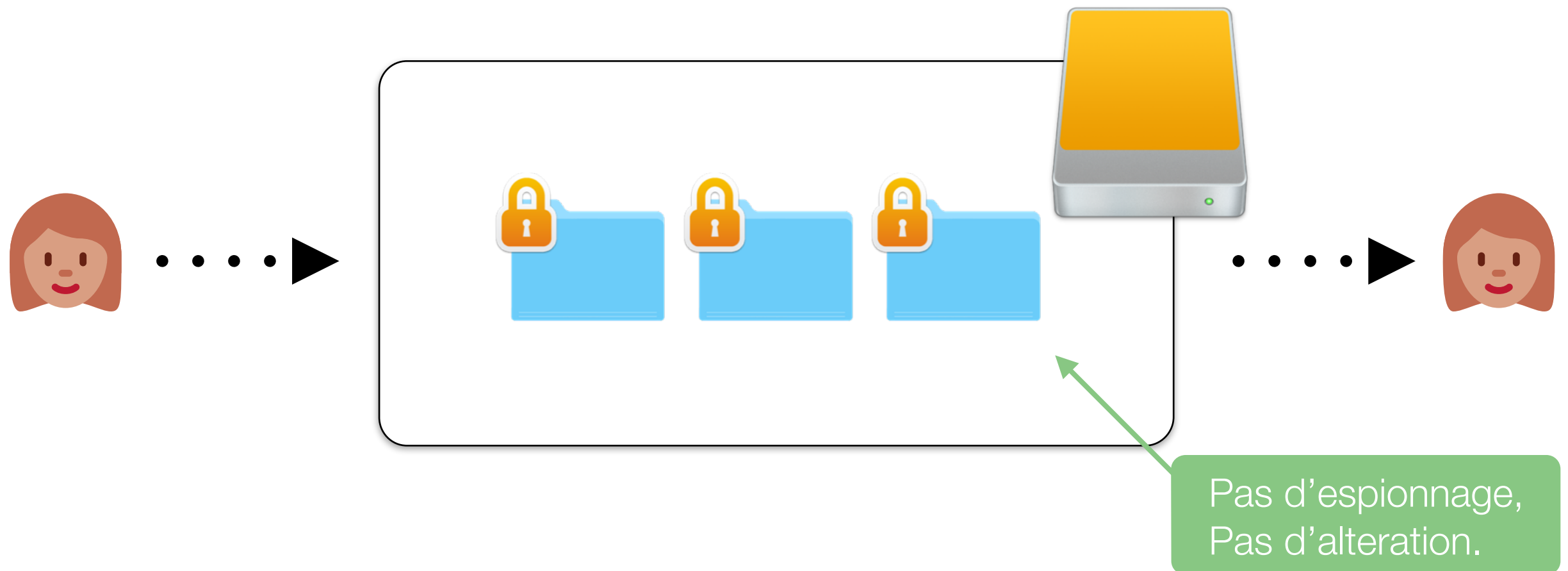
# Comment marche TLS?

---

- **Deux étapes principaux:**
- **1. Negotiation d'un Secret:** Etablir une clé commune entre ton navigateur et le serveur, en utilisant la cryptographie asymétrique. (*deuxième partie du cours*)
- **2. Transmission Chiffrée:** Chiffrer et transmettre toutes les données d'une façon sûre et authentifiée en utilisant la clé établie. (*première partie du cours*)

# Chiffrement des Fichiers

---



Analogue à la communication sécurisée:  
Alice du passé envoie un message à Alice du futur!

# Choses à retenir

---

- **La Cryptographie est:**
  - Un outil formidable.
  - La base de la sécurité numérique.
- **La cryptographie n'est pas:**
  - La solution à tout les problèmes.
  - Fiable, sauf si utilisée correctement.

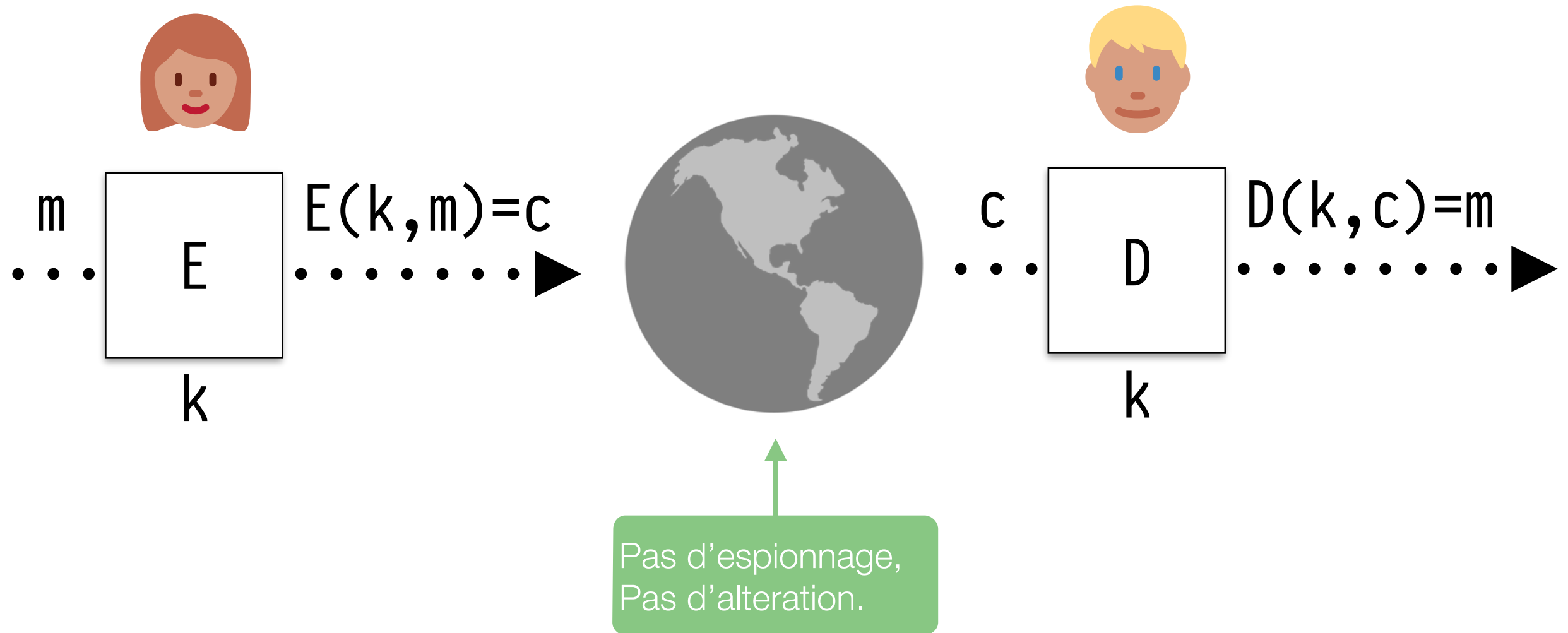


# Une Science Rigoureuse

---

- **Les trois étapes de la cryptographie:**
  - Specifier précisément le *modèle de menace*.
  - Proposer une construction.
  - Prouver que si on casse cette construction, ca casse aussi un *problème mathématique difficile sous-jacent*.

# Bloc de Construction: Chiffrement Symétrique



m: Message, k: Clé  
E, D: Fonctions de chiffrement (connus)  
c: Message chiffré

*Symétrique* parce-que la même operation avec la même clé est utilisée par les deux participants.

# Exemples Historiques: Chiffrement par Substitution

Texte Clair (“cleartext”)

JE SUIS UN CHAT

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮  
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

EJ TDWT DF QLMB

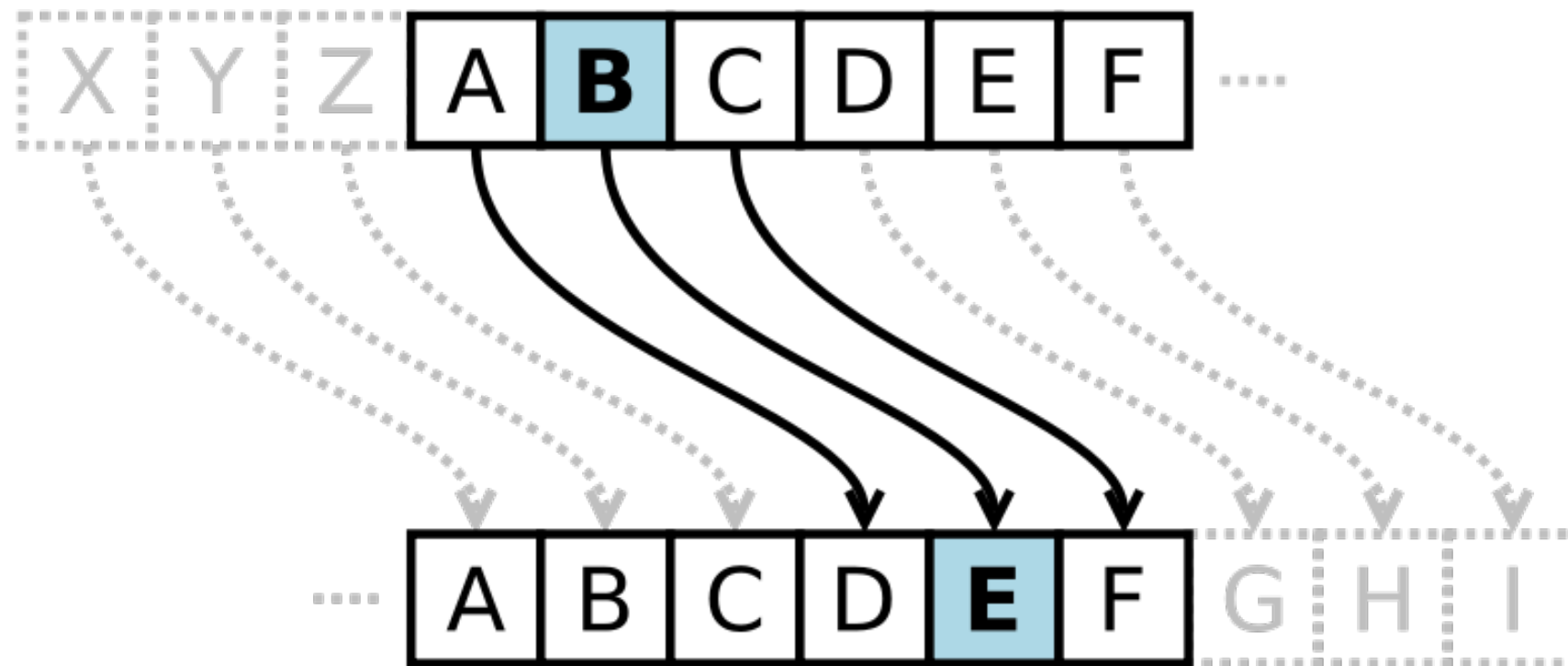
Cryptogramme (“ciphertext”)

{	A:	'M',	N:	'F',
	B:	'U',	O:	'N',
	C:	'Q',	P:	'P',
	D:	'C',	Q:	'O',
	E:	'J',	R:	'V',
	F:	'G',	S:	'T',
	G:	'S',	T:	'B',
	H:	'L',	U:	'D',
	I:	'W',	V:	'K',
	J:	'E',	W:	'Z',
	K:	'R',	X:	'I',
	L:	'H',	Y:	'A',
	M:	'Y',	Z:	'X' }

Clé

# Exemples Historiques: Chiffrement de César

- Décalage par trois:

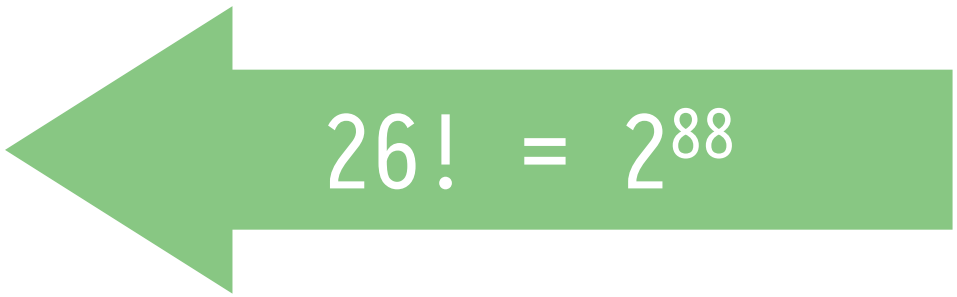


Question: Quelle est la clé?



# Question 1: Espace des clés

---

- Quelle est la taille de l'espace de clés dans un chiffrement par substitution, sur un alphabet de 26 lettres?
  - A)  $|K| = 26$
  - B)  $|K| = 26!$
  - C)  $|K| = 2^{26}$
- 

## Question 2: Casser un chiffrement de substitution

- Quelle est la lettre qui apparait la plus fréquemment dans la langue Française?

- A) E

14.7%

- B) S

- C) A

- D) I







## Question 2: Casser un chiffrement de substitution

- Un exemple


UKBYBIPOUZBCUFEEBORUKBYBHOBBERFESPVKBWFOFERNVNBCVBZPRUBOFERNVNBCVBPCYYFVUFO  
FEIKNWFRFIKJNUPWRFIPOUNVNI PUBRNCUKBEFWWFDNCHXC YBOHOPYXPUBNCUBOYNRVNIWN  
CPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVFZIXUP  
UNFCPWRVNBCVBRPYYNUNFCPWJUKBYBIPOUZBCUIPOUNVNI PUBRNCHOPYXPUBNCUB  
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	36	
N	34	
U	33	
P	32	
C	26	

Lettres

NC	11	
PU	10	
UB	10	
UN	9	

Digrammes

UKB	36	
RVN	34	
FZI	33	

Trigrammes

# Exemples Historiques: Chiffre de Vigenère

---

10 05 22 05 21 24 21 14 18 01 14 04 23 09 03 08  
**JEVEUXUNSANDWICH**

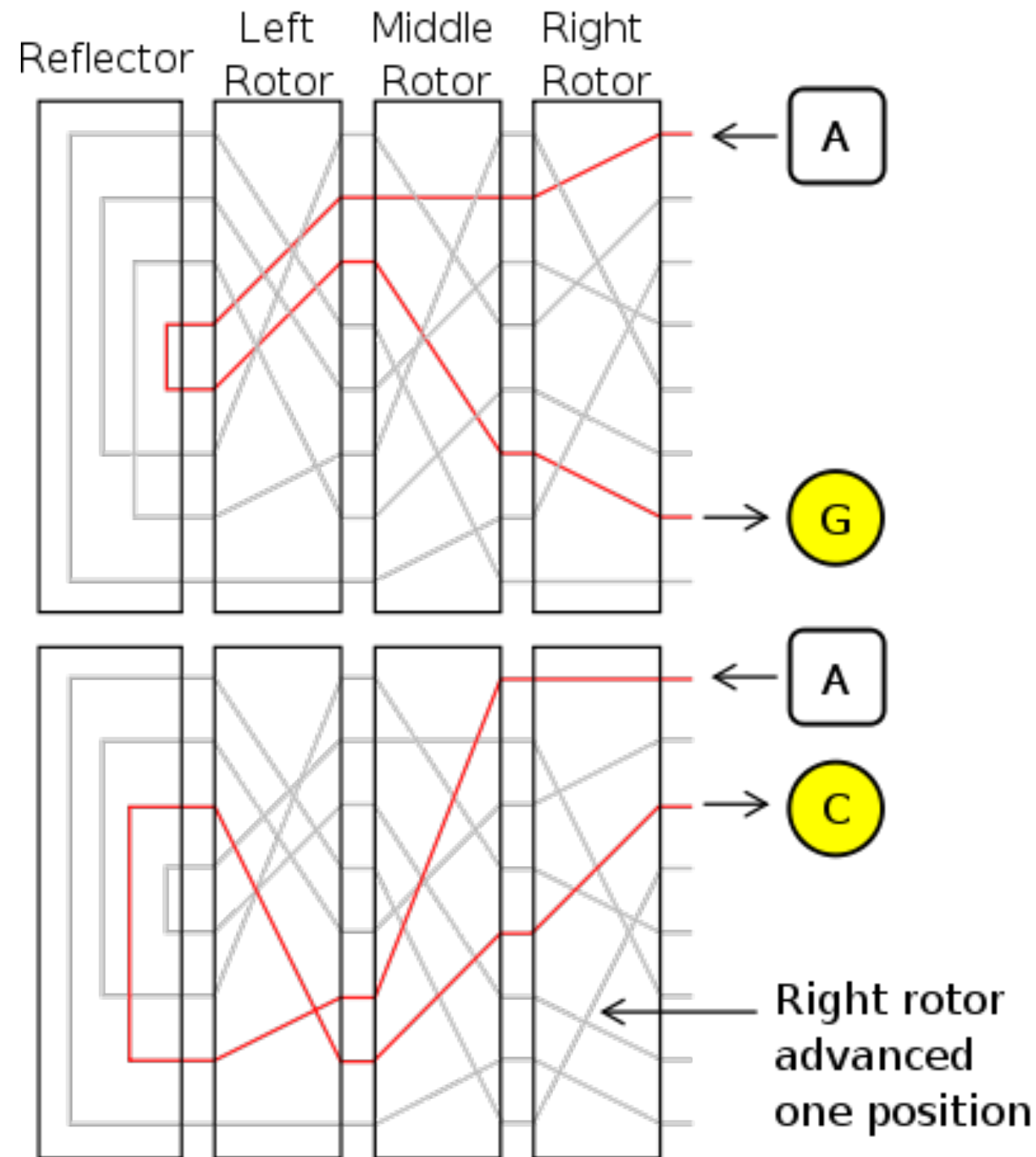
03 18 25 11 20 15 03 18 25 11 20 15 03 18 25 11  
**CRYPTO**CRYPTOCRYPT

10 05 22 05 21 24 21 14 18 01 14 04 23 09 03 08  
+ + + + + + + + + + + + + + +  
03 18 25 11 20 15 03 18 25 11 20 15 03 18 25 11  
= = = = = = = = = = = = = = = =  
13 22 21 16 15 13 24 06 17 12 08 19 26 01 02 19  
**MVUPOMWFQLHSZABS**

# Exemples

## Historiques: Enigma

- La fameuse machine cause une révolution dans la cryptographie.
- Seule une autre machine pourrait la casser. (la Bombe de Alan Turing)
- Un système de substitution, mais avec rotations et configurations compliqués. ( $2^{84}$ )



# Exemples Historiques: DES

---

- Data Encryption Standard (DES), 1974.
- AES, 2001.

# Probabilité Discrète: Petit Intro

---

- $U$ : Ensemble fini (exemple:  $U = \{0,1\}^n$ )
  - $\{0,1\}^2 = \{00, 01, 10, 11\}$
- Une **distribution probabiliste**  $P$  sur  $U$  est une fonction  $P: U \rightarrow [0,1]$  tel que:  $\sum_{x \in U} P(x) = 1$
- $P(\{0,1\}^2) = \{00, 01, 10, 11\}$  (Distribution uniforme)  
 $\quad \quad \quad 0.25 \quad 0.25 \quad 0.25 \quad 0.25$

# Probabilité Discrète: Événements

---

- Pour un ensemble  $A \subseteq U$ :  $\Pr[A] = \sum_{x \in U} P(x) \in [0, 1]$
- $\Pr[U] = 1$
- On appelle  $A$  un **événement**.

Exemple:  $U = \{0, 1\}^8$

$A = \{\text{les } x \text{ qui finissent avec } 11 \text{ (lsb}_2(x)=11)\} \subseteq U$

Quelle est la probabilité de l'événement  $\Pr[A]$ ?



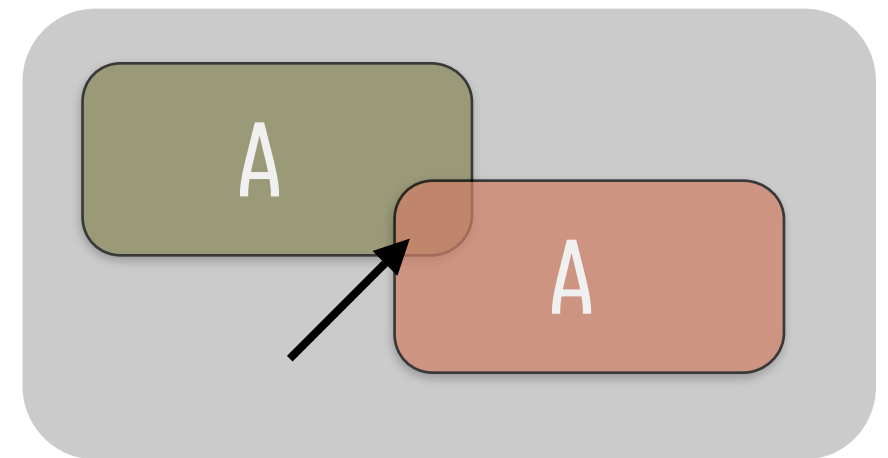
1/4



# Probabilité Discrète: Unions et Indépendance

---

- $\Pr[A_1 \cup A_2] \leq \Pr[A_1] + \Pr[A_2]$
- $\Pr[A_1 \wedge A_2] = \Pr[A_1] \cdot \Pr[A_2]$



# Probabilité Discrète: Variables Aléatoires

---

- $X: U \longrightarrow V$
- Exemple:  $X: \{0, 1\}^n \longrightarrow \{0, 1\}$
- Pour la distribution uniforme sur  $U$ :
- $\Pr[X=0] = 1/2, \Pr[X=1] = 1/2$

# Probabilité Discrète: XOR

---

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |



# Probabilité Discrète: XOR

---

- $Y$  est une distribution inconnue sur  $\{0, 1\}^n$ .
- $X$  est une distribution **uniforme** sur  $\{0, 1\}^n$ .
- $Z := Y \oplus X$  sera **uniforme** aussi! (Prouvé)

# Suivez le Cours En Ligne

---

- Homepage: <https://github.com/kaepora/courscrypto/>
  - Matériaux.
  - Devoirs/TPs.
  - Slides.
  - Discussions.
  - A la semaine prochaine!