



# Introduction à la Cryptologie

**Johanna Loyer**

Université de Limoges - Master 2 Cryptologie

Inria Paris - équipe-projet COSMIQ



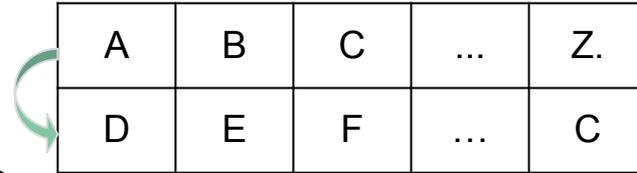
# Team bleue VS team rouge

## Equipe bleue = Cryptographie

Exemple : code de César

Message : MESSAGE A CODER

Chiffré : PHVVDJH D FRGHU



A	B	C	...	Z.
D	E	F	...	C

## Equipe rouge = Cryptanalyse

Lettre la plus fréquente = H



# Les problèmes cryptographiques

**Problème difficile** : un problème mathématique pour lequel le meilleur algorithme connu pour le résoudre ne se finit pas en temps raisonnable. Autrement dit sa complexité est exponentielle.

Exemple : problème de factorisation de  $N = p \times q$  avec  $p$  et  $q$  des nombres premiers.

$$14 = 2 \times 7$$

$$9853140135849754687163794731675473189431086471354 \\ 67137408316974693174817937481343187048371949 = ? \times ?$$

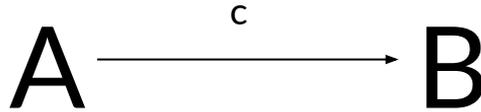
# Application - chiffrement RSA

Bob {

- Clé secrète :
  - $p$  un nombre premier
  - $q$  un nombre premier
  - $d$  tel que  $e.d = 1 \pmod{\varphi}$
- Clé publique :
  - $N = p \times q$
  - $e = 65\,537$

Message :  $m$

Calcule :  $c = m^e \pmod N$



Calcule :  $m = c^d \pmod N$

Vérification :

$$\begin{aligned} c^d \pmod N &= (m^e)^d \pmod N \\ &= m^{(ed)} \pmod N \\ &= m^1 \pmod N \\ &= m \pmod N \end{aligned}$$

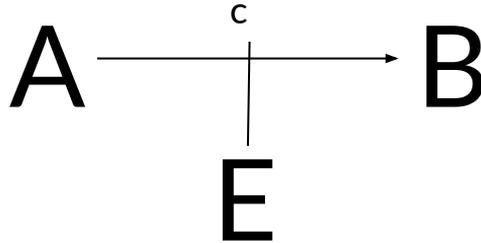
# Application - chiffrement RSA

Bob { Clé secrète :  
- p un nombre premier  
- q un nombre premier  
- d tel que  $e.d = 1 \pmod{\varphi}$

Clé publique :  
-  $N = p \times q$   
-  $e = 65\,537$

Message : m

Calcule :  $c = m^e \pmod{N}$



Calcule :  $m = c^d \pmod{N}$

Vérification :

$$\begin{aligned} c^d \pmod{N} &= (m^e)^d \pmod{N} \\ &= m^{(ed)} \pmod{N} \\ &= m^1 \pmod{N} \\ &= m \pmod{N} \end{aligned}$$

Peut connaître  $N, e, c$ .  
**Aucune information sur  
le contenu du message**

# Ordinateurs quantiques et cryptologie

**Algorithme classique** : données codées en bits, 0 ou 1.

**Algorithme quantique** : données qui peuvent valoir en même temps 0 ET 1 (avec une probabilité de mesurer l'un ou l'autre).

Illustration : chat de Schrödinger





# Ordinateurs quantiques et cryptologie

## **Applications possibles des ordinateurs quantiques :**

- Attaquer les systèmes de chiffrement de ses ennemis...
- Médecine
- Logistique
- Traduction automatisée
- Reconnaissance vocale et d'images
- Finance et analyse des risques
- Big Data
- Intelligence artificielle
- ...



Merci de m'avoir écoutée !