Principes de fonctionnement des machines binaires

2019/2020

Pierluigi Crescenzi
Université de Paris, IRIF

Université de Paris

INSTITUT DE RECHERCHE EN INFORMATIQUE FONDAMENTALE

cnrs dépasser les frontières

- Tests et examens
  - CC : résultat des tests en TD / TP (semaine 4 et semaine 10)
  - E0 : partiel (**samedi 26 octobre 9h30-11h30**)
  - E1 : examen mi décembre
  - E2 : examen fin juin
- Notes finales
  - Note session 1 : 25% CC + 25% E0 + 50% E1
  - Note session 2 : max(E2, 33% CC + 67% E2)
- Rappel
  - Pas de note $\Rightarrow$ pas de moyenne $\Rightarrow$ pas de semestre
- Site web
  - `moodlesupd.script.univ-paris-diderot.fr`

- Numération et arithmétique
- Numération et arithmétique en machine
- Numérisation et codage (texte, images)
- Compression, **cryptographie**, contrôle d'erreur
- Logique et calcul propositionnel
- Circuits numériques

Cryptographie

- Écriture cachée selon les Grecs
  - Des cas extrêmement simples
    - Le chiffre de César, ROT13, Vigénère, le masque jetable de Vernam
  - Des cas plus compliqués
    - LFSR, DES, RSA
- Idée
  - Utiliser une fonction difficilement inversible pour coder un texte
    - Le secret est justement la fonction inverse

- Attribué à l'empereur César (100--44 av. J.-C.)
  - Il l'aurait utilisé pour masquer certaines correspondances (ce n'est pas le premier mécanisme de cryptographie)
  - C'est un chiffrement monoalphabétique par substitution
- Il repose sur une permutation circulaire de l'alphabet
  - Les lettres sont décalées de p (pour un p choisi) rangs dans l'ordre alphabétique

- Attribué à l'empereur César (100--44 av. J.-C.)
  - Il l'aurait utilisé pour masquer certaines correspondances (ce n'est pas le premier mécanisme de cryptographie)
  - C'est un chiffrement monoalphabétique par substitution
- Il repose sur une permutation circulaire de l'alphabet
  - Les lettres sont décalées de p (pour un p choisi) rangs dans l'ordre alphabétique
  - Exemple : $p = 3$

A	B	C	D	E	F	…	X	Y	Z
D	E	F	G	H	I		A	B	C

- Attribué à l'empereur César (100--44 av. J.-C.)
  - Il l'aurait utilisé pour masquer certaines correspondances (ce n'est pas le premier mécanisme de cryptographie)
  - C'est un chiffrement monoalphabétique par substitution
- Il repose sur une permutation circulaire de l'alphabet
  - Les lettres sont décalées de p (pour un p choisi) rangs dans l'ordre alphabétique
  - Exemple : $p = 3$

A	B	C	D	E	F	…	X	Y	Z
D	E	F	G	H	I		A	B	C

    - `ATTAQUE` $\Rightarrow \ldots$

- Attribué à l'empereur César (100--44 av. J.-C.)
  - Il l'aurait utilisé pour masquer certaines correspondances (ce n'est pas le premier mécanisme de cryptographie)
  - C'est un chiffrement monoalphabétique par substitution
- Il repose sur une permutation circulaire de l'alphabet
  - Les lettres sont décalées de p (pour un p choisi) rangs dans l'ordre alphabétique
  - Exemple : $p = 3$

A	B	C	D	E	F	…	X	Y	Z
D	E	F	G	H	I		A	B	C

    - `ATTAQUE` $\Rightarrow$ `...`
    - `...DWWDTXH`

- Attribué à l'empereur César (100--44 av. J.-C.)
  - Il l'aurait utilisé pour masquer certaines correspondances (ce n'est pas le premier mécanisme de cryptographie)
  - C'est un chiffrement monoalphabétique par substitution
- Il repose sur une permutation circulaire de l'alphabet
  - Les lettres sont décalées de p (pour un p choisi) rangs dans l'ordre alphabétique
  - Exemple : $p = 3$

A	B	C	D	E	F	...	X	Y	Z
D	E	F	G	H	I		A	B	C

    - `ATTAQUE` $\Rightarrow$ `...`
    - `...DWWDTXH`
  - On peut utiliser l'arithmétique modulaire pour le définir

- Attribué à l'empereur César (100--44 av. J.-C.)
  - Il l'aurait utilisé pour masquer certaines correspondances (ce n'est pas le premier mécanisme de cryptographie)
  - C'est un chiffrement monoalphabétique par substitution
- Il repose sur une permutation circulaire de l'alphabet
  - Les lettres sont décalées de p (pour un p choisi) rangs dans l'ordre alphabétique
  - Exemple : $p = 3$

A	B	C	D	E	F	...	X	Y	Z
D	E	F	G	H	I		A	B	C

    - `ATTAQUE` $\Rightarrow$ `...`
    - `...DWWDTXH`
  - On peut utiliser l'arithmétique modulaire pour le définir
  - Son inverse est aussi un chiffre de César : lequel ?

- Attribué à l'empereur César (100--44 av. J.-C.)
  - Il l'aurait utilisé pour masquer certaines correspondances (ce n'est pas le premier mécanisme de cryptographie)
  - C'est un chiffrement monoalphabétique par substitution
- Il repose sur une permutation circulaire de l'alphabet
  - Les lettres sont décalées de p (pour un p choisi) rangs dans l'ordre alphabétique
  - Exemple : $p = 3$

A	B	C	D	E	F	...	X	Y	Z
D	E	F	G	H	I		A	B	C

    - `ATTAQUE` $\Rightarrow$ `...`
    - `...DWWDTXH`
  - On peut utiliser l'arithmétique modulaire pour le définir
  - Son inverse est aussi un chiffre de César : lequel ?
  - Le codage ROT13 est le chiffre de César pour $p = 13$

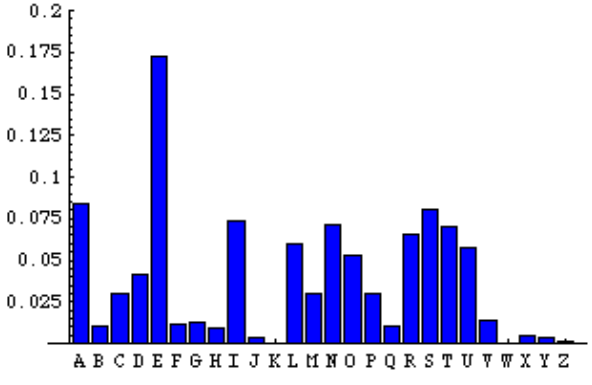
- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur

- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur
  - Analyse de fréquences pour casser le code

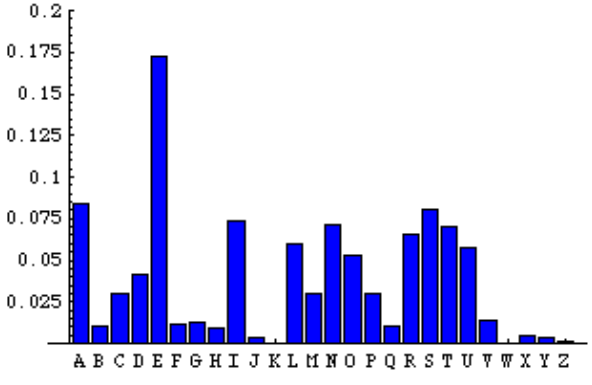
- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur
  - Analyse de fréquences pour casser le code
    - `PUALYNVBCLYULTLUAHSPZHAPVU`

- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur
  - Analyse de fréquences pour casser le code
    - `PUALYNVBCLYULTLUAHSPZHAPVU`
      - Les lettres les plus fréquentes : `L` et `U`

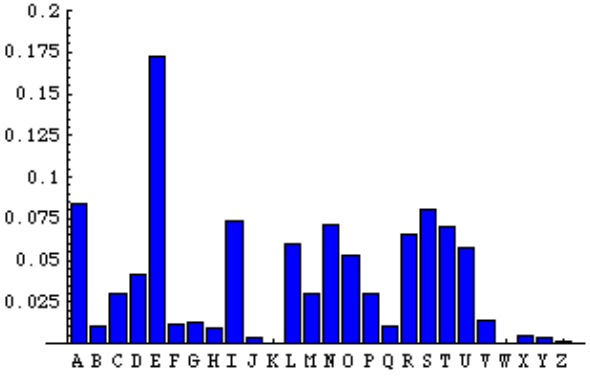
- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur
  - Analyse de fréquences pour casser le code
    - `PUALYNVBCLYULTLUAHSPZHAPVU`
      - Les lettres les plus fréquentes : `L` et `U`
      - `E` $\Rightarrow$ `L` ou `E` $\Rightarrow$ `U`



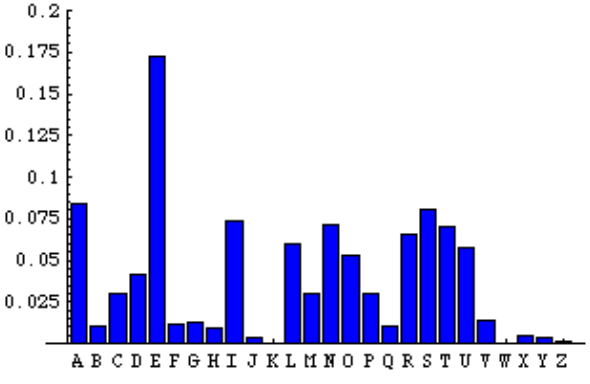
- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur
  - Analyse de fréquences pour casser le code
    - `PUALYNVBCLYULTLUAHSPZHAPVU`
      - Les lettres les plus fréquentes : `L` et `U`
      - `E` $\Rightarrow$ `L` ou `E` $\Rightarrow$ `U`
        - $p = 7$ ou $p = 16$



- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur
  - Analyse de fréquences pour casser le code
    - `PUALYNVBCLYULTLUAHSPZHAPVU`
      - Les lettres les plus fréquentes : `L` et `U`
      - `E` $\Rightarrow$ `L` ou `E` $\Rightarrow$ `U`
        - $p = 7$ ou $p = 16$
    - $p = 7 \Rightarrow$ `INTERGOUVERNEMENTALISATION`
      - Le mot le plus long de la langue française



- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
  - Force brute (seulement 25 chiffres possibles)
    - Vous seul avec un (petit) poil de courage
    - Un ordinateur
  - Analyse de fréquences pour casser le code
    - `PUALYNVBCLYULTLUAHSPZHAPVU`
      - Les lettres les plus fréquentes : `L` et `U`
      - `E` $\Rightarrow$ `L` ou `E` $\Rightarrow$ `U`
        - $p = 7$ ou $p = 16$
    - $p = 7 \Rightarrow$ `INTERGOUVERNEMENTALISATION`
      - Le mot le plus long de la langue française
    - $p = 16 \Rightarrow$ `ZEKVIXFLMVIEVDVEKRCZJRKZFE`



- Créé par Blaise de Vigénère (1523--1596)
  - Il utilise différents chiffres de César pour les lettres du message
    - Pour César la **clé** est p, le décalage
    - Pour Vigénère on utilise n clés p_i, $0 \leq i < n$
      - En fait la clé est elle-même un texte en général plus court que le texte à encoder

- Clé secrète `PARISDIDEROT`
- Message `JADORELINFORMATIQUE`
- Message codé

	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

- Clé secrète `PARISDIDEROT`
- Message `JADORELINFORMATIQUE`
- Message codé
  - $\texttt{J}, \texttt{P} \Rightarrow \texttt{Y}$

	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

- Clé secrète `PARISDIDEROT`
- Message `JADORELINFORMATIQUE`
- Message codé
  - $\texttt{J}, \texttt{P} \Rightarrow \texttt{Y}$
  - $\texttt{A}, \texttt{A} \Rightarrow \texttt{A}$

	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
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

- Clé secrète `PARISDIDEROT`
- Message `JADORELINFORMATIQUE`
- Message codé
  - `J, P` $\Rightarrow$ `Y`
  - `A, A` $\Rightarrow$ `A`
  - `D, R` $\Rightarrow$ `U`

	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

- Clé secrète
  `PARISDIDEROT`
- Message
  `JADORELINFORMATIQUE`
- Message codé
  - `J`, `P` $\Rightarrow$ `Y`
  - `A`, `A` $\Rightarrow$ `A`
  - `D`, `R` $\Rightarrow$ `U`
  - `O`, `I` $\Rightarrow$ `W`

	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

- Clé secrète
  `PARISDIDEROT`
- Message
  `JADORELINFORMATIQUE`
- Message codé
  - `J, P` $\Rightarrow$ `Y`
  - `A, A` $\Rightarrow$ `A`
  - `D, R` $\Rightarrow$ `U`
  - `O, I` $\Rightarrow$ `W`
  - ...
  - `M, P` $\Rightarrow$ `B`

	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

- Clé secrète
  `PARISDIDEROT`
- Message
  `JADORELINFORMATIQUE`
- Message codé
  - `J, P` $\Rightarrow$ `Y`
  - `A, A` $\Rightarrow$ `A`
  - `D, R` $\Rightarrow$ `U`
  - `O, I` $\Rightarrow$ `W`
  - ...
  - `M, P` $\Rightarrow$ `B`
  - ...

`YAUWJHTLRWCKBAKQIXM`

	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

- Clé secrète `PARISDIDEROT`
- Message reçu `HADMVLDLRXHLXXGIJWQHP`
- Message original

	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

- Clé secrète `PARISDIDEROT`
- Message reçu `HADMVLDLRXHLXXGIJWQHP`
- Message original
  - $\texttt{P}, \texttt{H} \Rightarrow \texttt{S}$

	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

- Clé secrète
  `PARISDIDEROT`
- Message reçu
  `HADMVLDLRXHLXXGIJWQHP`
- Message original
  - `P`, `H` $\Rightarrow$ `S`
  - `A`, `A` $\Rightarrow$ `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
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

- Clé secrète
  `PARISDIDEROT`
- Message reçu
  `HADMVLDLRXHLXXGIJWQHP`
- Message original
  - `P, H` $\Rightarrow$ `S`
  - `A, A` $\Rightarrow$ `A`
  - `R, D` $\Rightarrow$ `M`

	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

- Clé secrète `PARISDIDEROT`
- Message reçu `HADMVLDLRXHLXXGIJWQHP`
- Message original
  - `P, H` $\Rightarrow$ `S`
  - `A, A` $\Rightarrow$ `A`
  - `R, D` $\Rightarrow$ `M`
  - `I, M` $\Rightarrow$ `E`

	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

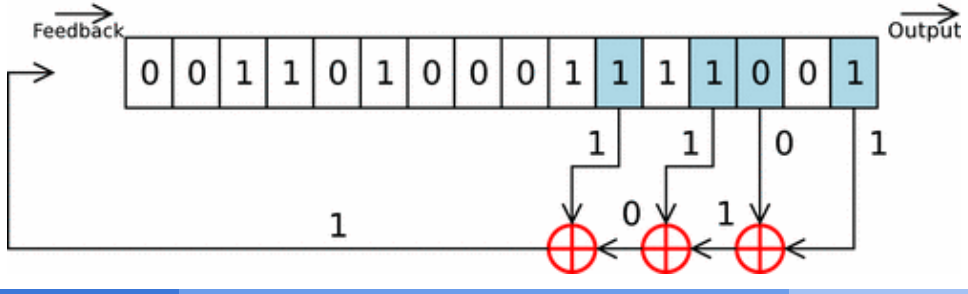
- Clé secrète
  `PARISDIDEROT`
- Message reçu
  `HADMVLDLRXHLXXGIJWQHP`
- Message original
  - `P, H` $\Rightarrow$ `S`
  - `A, A` $\Rightarrow$ `A`
  - `R, D` $\Rightarrow$ `M`
  - `I, M` $\Rightarrow$ `E`
  - ...

`SAMEDIVINGTSIXPARTIEL`

	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

- Il a fallu attendre environ 300 ans avant de trouver la méthode permettant de casser ce code
  - Maintenant, casser ce code n'est pas très difficile, si le message est assez long
    - On peut y repérer des répétitions et deviner la longueur de la clé, sinon on peut essayer diverses longueurs de clés
    - Puis faire des analyses fréquentielles
    - Un bon ordinateur (ou beaucoup de patience) et le tour est joué
- Chiffre de Vernam/Mauborgne
  - Un chiffre de Vigénère pour lequel
    - La clé est aussi longue que le texte
    - La clé est obtenue par distribution aléatoire
    - La clé ne doit être employée qu'une seule fois
    - Si les conditions sont réunies, le chiffre est inviolable
      - Il a probablement été utilisé pour sécuriser le « téléphone rouge »

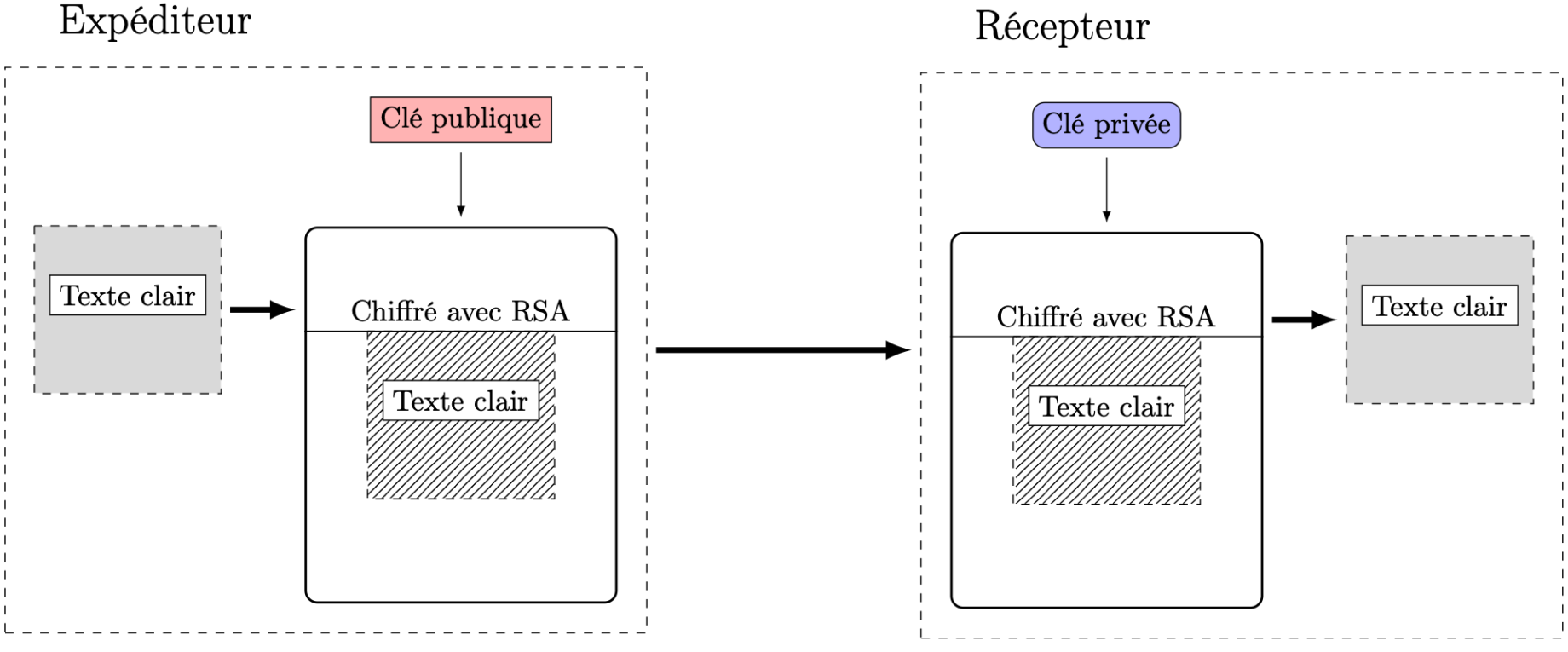
- Aujourd'hui on utilise des systèmes plus solides
  - Symétriques ou à clé secrète
  - Par bloc (par exemple le DES) ou par flot
- Les plus standards ne sont pas considérés comme très solides
  - Le DES peut être cassé en quelques jours/heures avec quelques dizaines d'ordinateurs
  - Mais c'est utile tout de même si vos messages n'ont pas un caractère vital ou si la durée de vie du contenu du message n'est pas très longue
- LFSR
  - Permet d'obtenir une suite pseudo-aléatoire
    - Utile, par exemple, pour obtenir un masque jetable



- Aujourd'hui on utilise des systèmes plus solides que les chiffrement par flot pour les échanges très secrets
  - Asymétriques ou à clés publiques

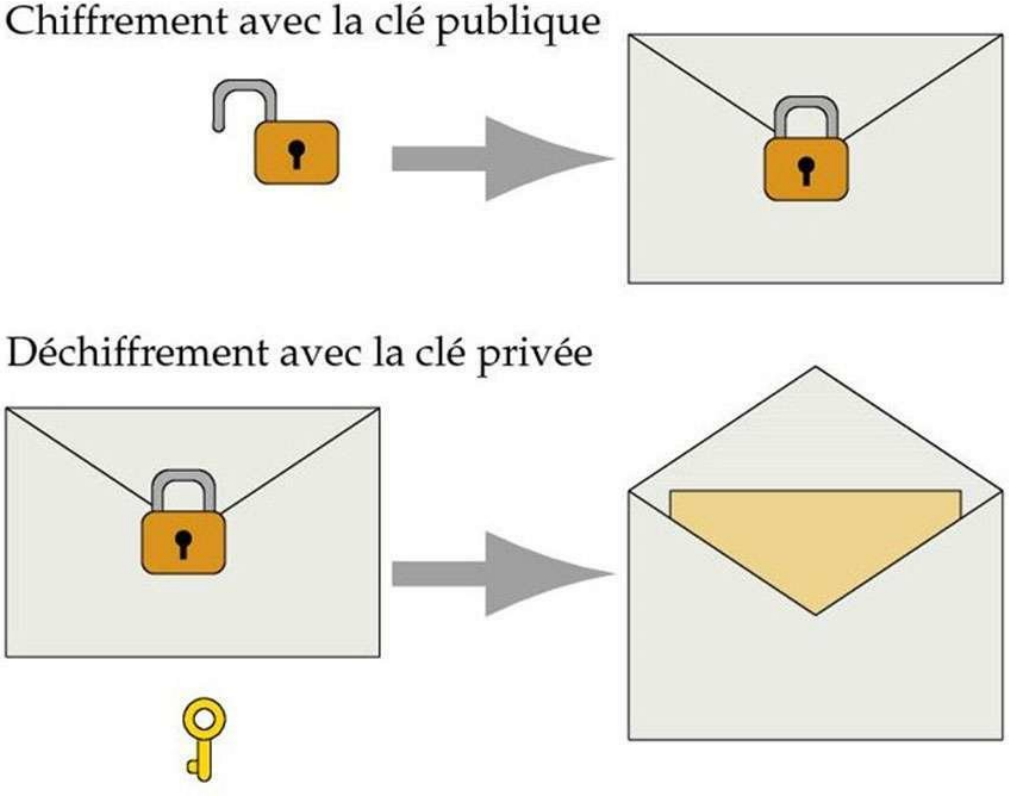
- Aujourd'hui on utilise des systèmes plus solides que les chiffrement par flot pour les échanges très secrets
  - Asymétriques ou à clés publiques
- Comment ça marche ?
  - Deux clés : publique pour coder et privée pour decoder

- Aujourd'hui on utilise des systèmes plus solides que les chiffrement par flot pour les échanges très secrets
  - Asymétriques ou à clés publiques
- Comment ça marche ?
  - Deux clés : publique pour coder et privée pour decoder



- Qui sont les clés publiques et privées ?

- Qui sont les clés publiques et privées ?
  - Dans le monde physique, nous pourrions utiliser des cadenas et des clés

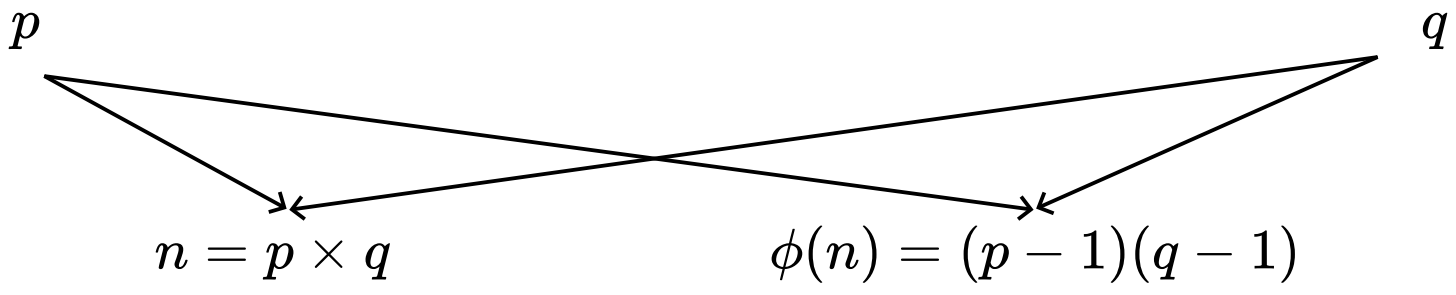


- Qui sont les clés publiques et privées ?
  - Dans le monde physique, nous pourrions utiliser des cadenas et des clés
  - Dans le monde numérique, nous utilisons les mathématique

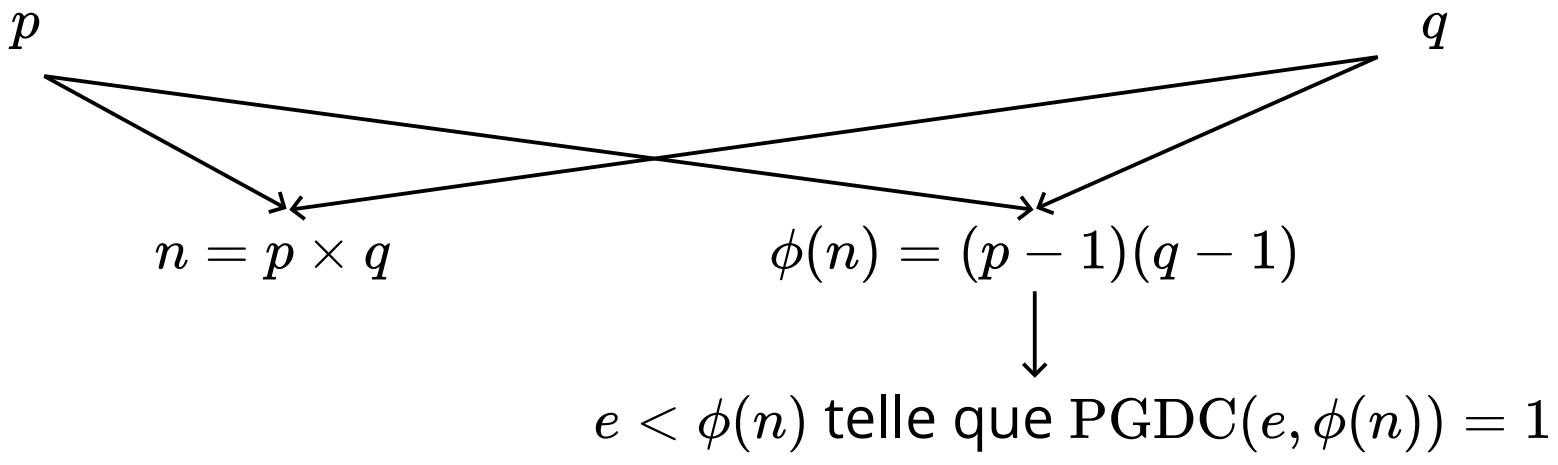
- On prend deux nombres p et q premiers

p q

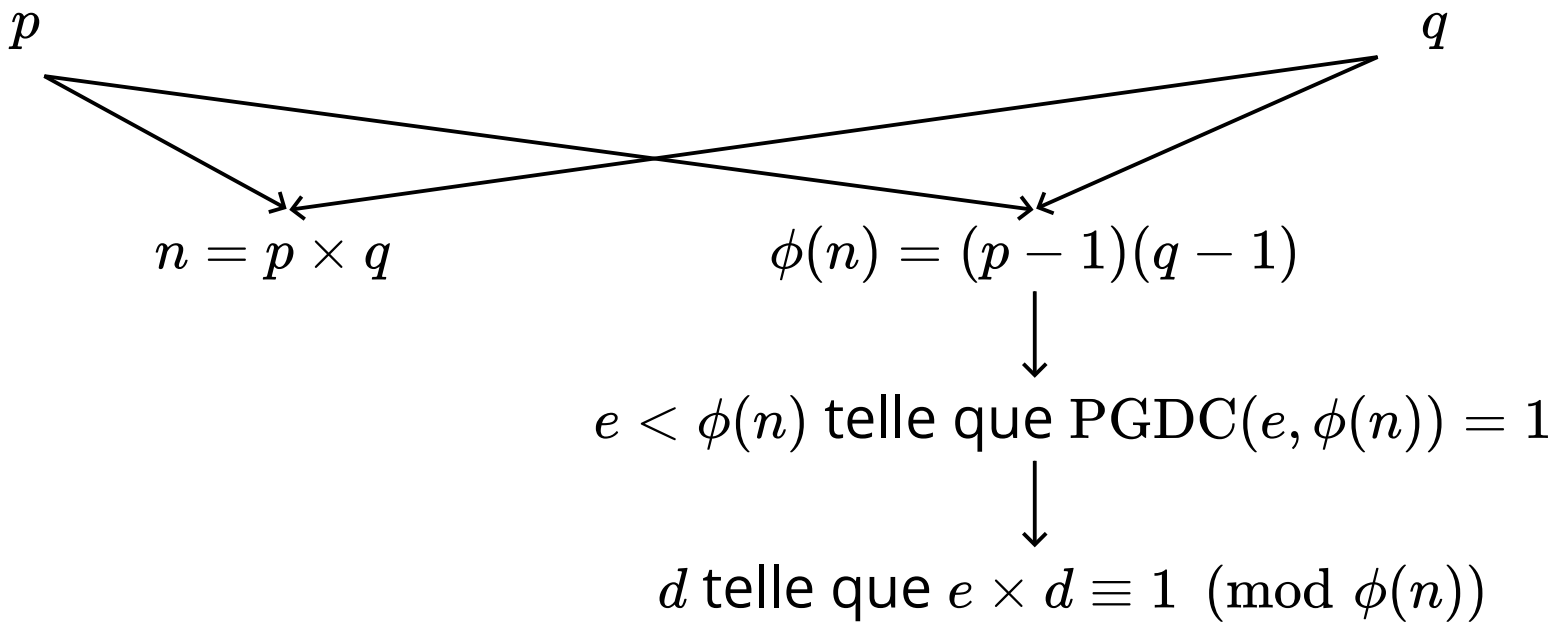
- On prend deux nombres p et q premiers



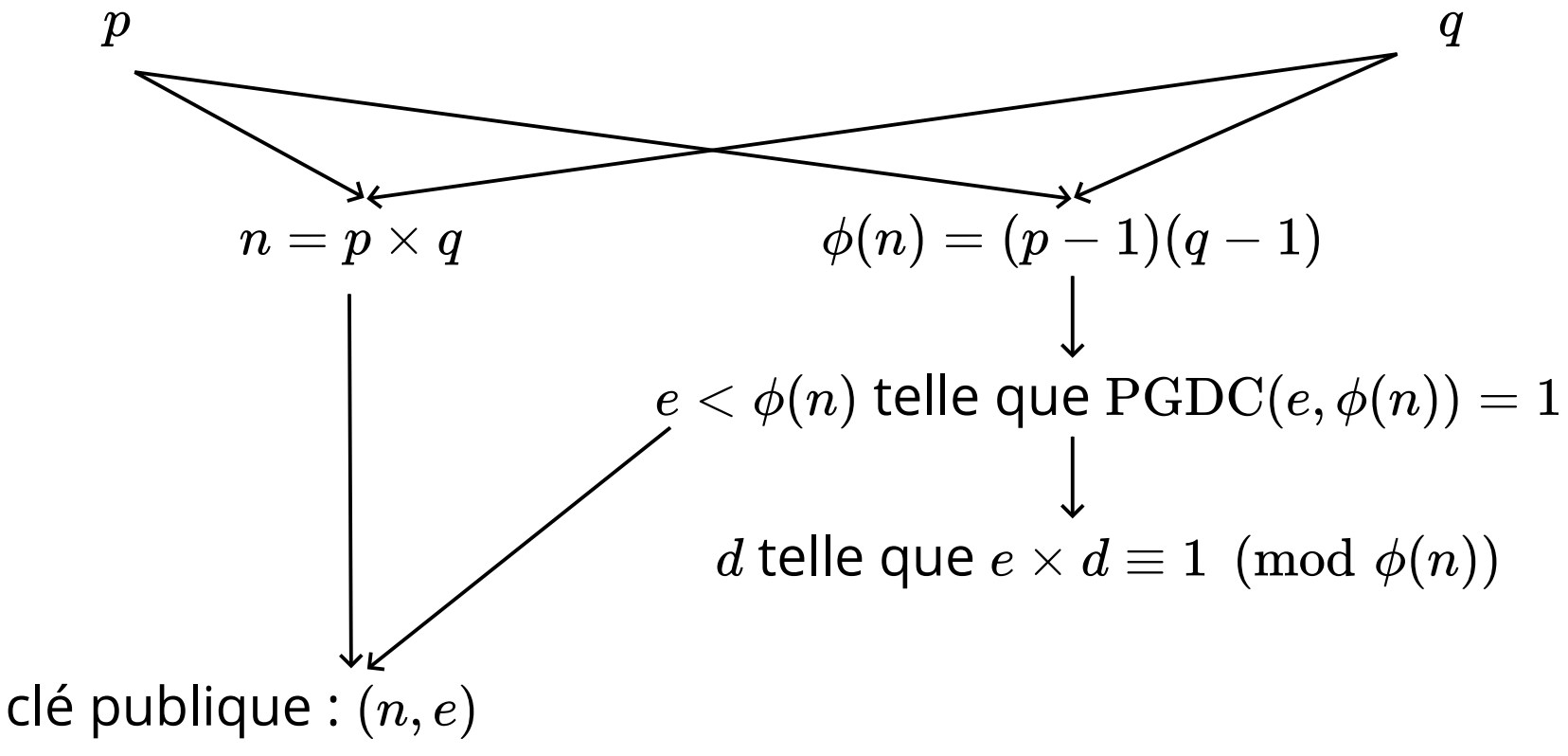
- On prend deux nombres p et q premiers



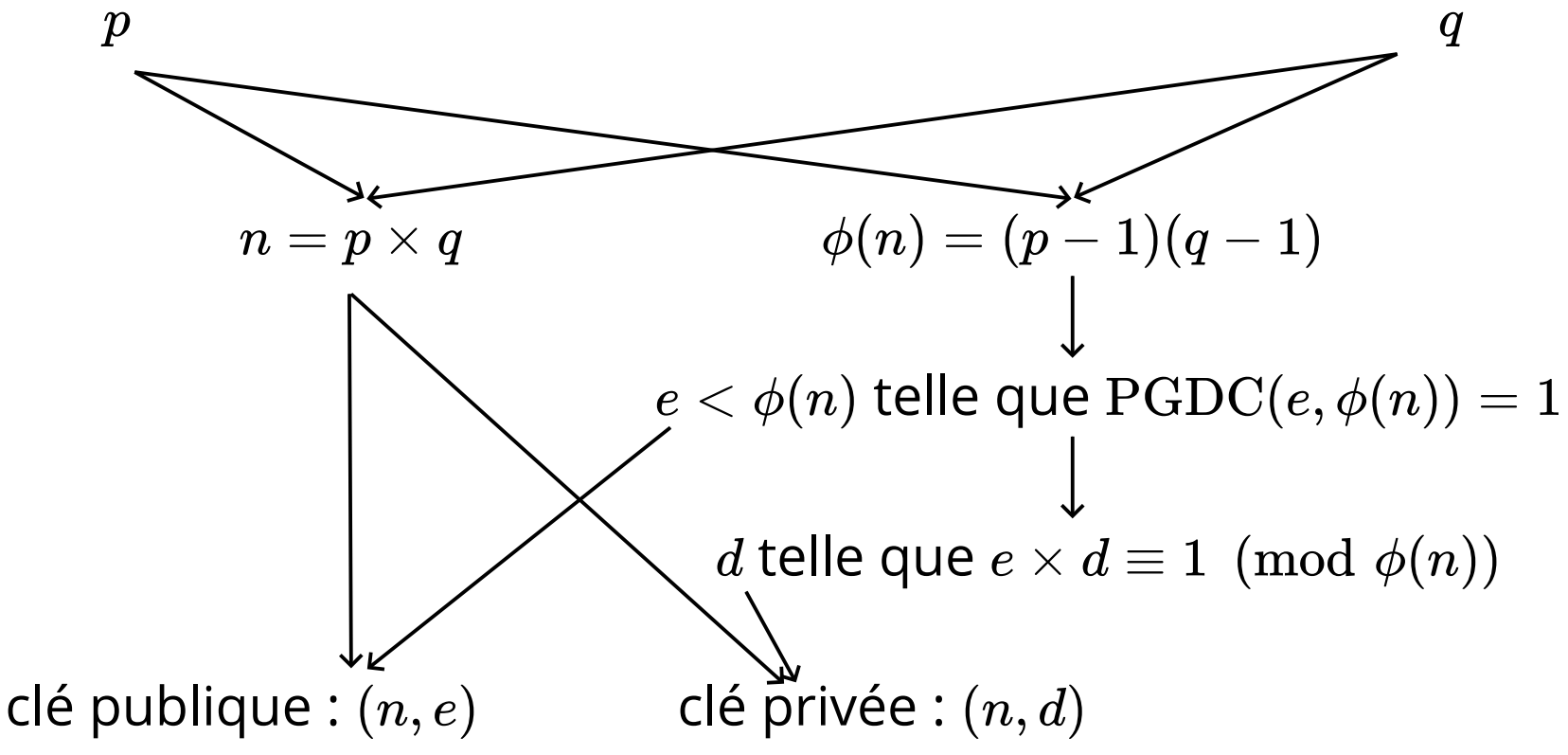
- On prend deux nombres p et q premiers

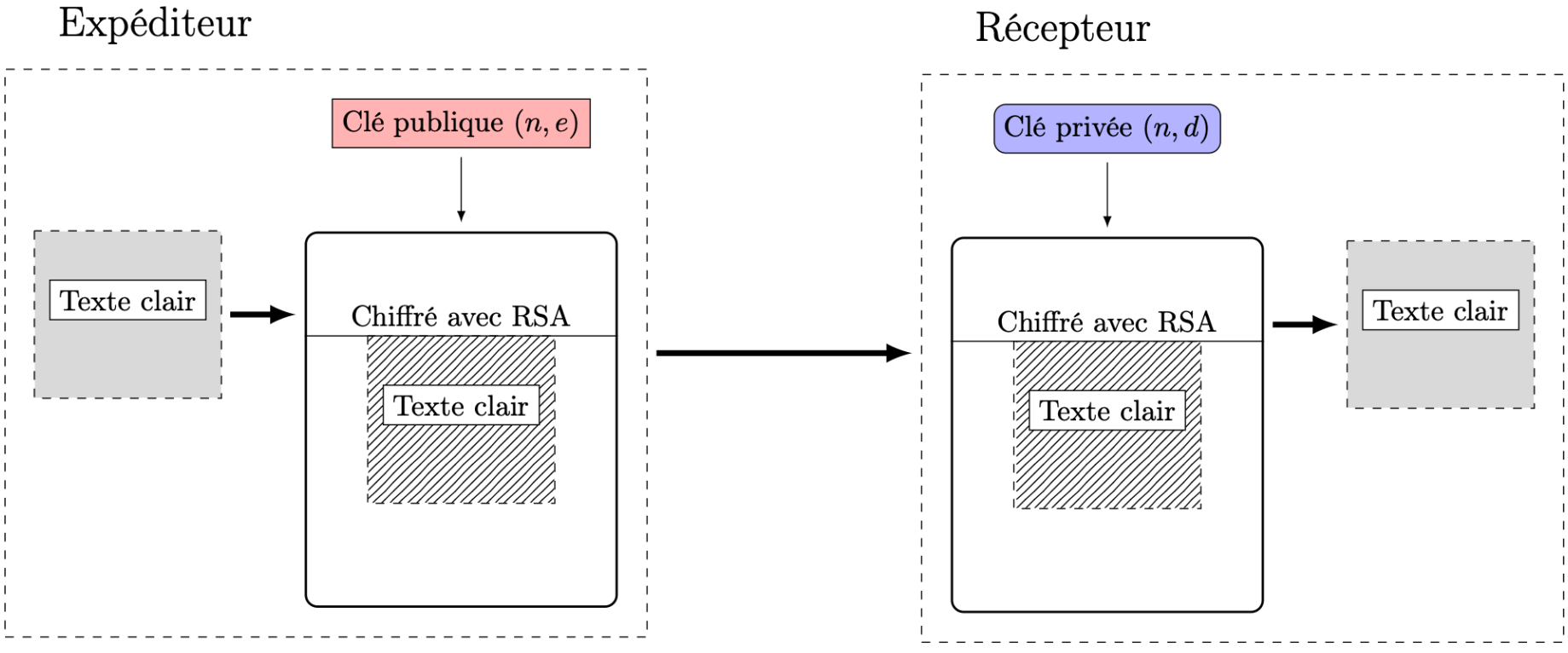


- On prend deux nombres p et q premiers



- On prend deux nombres p et q premiers





- Pour chiffrer le message M (entier strictement inférieur à n)
  - On calcule $C \equiv M^e \pmod{n}$
- Pour déchiffrer C
  - On calcule $M \equiv C^d \pmod{n}$

- Exemple
  - $p = 7$ et $q = 11$
  - $n = 7 \times 11 = 77$ et $\phi(n) = 6 \times 10 = 60$
  - Prenons $e = 7 < 60$ qui est premier avec 60
  - $d = 43$: $7 \times 43 = 301 = 5 \times 60 + 1$
  - Clé publique $(77, 7)$, clé privée $(77, 43)$
  - Message : `B`
    - En ASCII : 42
    - Valeur décimale : $42 < 77$
      - Si supérieur, on découpe en une suite de nombres plus petits que $n = 77$
      - 18664546135659858 devient $18\ 66\ 45\ 46\ 13\ 56\ 59\ 8\ 58$
  - Codage : $42^7 \pmod{77} = 70$
  - Décodage : $70^{43} \pmod{77} = 42$

- Puissance modulo : $42^7 \pmod{77}$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
- Algorithme plus efficace : $70^{43} \pmod{77}$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
- Algorithme plus efficace : $70^{43} \pmod{77}$
  - $70^2 \pmod{77} = 49$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
- Algorithme plus efficace : $70^{43} \pmod{77}$
  - $70^2 \pmod{77} = 49$
  - $70^4 \pmod{77} = 49 \times 49 \pmod{77} = 14$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
- Algorithme plus efficace : $70^{43} \pmod{77}$
  - $70^2 \pmod{77} = 49$
  - $70^4 \pmod{77} = 49 \times 49 \pmod{77} = 14$
  - $70^8 \pmod{77} = 14 \times 14 \pmod{77} = 42$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
- Algorithme plus efficace : $70^{43} \pmod{77}$
  - $70^2 \pmod{77} = 49$
  - $70^4 \pmod{77} = 49 \times 49 \pmod{77} = 14$
  - $70^8 \pmod{77} = 14 \times 14 \pmod{77} = 42$
  - $70^{16} \pmod{77} = 42 \times 42 \pmod{77} = 70$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
- Algorithme plus efficace : $70^{43} \pmod{77}$
  - $70^2 \pmod{77} = 49$
  - $70^4 \pmod{77} = 49 \times 49 \pmod{77} = 14$
  - $70^8 \pmod{77} = 14 \times 14 \pmod{77} = 42$
  - $70^{16} \pmod{77} = 42 \times 42 \pmod{77} = 70$
  - $70^{32} \pmod{77} = 70 \times 70 \pmod{77} = 49$

- Puissance modulo : $42^7 \pmod{77}$
  - $42^1 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
  - $70 \times 42 \pmod{77} = 2940 \pmod{77} = 14$
  - $14 \times 42 \pmod{77} = 588 \pmod{77} = 49$
  - $49 \times 42 \pmod{77} = 2058 \pmod{77} = 56$
  - $56 \times 42 \pmod{77} = 2352 \pmod{77} = 42$
  - $42 \times 42 \pmod{77} = 1764 \pmod{77} = 70$
- Algorithme plus efficace : $70^{43} \pmod{77}$
  - $70^2 \pmod{77} = 49$
  - $70^4 \pmod{77} = 49 \times 49 \pmod{77} = 14$
  - $70^8 \pmod{77} = 14 \times 14 \pmod{77} = 42$
  - $70^{16} \pmod{77} = 42 \times 42 \pmod{77} = 70$
  - $70^{32} \pmod{77} = 70 \times 70 \pmod{77} = 49$
  - $70^{43} \pmod{77} = 70^{32} * 70^8 * 70^2 * 70 \pmod{77} = 49 * 42 * 49 * 70 \pmod{77} = 42$

- La difficulté repose sur le fait que connaissant n et e il est très difficile de trouver d
  - Il faut pour cela connaître p et q
    - C'est-à-dire décomposer le nombre n en facteurs premiers
  - p, q, d, e sont normalement de très très très grand nombres

- La difficulté repose sur le fait que connaissant n et e il est très difficile de trouver d
  - Il faut pour cela connaître p et q
    - C'est-à-dire décomposer le nombre n en facteurs premiers
  - p, q, d, e sont normalement de très très très grand nombres
- Trouver de très grands nombres premiers est une tâche très ardue
  - En 1456 le plus grand nombre premier connu était 8191, soit de 4 chiffres
  - En 1750 Euler a produit le premier nombre premier de 10 chiffres
  - En 1996 le plus grand nombre premier connu s'écrivait avec ≈ 420.000 chiffres
  - En 2017 le plus grand s'écrit avec $\approx 23.000.000$ chiffres
    - Consulter le *Great Internet Mersenne Prime Search*