Principes de fonctionnement des machines binaires

2019/2020

Pierluigi Crescenzi

Université de Paris, IRIF







- 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 ⇒ pas de moyenne ⇒ 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
 - lacktriangle 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

Α	В	C	D	Ε	F	•••	Χ	Υ	Z
D	Е	F	G	Н			Α	В	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

Α	В	C	D	Е	F	•••	X	Υ	Z
D	Е	F	G	Н			Α	В	C

 \circ ATTAQUE $\Rightarrow \dots$

- 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

Α	В	C	D	Е	F	•••	X	Υ	Z
D	Е	F	G	Н			Α	В	С

- \circ ATTAQUE $\Rightarrow \dots$
- ...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

Α	В	C	D	Е	F	•••	X	Υ	Z
D	Е	F	G	Н			Α	В	C

- \circ ATTAQUE $\Rightarrow \dots$
- O ... 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

Α	В	C	D	Е	F	•••	X	Υ	Z
D	Е	F	G	Н	I		Α	В	С

- \circ ATTAQUE $\Rightarrow \dots$
- O ... 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

Α	В	C	D	Е	F	•••	X	Υ	Z
D	Е	F	G	Н			Α	В	C

- \circ ATTAQUE $\Rightarrow \dots$
- O ... 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

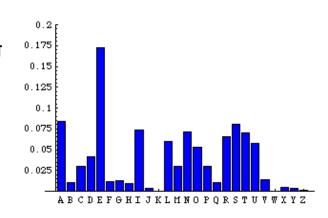
- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
 - Force brute (seulement 25 chiffres possibles)
 - Vous seul avec un (petit) poil de courage
 - Un ordinateur

- 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
 - O PUALYNVBCLYULTLUAHSPZHAPVU
 - Les lettres les plus fréquentes : L et ʊ

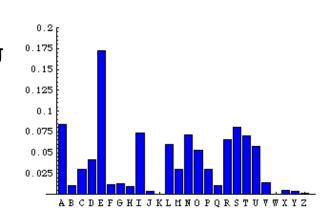
- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
 - Force brute (seulement 25 chiffres possibles)
 - Vous seul avec un (petit) poil de courage
 - Un ordinateur
 - Analyse de fréquences pour casser le code
 - O PUALYNVBCLYULTLUAHSPZHAPVU
 - Les lettres les plus fréquentes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

$$\circ$$
 E \Rightarrow L ou E \Rightarrow U

$$\circ~p=7$$
 ou $p=16$

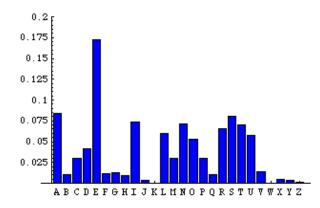


- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
 - Force brute (seulement 25 chiffres possibles)
 - Vous seul avec un (petit) poil de courage
 - Un ordinateur
 - Analyse de fréquences pour casser le code
 - O PUALYNVBCLYULTLUAHSPZHAPVU
 - Les lettres les plus fréquentes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

$$\circ$$
 E \Rightarrow L ou E \Rightarrow U

$$\circ~p=7$$
 ou $p=16$

- \circ $p=7\Rightarrow$ INTERGOUVERNEMENTALISATION
 - Le mot le plus long de la langue française

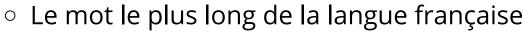


- L'utilisation du chiffre de César ne peut pas bluffer quelqu'un très longtemps
 - Force brute (seulement 25 chiffres possibles)
 - Vous seul avec un (petit) poil de courage
 - Un ordinateur
 - Analyse de fréquences pour casser le code
 - O PUALYNVBCLYULTLUAHSPZHAPVU
 - Les lettres les plus fréquentes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

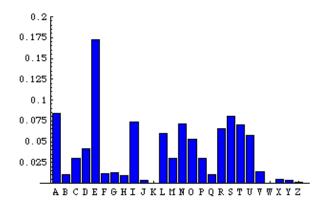
$$\circ \ \ E \Rightarrow L \ ou \ E \Rightarrow U$$

$$\circ~p=7$$
 ou $p=16$



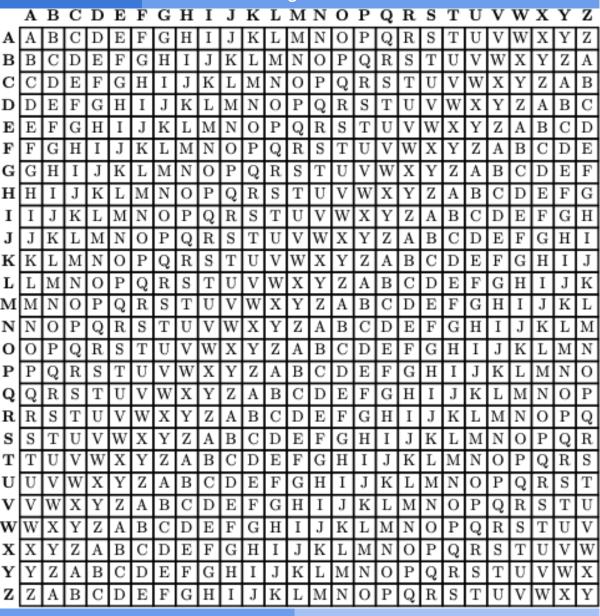


$$\circ$$
 $p=16\Rightarrow$ ZEKVIXFLMVIEVDVEKRCZJRKZFE



- 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
 - \circ Pour Vigénère on utilise n clés p_i , $0 \le i < n$
 - En fait la clé est elle-même un texte en général plus court que le texte à encoder

- Clé secrète
 PARISDIDEROT
- MessageJADORELINFORMATIQUE
- Message codé



- Clé secrète
 PARISDIDEROT
- Message JADORELINFORMATIQUE
- Message codé
 - \blacksquare J,P \Rightarrow Y

								<u> </u>			ac	V 1	90	'''												
	<u>A</u>	В	$^{\rm c}$	D	Е	F	G	н	<u> </u>	J	к	L	м	N	<u>o</u>	Р	$\frac{\mathbf{Q}}{\mathbf{Q}}$	R	s	т	U	$\underline{\mathbf{v}}$	$\underline{\mathbf{w}}$	<u>x</u>	Y	\mathbf{z}
A	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z
В	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{C}	С	D	Е	F	$^{\mathrm{G}}$	Η	Ι	J	Κ	$_{\rm L}$	М	Ν	0	Р	Q	${\bf R}$	S	Т	${\rm U}$	${\bf v}$	W	Х	Y	Z	Α	В
D	D	Е	F	\mathbf{G}	Η	Ι	J	K	L	М	Ν	О	Ρ	Q	${\bf R}$	S	Т	U	${\bf v}$	W	Х	Y	\mathbf{z}	Α	В	$^{\rm C}$
\mathbf{E}	Е	F	G	Н	Ι	J	Κ	$_{\rm L}$	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D
\mathbf{F}	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
\mathbf{G}	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н
J	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι
\mathbf{K}	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J
\mathbf{L}	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ
\mathbf{M}	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L
N	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М
o	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О
Q	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р
\mathbf{R}	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	М	Ν	О	Р	Q
\mathbf{s}	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R
\mathbf{T}	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S
\mathbf{U}	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	N	О	Р	Q	R	S	Т	U
\mathbf{w}	w	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V
\mathbf{x}	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W
\mathbf{Y}	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	w	Х
\mathbf{z}	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	х	Y
													T					_								_

- Clé secrète
 PARISDIDEROT
- Message JADORELINFORMATIQUE
- Message codé
 - lacksquare J, P \Rightarrow Y
 - lacksquare A, A \Rightarrow A

	Δ	В	C	D	Е	F	G	н	Ι	J	K	T.	м	N	o	Р	Q	R	s	т	П	v	w	x	Y	\mathbf{z}
A	A.	Б	6	<u></u>	E	F	G	ш	Ť	Γī	IV.	Ē	3.4	N	_	Р	र्ज्	Б	S	T	ĪΤ	v	777	v	Ī	Z
A	A.	Δ	5	D D	-	-		п	7	J TZ	T	п	IVI NT	77	0	-	ν, D	n.		T.T.	v	V 337	37	A 37	7	$\overline{}$
В	В	С	D	Е	F	G	H	I	J	K	L	M	N	0	Р	Q	R	S	Т	U	·	W	X	Y	Z	A
C	С	D	Е	F	G	Н	I	J	K	-	М	N	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	A	В
D	D	Е	F	G	Η	Ι	J	K	-	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С
Е	Е	F	G	Η	I	J	K	-	Μ	-	0	Ρ	Q	R	-	Т	U	V	W	Х	Y	Z	Α	В	С	D
F	F	G	Н	I	J	K	L	М		О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
\mathbf{G}	G	Η	Ι	J	K	L	М	Ν	-	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Η	Ι	J	K	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
Ι	Ι	J	K	$_{\rm L}$	М	Ν	0	Ρ	Q	R	S	Т	D	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η
\mathbf{J}	J	Κ	L	\mathbf{M}	Ν	0	Р	Q	${\bf R}$	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	\mathbf{E}	F	G	Η	Ι
\mathbf{K}	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J
${f L}$	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ
\mathbf{M}	Μ	Ν	О	Ρ	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L
\mathbf{N}	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М
\mathbf{o}	О	Р	Q	R	S	Т	U	V	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О
Q	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р
\mathbf{R}	R	s	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q
\mathbf{s}	s	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R
\mathbf{T}	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S
\mathbf{U}	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	N	О	Р	Q	R	S	Т	U
w	w	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	s	Т	U	V
\mathbf{x}	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	w
\mathbf{Y}	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	_	0	Ρ	Q	R	S	Т	U	V	W	Х
\mathbf{z}	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y
	_	_											T					Ť					_			_

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

							۰ ک	<u> </u>		<u> </u>	uc	VI	90	110	10											
	A	В	\mathbf{c}	D	\mathbf{E}	\mathbf{F}	\mathbf{G}	Н	Ι	J	K	\mathbf{L}	М	Ν	О	Р	Q	\mathbf{R}	\mathbf{s}	Т	U	\mathbf{v}	W	\mathbf{X}	\mathbf{Y}	\mathbf{z}
${\bf A}$	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	\mathbf{R}	S	Т	U	\mathbf{V}	W	Х	Y	Z
\mathbf{B}	В	С	D	Ε	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{c}	$^{\rm C}$	D	Е	F	G	Η	Ι	J	K	L	М	Ν	O	Ρ	Q	R	S	Т	U	\mathbf{V}	W	Х	Y	Z	Α	В
\mathbf{D}	D	Е	F	\mathbf{G}	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	\mathbf{v}	W	Х	Y	\mathbf{z}	Α	В	$^{\rm C}$
\mathbf{E}	Е	F	G	Н	Ι	J	K	$_{\rm L}$	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	$^{\rm C}$	D
\mathbf{F}	F	G	Η	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
\mathbf{G}	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
н	Η	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η
J	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι
\mathbf{K}	K	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J
\mathbf{L}	L	Μ	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	K
\mathbf{M}	Μ	Ν	О	Р	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L
${\bf N}$	Ν	О	Р	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	M
О	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	О
Q	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	P
${f R}$	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ	\mathbf{L}	М	Ν	О	Р	Q
\mathbf{s}	S	Τ	U	V	W	Х	Y	\mathbf{Z}	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ	${\rm L}$	М	Ν	О	Р	Q	${\bf R}$
\mathbf{T}	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	Ν	0	Р	Q	\mathbf{R}	S
U	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	O	Р	Q	R	S	Т	U
W	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V
\mathbf{x}	Х	Y	Z	Α	В	C	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	P	Q	R	S	Τ	U	V	W
\mathbf{Y}	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	P	Q	R	S	Τ	U	V	W	Х
\mathbf{z}	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y

Le chiffre de Vigénère

- Clé secrète
 PARISDIDEROT
- Message JADORELINFORMATIQUE
- Message codé
 - \blacksquare J, P \Rightarrow Y
 - lacksquare A, A \Rightarrow A
 - lacksquare D, R \Rightarrow U
 - lacksquare 0, I \Rightarrow W

								C11		•	ac	VI	90	110												
	A	В	\mathbf{c}	D	Е	F	\mathbf{G}	Н	Ι	J	K	\mathbf{L}	М	Ν	О	Р	Q	\mathbf{R}	\mathbf{s}	т	U	\mathbf{v}	W	Х	Y	\mathbf{z}
\mathbf{A}	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	$_{\rm L}$	М	Ν	О	Р	Q	\mathbf{R}	\mathbf{s}	Т	U	V	W	Х	Y	\mathbf{Z}
\mathbf{B}	В	С	D	Е	F	G	Η	Ι	J	K	L	$_{\mathrm{M}}$	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{C}	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В
\mathbf{D}	D	Е	F	G	Н	Ι	J	K	$_{\rm L}$	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С
\mathbf{E}	Е	F	G	Н	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D
\mathbf{F}	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
\mathbf{G}	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Н	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н
J	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι
\mathbf{K}	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J
${f L}$	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ
\mathbf{M}	Μ	Ν	О	Ρ	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L
\mathbf{N}	Ν	0	Р	Q	\mathbf{R}	S	Т	U	V	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М
О	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	Κ	L	Μ	Ν	О
Q	Q	R	S	Т	U	V	w	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ
\mathbf{R}	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q
\mathbf{s}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R
\mathbf{T}	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S
\mathbf{U}	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U
\mathbf{w}	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V
\mathbf{x}	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W
\mathbf{Y}	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х
\mathbf{z}	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y
													T									_			11.6	

Le chiffre de Vigénère

- Clé secrète
 PARISDIDEROT
- Message JADORELINFORMATIQUE
- Message codé

$$\blacksquare$$
 J, P \Rightarrow Y

$$lacksquare$$
 A, A \Rightarrow A

$$\blacksquare$$
 D, R \Rightarrow U

$$lacksquare$$
 0, I \Rightarrow W

$$\blacksquare$$
 M, P \Rightarrow B

								C 1 1		<u> </u>	uc	VI	90	'''												
	A	В	С	D	Е	F	\mathbf{G}	н	I	J	к	L	М	Ν	o	Р	Q	R	\mathbf{s}	т	U	\mathbf{v}	w	X	Y	\mathbf{z}
\mathbf{A}	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Р	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z
\mathbf{B}	В	С	D	Ε	F	G	Η	Ι	J	Κ	L	М	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{C}	С	D	Е	F	$^{\mathrm{G}}$	Η	Ι	J	Κ	$_{\rm L}$	М	Ν	0	Р	Q	${\bf R}$	S	Т	${\rm U}$	${\bf v}$	W	Х	Y	Z	Α	В
D	D	Е	F	$^{\mathrm{G}}$	$_{\mathrm{H}}$	Ι	J	K	L	М	Ν	О	Ρ	Q	${\bf R}$	S	Т	U	${\bf v}$	W	Х	Y	\mathbf{Z}	Α	В	$^{\rm C}$
\mathbf{E}	\mathbf{E}	F	G	Н	Ι	J	K	\mathbf{L}	Μ	Ν	О	Ρ	Q	R	S	Т	U	\mathbf{V}	W	Х	Y	\mathbf{Z}	Α	В	С	D
\mathbf{F}	F	G	Н	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
\mathbf{G}	G	Η	Ι	J	Κ	L	Μ	Ν	О	Р	Q	$_{\mathrm{R}}$	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Η	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н
J	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι
\mathbf{K}	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J
\mathbf{L}	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ
\mathbf{M}	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L
N	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М
О	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О
Q	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Н	Ι	J	K	L	Μ	Ν	О	Ρ
\mathbf{R}	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р	Q
\mathbf{s}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R
\mathbf{T}	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	О	Р	Q	R	S
\mathbf{U}	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	Α	В	С	D	Е	F	\mathbf{G}	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U
\mathbf{W}	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V
\mathbf{X}	Χ	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W
\mathbf{Y}	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х
\mathbf{z}	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y

- Clé secrète
 PARISDIDEROT
- MessageJADORELINFORMATIQUE
- Message codé

$$\blacksquare$$
 J, P \Rightarrow Y

$$lacksquare$$
 A, A \Rightarrow A

$$lacksquare$$
 D, R \Rightarrow U

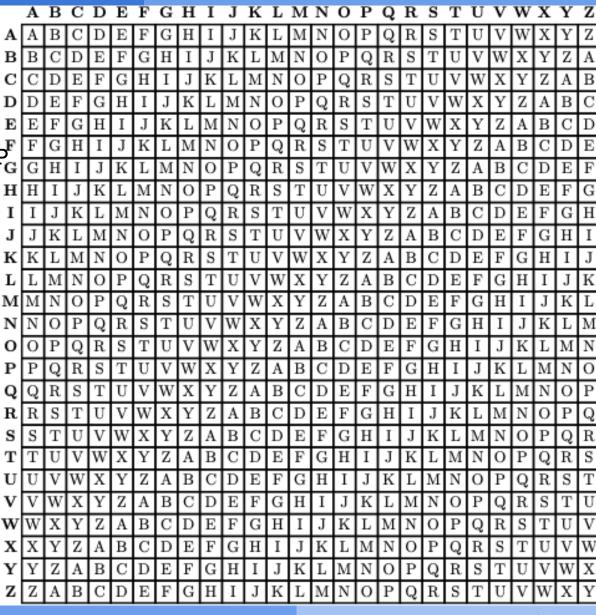
$$lacksquare$$
 0, I \Rightarrow W

$$\blacksquare$$
 M, P \Rightarrow B

YAUWJHTLRWCKBAKQIXM

	A	В	С	D	Е	\mathbf{F}	\mathbf{G}	н	Ι	J	K	\mathbf{L}	М	N	o	Р	Q	R	\mathbf{s}	т	U	v	w	х	Y	z
\mathbf{A}	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z
В	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{C}	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В
D	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С
\mathbf{E}	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Χ	Y	Z	Α	В	С	D
\mathbf{F}	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Ε
\mathbf{G}	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η
J	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι
K	K	\mathbf{L}	М	Ν	О	Р	Q	${\bf R}$	S	Τ	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	\mathbf{E}	F	\mathbf{G}	Η	Ι	J
\mathbf{L}	\mathbf{L}	Μ	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	K
М	М	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L
Ν	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М
О	0	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν
P	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О
Q	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Ρ
\mathbf{R}	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Ρ	Q
S	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	I	J	K	L	M	N	0	Р	Q	R
Т	Т	U	V	W	Х	Y	Z	A	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S
U	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т
v	V	W	X	Y	Z	A	В	С	D	Е	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	Т	U
W	W	X	Y	Z	A	В	С	D	Е	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	Т	U	V
X	X	Y	Z	A	В	С	D	Е	F	G	H	I	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W
Y	Y	Z	A	В	С	D	Е	F	G	H	I	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	X
Z	Z	А	В	С	D	Е	F	G	Η	Ι	J	K	L	М	N	О	Р	Q	R	S	Т	U	V	W	X	Y

- Clé secrète
 PARISDIDEROT
- Message reçu E
 HADMVLDLRXHLXXGIJWQHP_G
- Message original



- Clé secrète
 PARISDIDEROT
- Message reçu
 HADMVLDLRXHLXXGIJWQHP
- Message original
 - ightharpoonup P, H \Rightarrow S

ABCDEFGHIJKLMNOPQRSTUVWXY																										
	A	В	\mathbf{c}	D	\mathbf{E}	\mathbf{F}	\mathbf{G}	н	Ι	J	K	\mathbf{L}	М	Ν	О	Р	Q	\mathbf{R}	S	\mathbf{T}	U	\mathbf{v}	W	\mathbf{X}	\mathbf{Y}	\mathbf{z}
\mathbf{A}	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z
\mathbf{B}	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{C}	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В
D	D	Е	F	G	Н	Ι	J	Κ	$_{\rm L}$	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С
\mathbf{E}	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D
P_{C}^{F}	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε
\mathbf{G}	G	Η	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н
J	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι
\mathbf{K}	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J
\mathbf{L}	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ
\mathbf{M}	Μ	Ν	0	Р	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L
N	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М
О	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О
Q	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р
\mathbf{R}	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Р	Q
\mathbf{s}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R
\mathbf{T}	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S
\mathbf{U}	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U
\mathbf{W}	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V
\mathbf{x}	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Т	U	V	W
\mathbf{Y}	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Т	U	V	W	Х
\mathbf{z}	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y
						<u></u>							T									_			11.6	

- Clé secrète
 PARISDIDEROT
- Message reçu
 HADMVLDLRXHLXXGIJWQHP
- Message original
 - ightharpoonup P, H \Rightarrow S
 - lacksquare A, A \Rightarrow A

ABCDEFGHIJKLMNOPQRSTUVWXY																										
	A	В	\mathbf{C}	D	\mathbf{E}	F	\mathbf{G}	н	Ι	J	\mathbf{K}	\mathbf{L}	М	Ν	О	Р	Q	\mathbf{R}	\mathbf{s}	\mathbf{T}	U	\mathbf{v}	W	\mathbf{X}	\mathbf{Y}	\mathbf{z}
${\bf A}$	Α	В	С	D	Е	F	G	Η	Ι	J	К	L	М	Ν	О	Р	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z
\mathbf{B}	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{C}	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В
\mathbf{D}	D	Е	F	G	Н	Ι	J	K	$_{\rm L}$	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	$^{\rm C}$
\mathbf{E}	Е	F	G	Н	Ι	J	K	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	$^{\rm C}$	D
P_{G}^{F}	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
\mathbf{G}	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η
\mathbf{J}	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι
\mathbf{K}	Κ	L	М	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J
${f L}$	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	\mathbf{G}	Η	Ι	J	Κ
\mathbf{M}	Μ	Ν	О	Р	Q	${\bf R}$	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L
N	Ν	О	Ρ	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	${\rm M}$
О	О	Р	Q	R	S	Т	U	V	W	Χ	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	О
\mathbf{Q}	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	$_{\rm L}$	Μ	Ν	О	Р
\mathbf{R}	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	О	Р	Q
\mathbf{s}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	$_{\rm L}$	Μ	Ν	О	Ρ	Q	${\bf R}$
\mathbf{T}	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	О	Р	Q	R	S
\mathbf{U}	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т
\mathbf{v}	V	W	Χ	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Τ	U
\mathbf{W}	W	Χ	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V
\mathbf{X}	Χ	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Τ	U	V	W
\mathbf{Y}	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Τ	U	V	W	Х
\mathbf{z}	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y
																									11.6	

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

	Λ	В	С	D	Е	F	G	н	т	J	K	T.	м	N	O	Р	Q	R	\mathbf{s}	т	TT	v	w	v	Y	\mathbf{z}
	A	Б	6	듑		_	_	77	Ť	Ť	K V	Ŧ	3.4	NT.	_	Б	Š	Б	_	<u>T</u>	TT	77	77	v	<u>.</u>	
A	A	В	0	Ξ.	Е	F	G	н	1	J	K.	г	M	N	0	Ρ	Q	ĸ	S	1	0	V	W	Λ.	Y	Z
В	В	С	D	Ε	F	G	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α
С	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В
D	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С
Е	Е	F	G	Η	Ι	J	K	L	-	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D
${ extstyle P_{ extbf{G}}^{ extbf{F}}}$	F	G	Η	Ι	J	K	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
G	G	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
Н	Η	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н
J	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι
\mathbf{K}	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J
\mathbf{L}	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ
\mathbf{M}	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L
Ν	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М
o	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	К	L	М	Ν
Р	Р	Q	R	S	Т	U	v	w	х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О
Q	Q	R	S	Т	U	v	w	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	М	Ν	О	Р
R	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	Ν	О	Р	Q
S	S	Т	U	v	w	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	Μ	Ν	О	P	Q	R
т	T	U	v	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	М	N	0	Р	Q	R	S
\mathbf{U}	U	v	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	Κ	L	М	N	О	P	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	A	В	С	D	Е	F	G	Н	Ι	J	K	L	М	N	0	P	Q	R	S	Т	U
w	w	X	Y	Z	A	В	C	D	Е	F	G	Н	I	J	K	-	М	N	0	Р	Q	R	S	Т	U	v
x	X	Y	Z	A	В	C	D	E	F	G	Н	I	J	K	L	М	N	0	Р	Q	R	S	Т	U	v	W
Y	Y	Z	Δ	В	С	D	E	F	G	Н	I	J	K	T.	М	N	0	Р	Q	R	S	Т	U	v	W	X
Z	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	М	N	0	Р	Q	R	S	Т	U	V	W	X	Y
L	L	А	ь		ъ	Е	г	G	11	1	J	I	ш	IVI	14	\Box	1	ų.	п	S	1		v	**	Λ	

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

	A	В	\mathbf{c}	D	Е	F	\mathbf{G}	н	Ι	J	K	\mathbf{L}	М	Ν	О	Р	Q	\mathbf{R}	\mathbf{s}	Т	U	\mathbf{V}	W	\mathbf{X}	\mathbf{Y}	\mathbf{z}
${\bf A}$	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	$_{\rm L}$	М	Ν	О	Р	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z
В	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
\mathbf{c}	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В
\mathbf{D}	D	Е	F	\mathbf{G}	Н	Ι	J	K	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	$^{\rm C}$
\mathbf{E}	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D
$\mathbf{p}^{\mathbf{F}}$	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
\mathbf{G}	G	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
н	Η	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G
Ι	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η
J	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι
\mathbf{K}	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Χ	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J
\mathbf{L}	$_{\rm L}$	Μ	Ν	О	Ρ	Q	${\bf R}$	S	Т	U	V	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ
\mathbf{M}	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L
\mathbf{N}	Ν	О	Ρ	Q	\mathbf{R}	S	Т	U	V	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М
О	О	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	М	Ν
\mathbf{P}	Р	Q	R	S	Т	U	V	W	Χ	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	О
\mathbf{Q}	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	О	Ρ
${\bf R}$	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Р	Q
\mathbf{s}	S	Т	U	V	W	Х	Y	\mathbf{Z}	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ	$_{\rm L}$	Μ	Ν	О	Р	Q	\mathbf{R}
\mathbf{T}	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	М	Ν	О	Р	Q	R	S
U	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т
\mathbf{v}	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U
\mathbf{w}	W	Х	Y	Z	Α	В	$^{\rm C}$	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	O	Р	Q	R	S	Т	U	V
\mathbf{x}	Χ	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Τ	U	V	W
\mathbf{Y}	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х
\mathbf{z}	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y

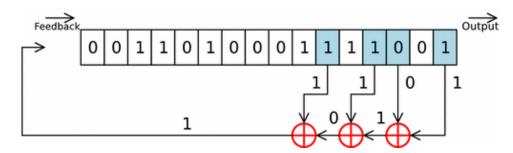
- Clé secrète
 PARISDIDEROT
- Message reçu
 HADMVLDLRXHLXXGIJWQHP
- Message original
 - \blacksquare P,H \Rightarrow S
 - lacksquare A, A \Rightarrow A
 - \blacksquare R, D \Rightarrow M
 - \blacksquare I,M \Rightarrow E
 - **-** ...

SAMEDIVINGTSIXPARTIELS

A A B B C C	7	B C D	D	D E	Е	F	G	TT	1																	
c	7	\rightarrow	_	\mathbf{E}			9	н	1	J	Κ	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	X	Y	\mathbf{z}
\vdash)	\rightarrow	-	123	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α
ᆔ	+	_	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В
~ ~	. 1	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С
ΕE	91	F	G	Н	Ι	J	K	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D
FF	7	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е
G	;	Н	Ι	J	K	L	Μ	Ν	О	Ρ	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F
ΗН	ī	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G
ΙŪ	1	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н
JŪ	ī	Κ	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	\mathbf{z}	Α	В	С	D	Е	F	G	Н	Ι
KK	ी	L	М	Ν	О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J
гĮ	,	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ
мΝ	1	Ν	О	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L
NN	1	0	Р	Q	\mathbf{R}	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М
olo	र्ग	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν
PΕ	7	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О
Q	īΤ	R	S	Т	U	V	w	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	М	Ν	О	Р
RR	-	S	Т	U	V	w	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q
$\mathbf{s} \mid \mathbf{s}$;	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R
тП	1	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S
υŪ	Ţ	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т
$\mathbf{v} _{\overline{\mathbf{v}}}$	7	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Р	Q	R	S	Т	U
$w _{\overline{w}}$	V	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	О	Ρ	Q	R	S	Т	U	V
$\mathbf{x} \mathbf{x}$	7	Υ	Z	Α	В	С	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	О	Ρ	Q	R	S	Т	U	V	W
$Y \overline{Y}$	-	Z	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х
-	-	$\overline{}$	В	-	-	Е	-	G	Н	_	J	Κ	-	Μ	-	0	Р	Q	R	S	Т	U	V	W	Х	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 »

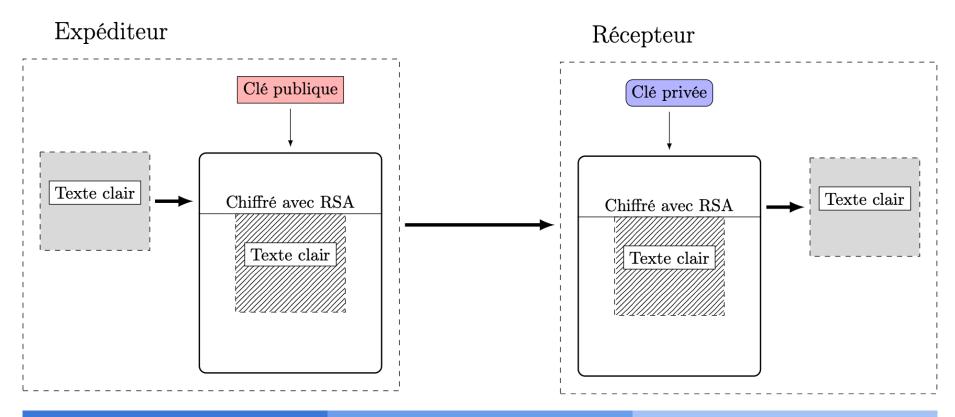
- Aujourd'hui on utilise des systèmes plus solides
 - Symétriques ou à clé secrète
 - Par bloc (par exemple le DES) ou par flot
- Les plus standards ne sont pas considérés comme très solides
 - Le DES peut être cassé en quelques jours/heures avec quelques dizaines d'ordinateurs
 - Mais c'est utile tout 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

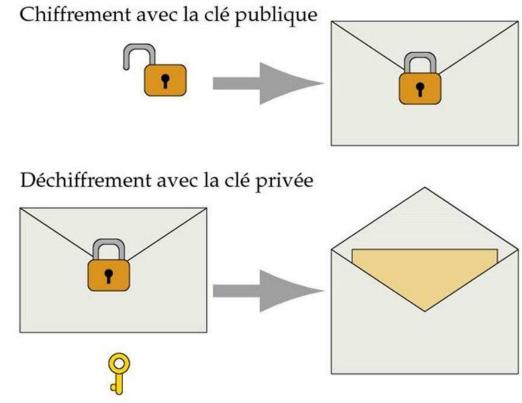
- Aujourd'hui on utilise des systèmes plus solides que les chiffrement par flot pour les échanges très secrets
 - Asymétriques ou à clés publiques
- Comment ça marche?
 - Deux clés : publique pour coder et privée pour decoder

- 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 ?

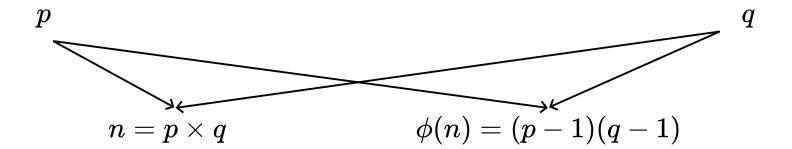
- Qui sont les clés publiques et privées ?
 - Dans le monde physique, nous pourrions utiliser des cadenas et des clés

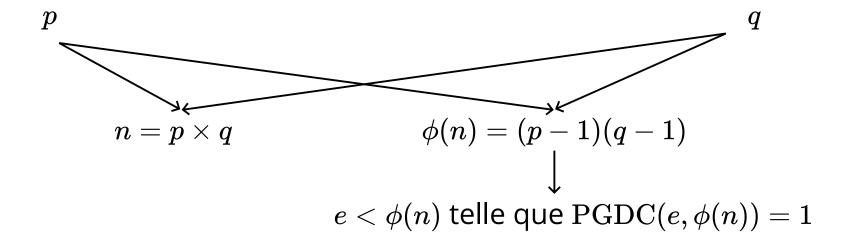


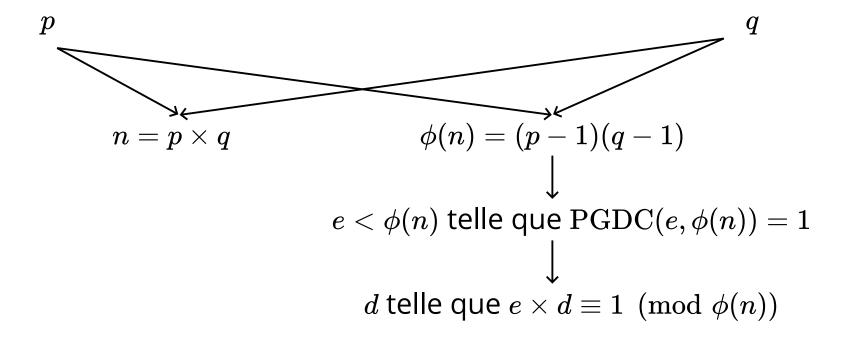
- Qui sont les clés publiques et privées ?
 - Dans le monde physique, nous pourrions utiliser des cadenas et des clés
 - Dans le monde numérique, nous utilisons les mathématique

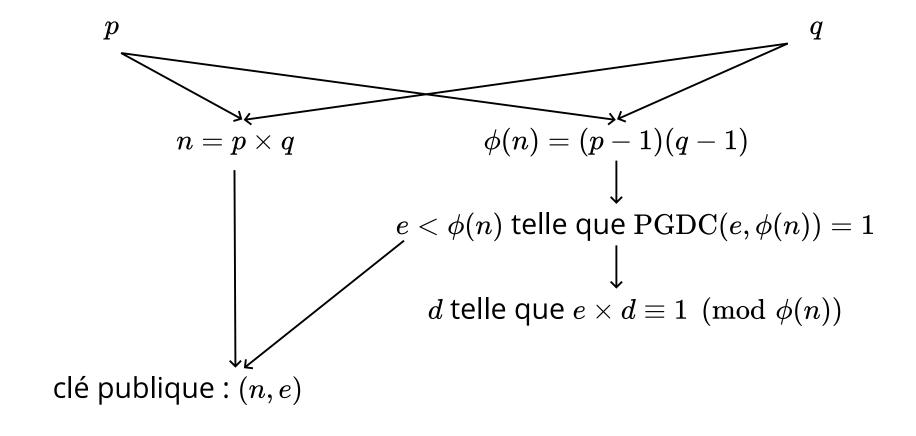
p

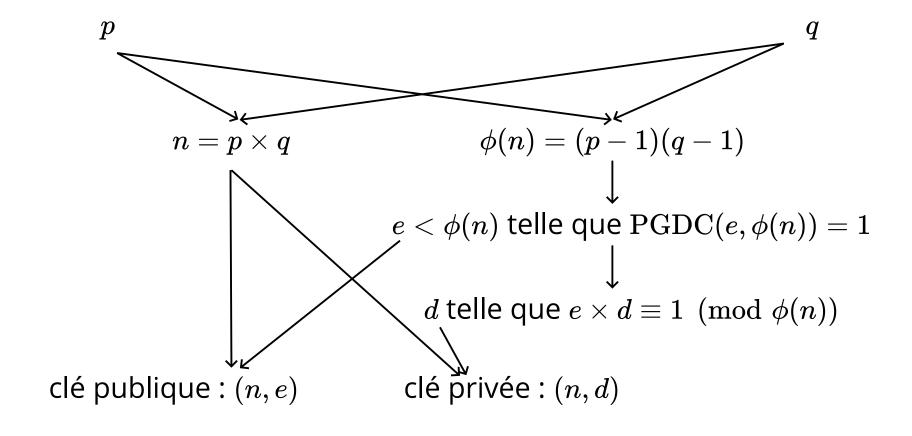
 \boldsymbol{q}

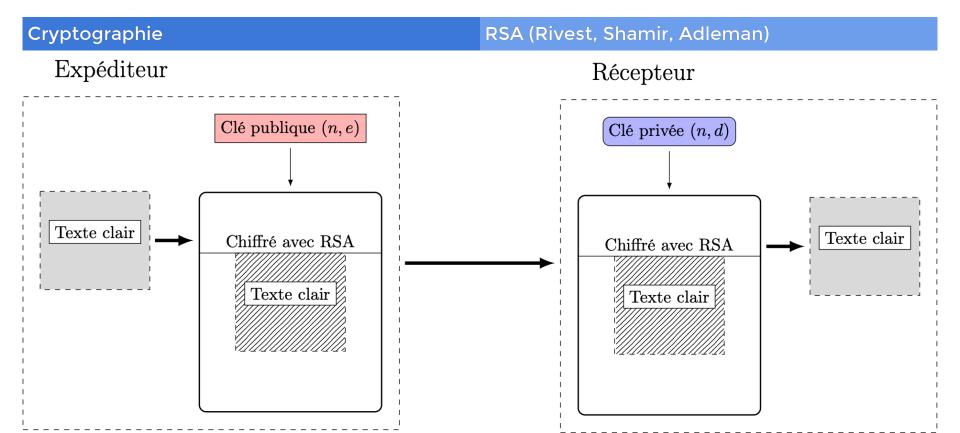












- Pour chiffrer le message M (entier strictement inférieur à n)
 - lacksquare On calcule $C \equiv M^e \pmod n$
- Pour déchiffrer C
 - On calcule $M \equiv C^d \pmod{n}$

- 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
 - \bullet $d = 43:7 \times 43 = 301 = 5 \times 60 + 1$
 - Clé publique (77, 7), clé privée (77, 43)
 - Message:B
 - o En ASCII: 42
 - \circ Valeur décimale : 42 < 77
 - \circ 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 : $42^7 \pmod{77}$
 - $-42^1 \pmod{77} = 42$
 - $\blacksquare \ 42 \times 42 \ (\bmod \ 77) = 1764 \ (\bmod \ 77) = 70$

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

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

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

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

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

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