

# Cryptologie

# Introduction

# Cryptologie

# Cryptologie

**Cryptographie**

*science autour des  
méthodologies et des  
outils de chiffrement*

# Cryptologie

**Cryptographie**

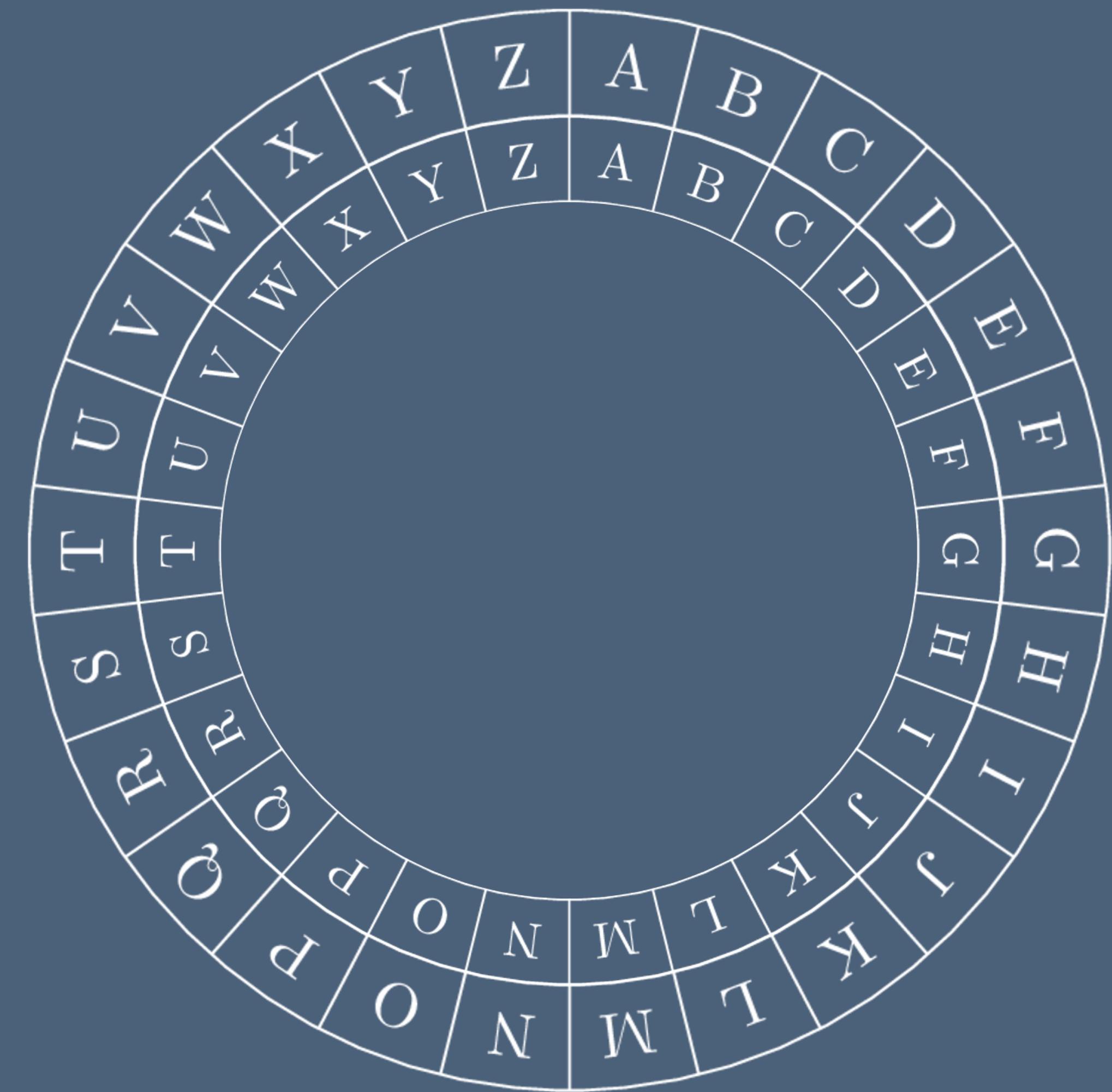
*science autour des  
méthodologies et des  
outils de chiffrement*

**Cryptanalyse**

*science analysant les  
cryptogrammes en  
vue de les déchiffrer*

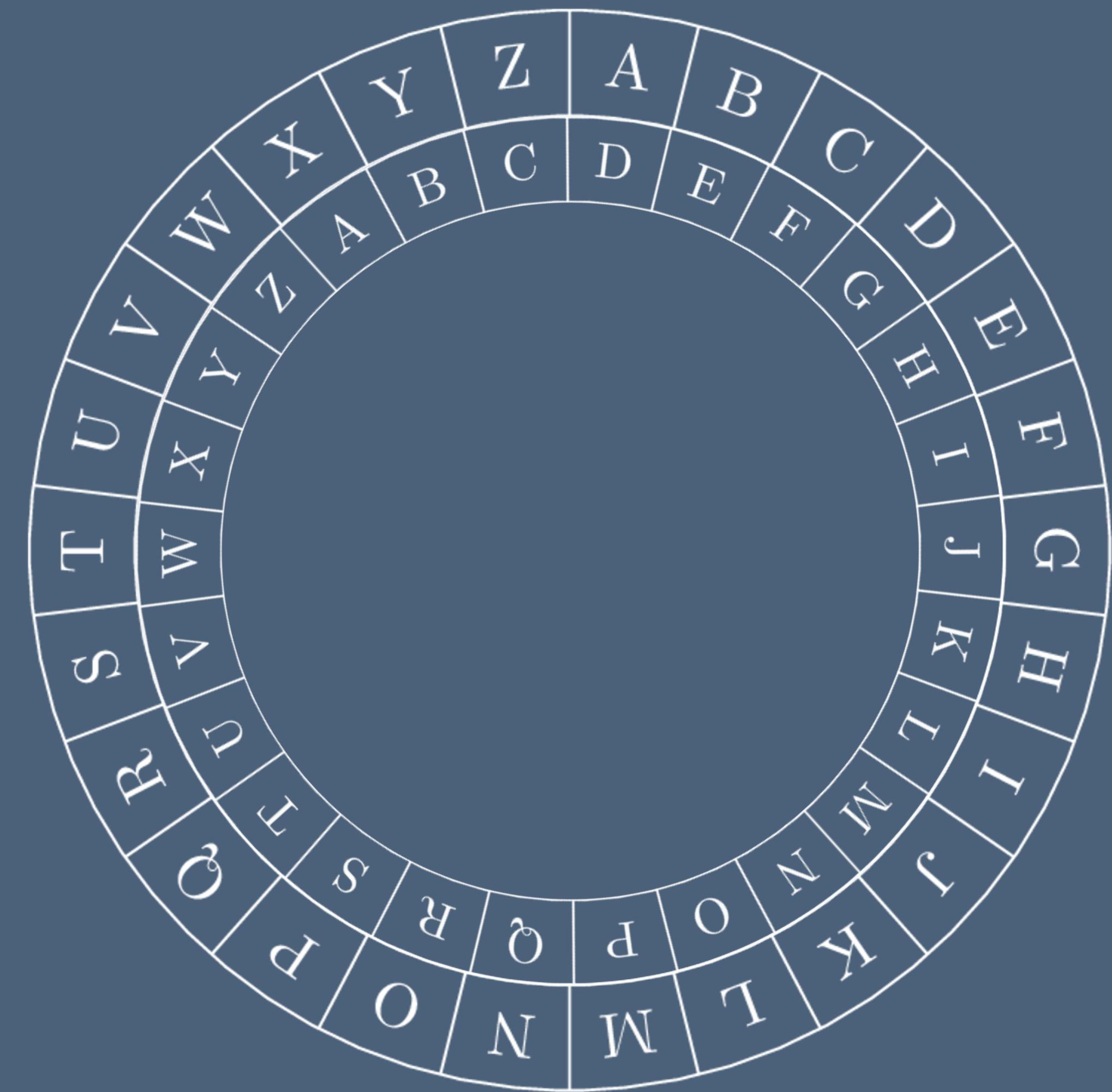
# *Historique*

Chiffrement de César (50 av. J.-C.)



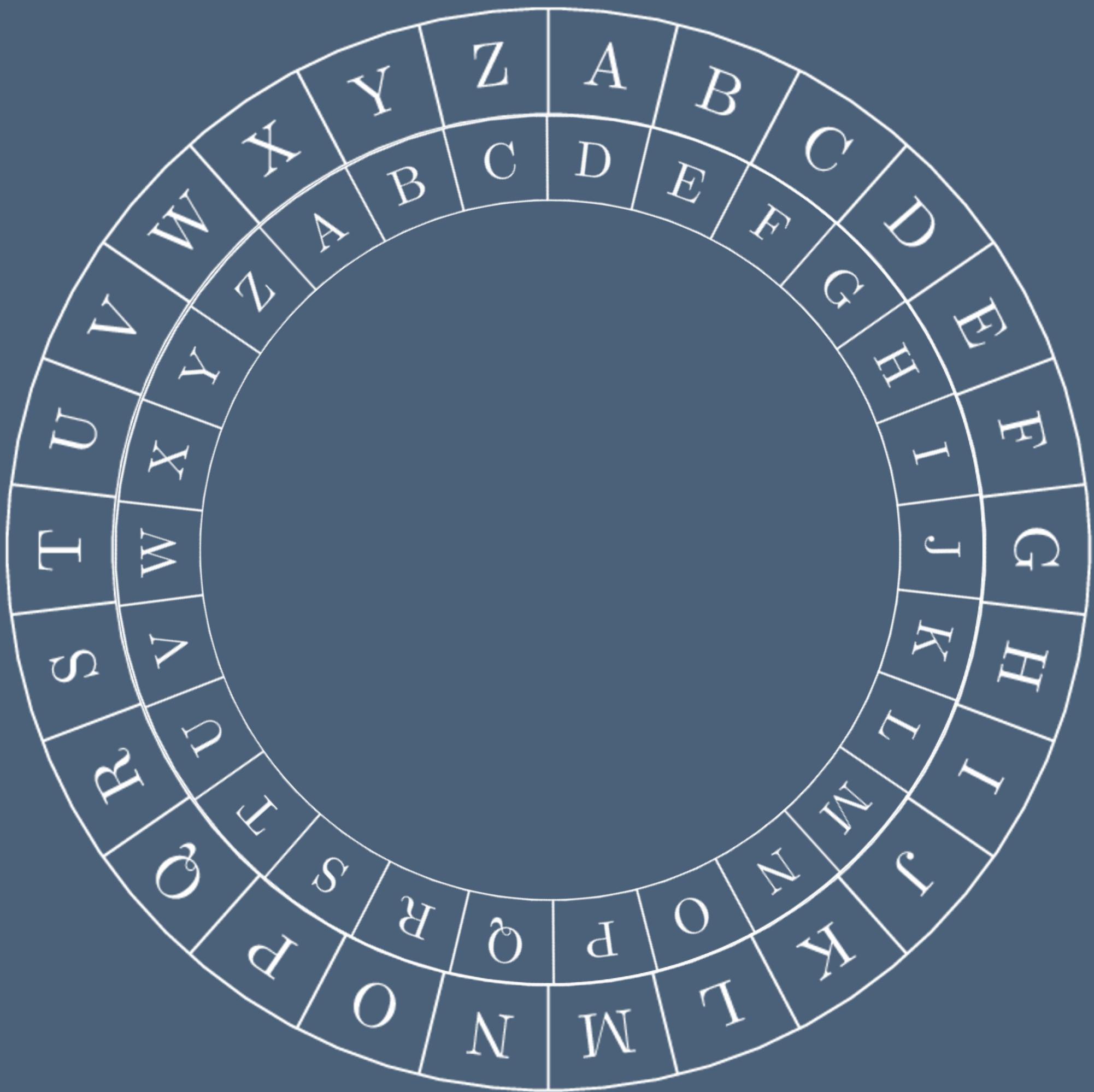
# *Historique*

Chiffrement de César (50 av. J.-C.)



# *Historique*

Chiffrement de César (50 av. J.-C.)

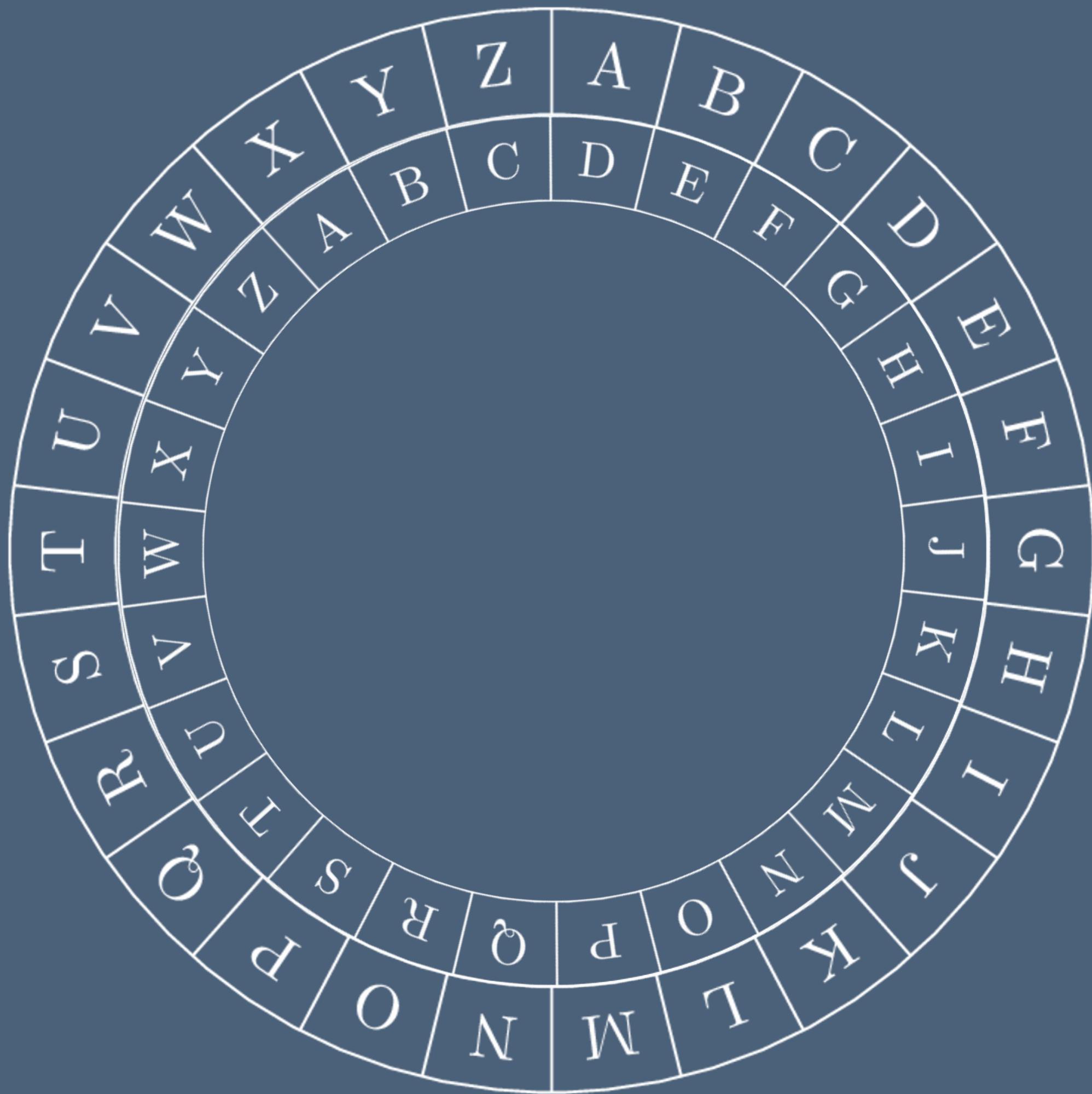


**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

# *Historique*

Chiffrement de César (50 av. J.-C.)



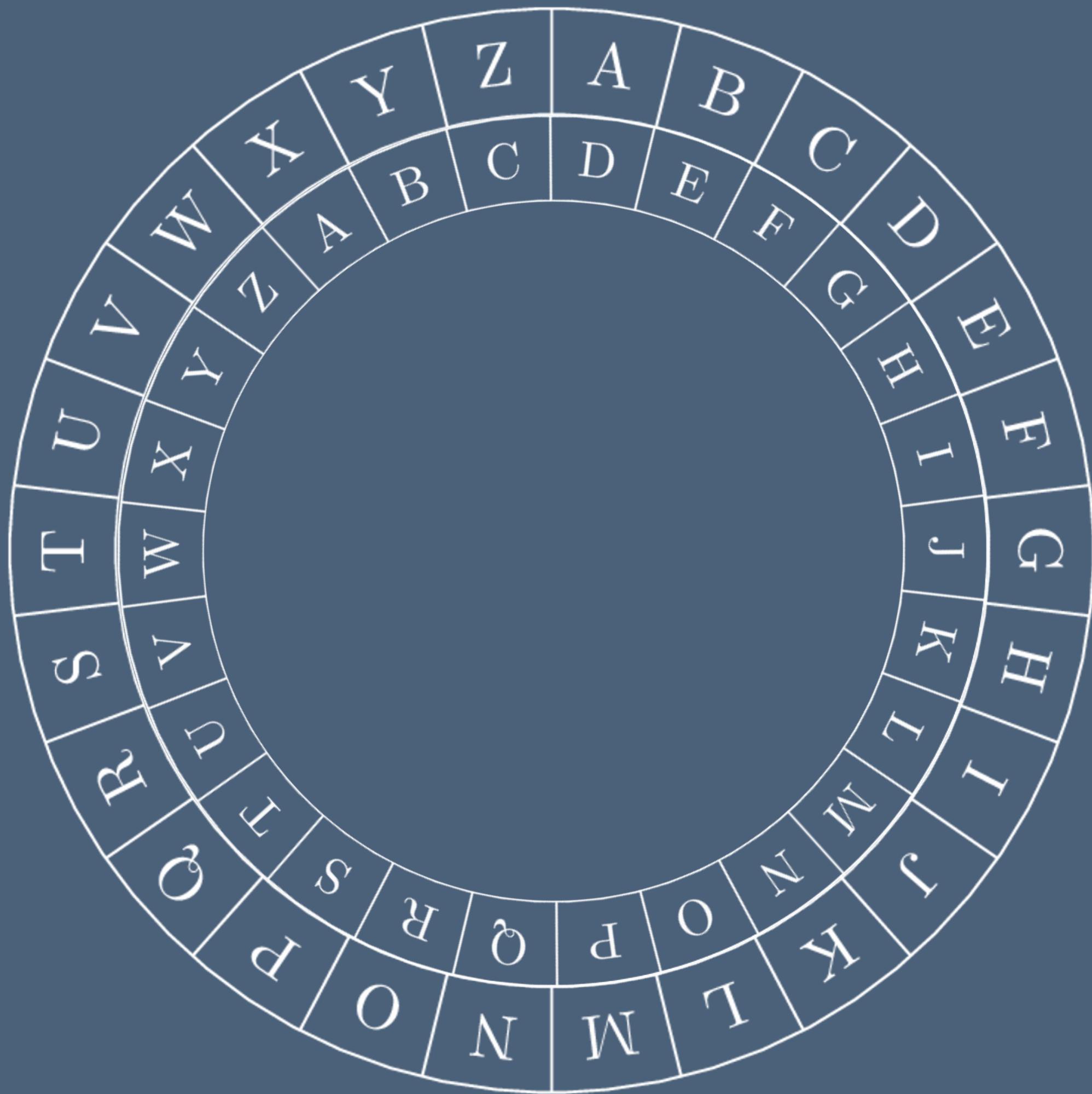
**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**s**

# *Historique*

Chiffrement de César (50 av. J.-C.)



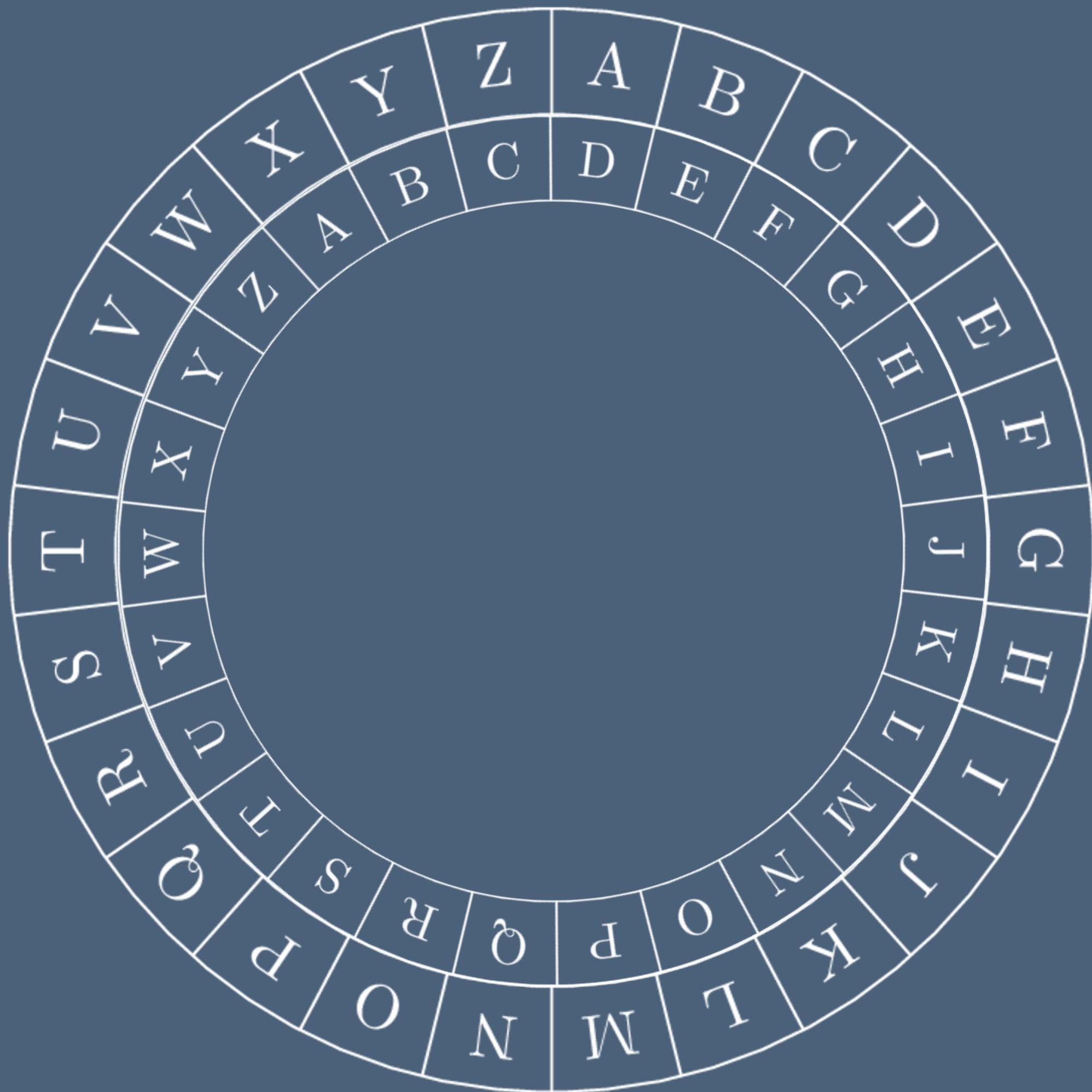
**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**SU**

# *Historique*

Chiffrement de César (50 av. J.-C.)



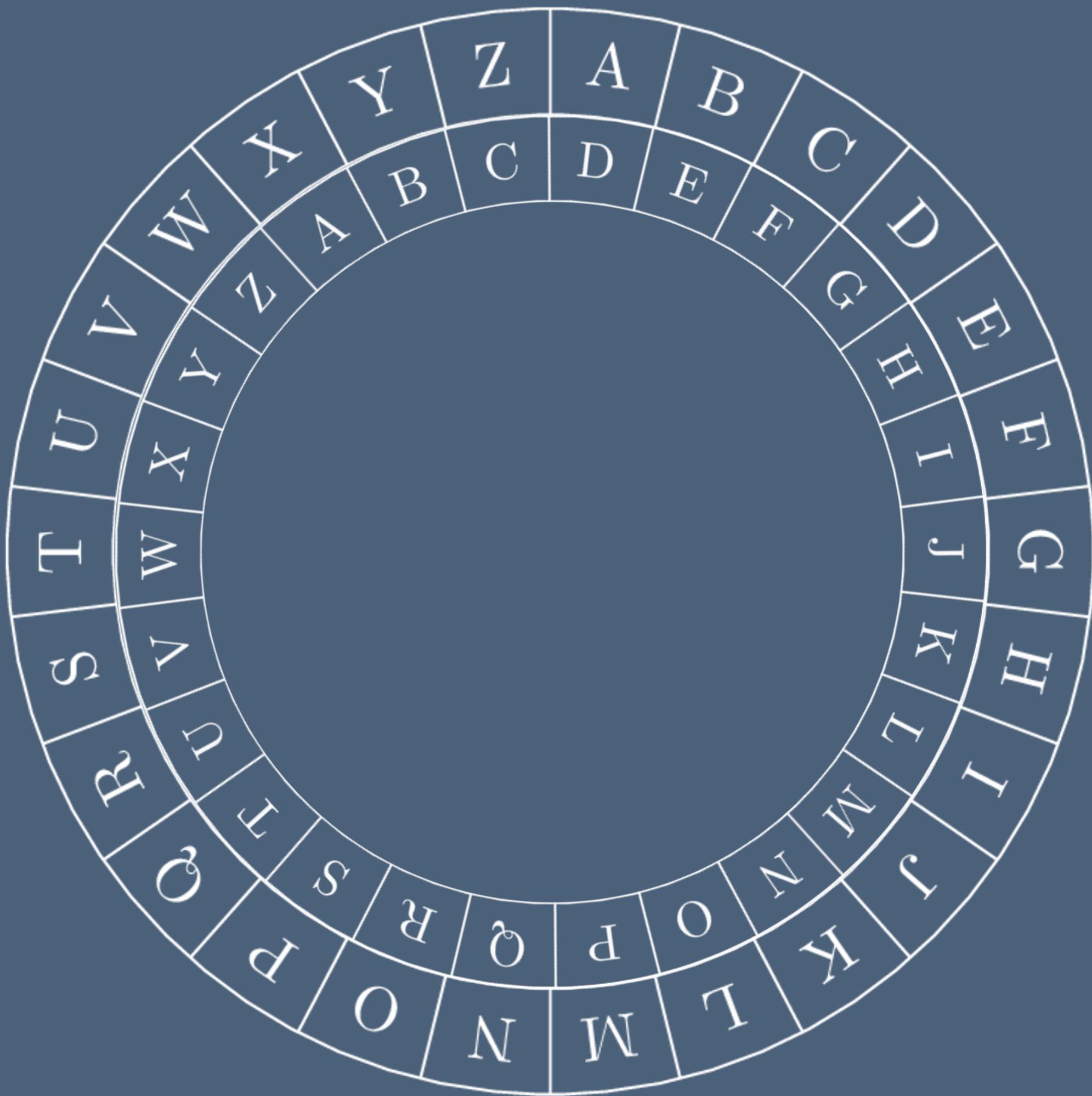
**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**SUH**

# *Historique*

Chiffrement de César (50 av. J.-C.)



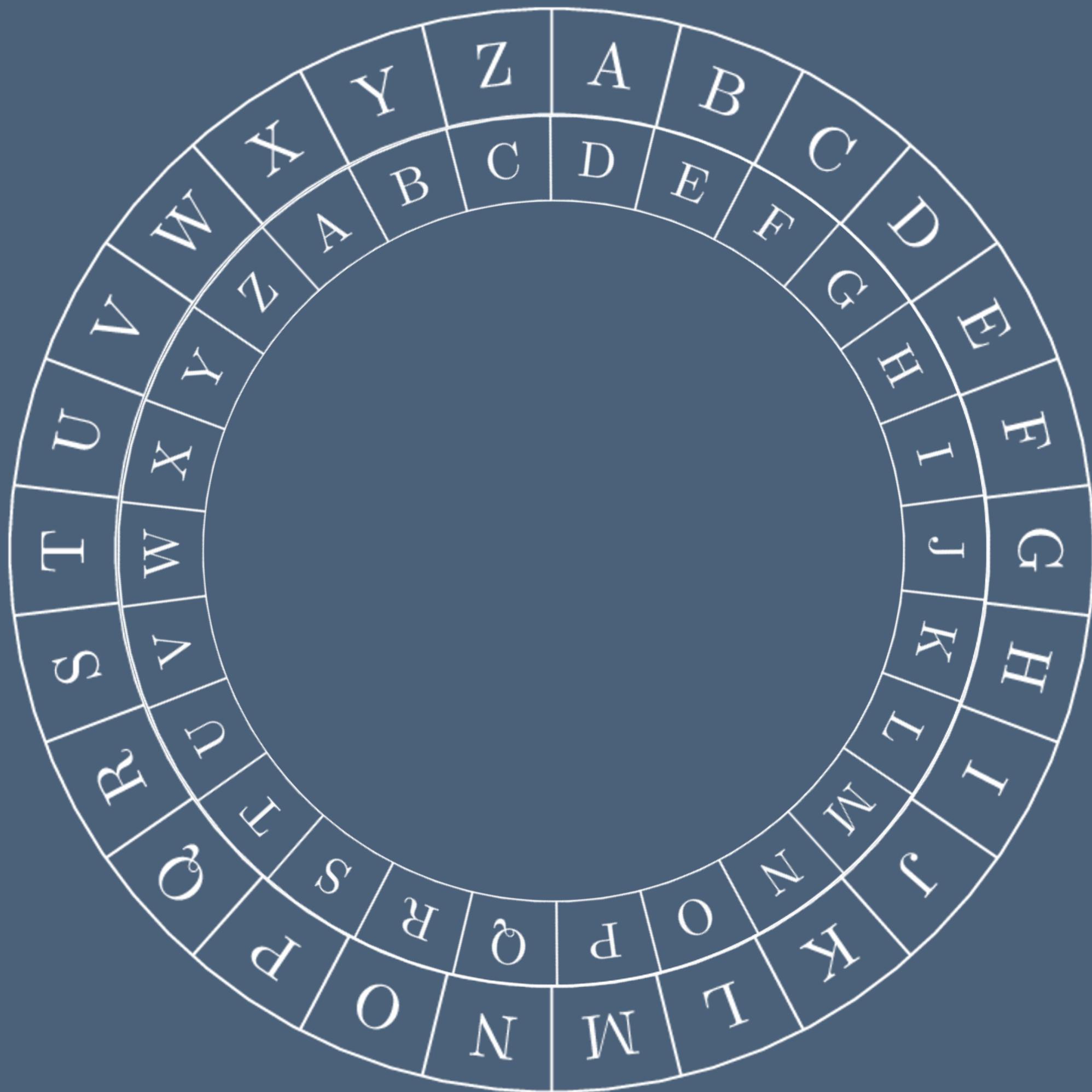
**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**SUHQ**

# *Historique*

Chiffrement de César (50 av. J.-C.)



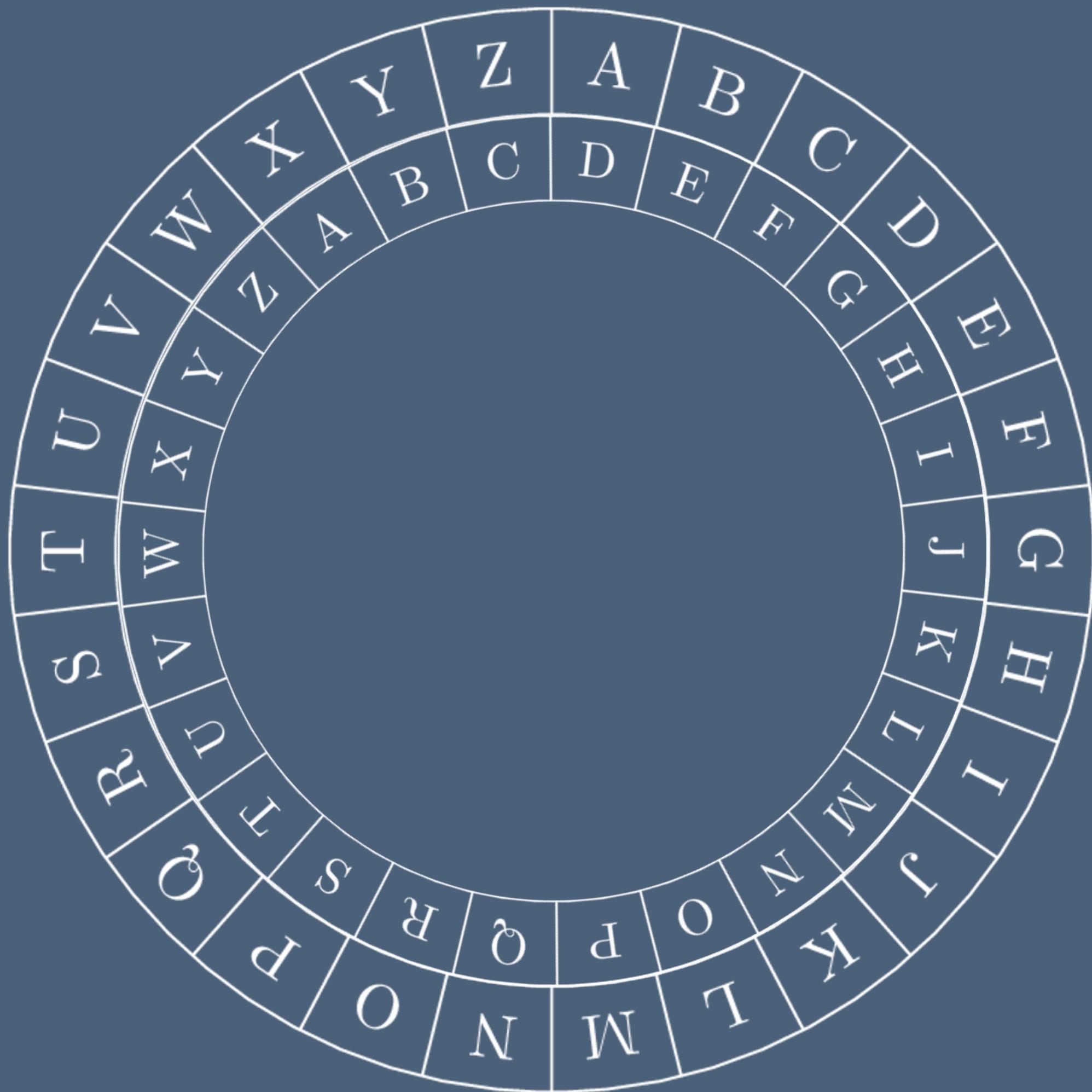
**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**SUHQG**

# *Historique*

Chiffrement de César (50 av. J.-C.)



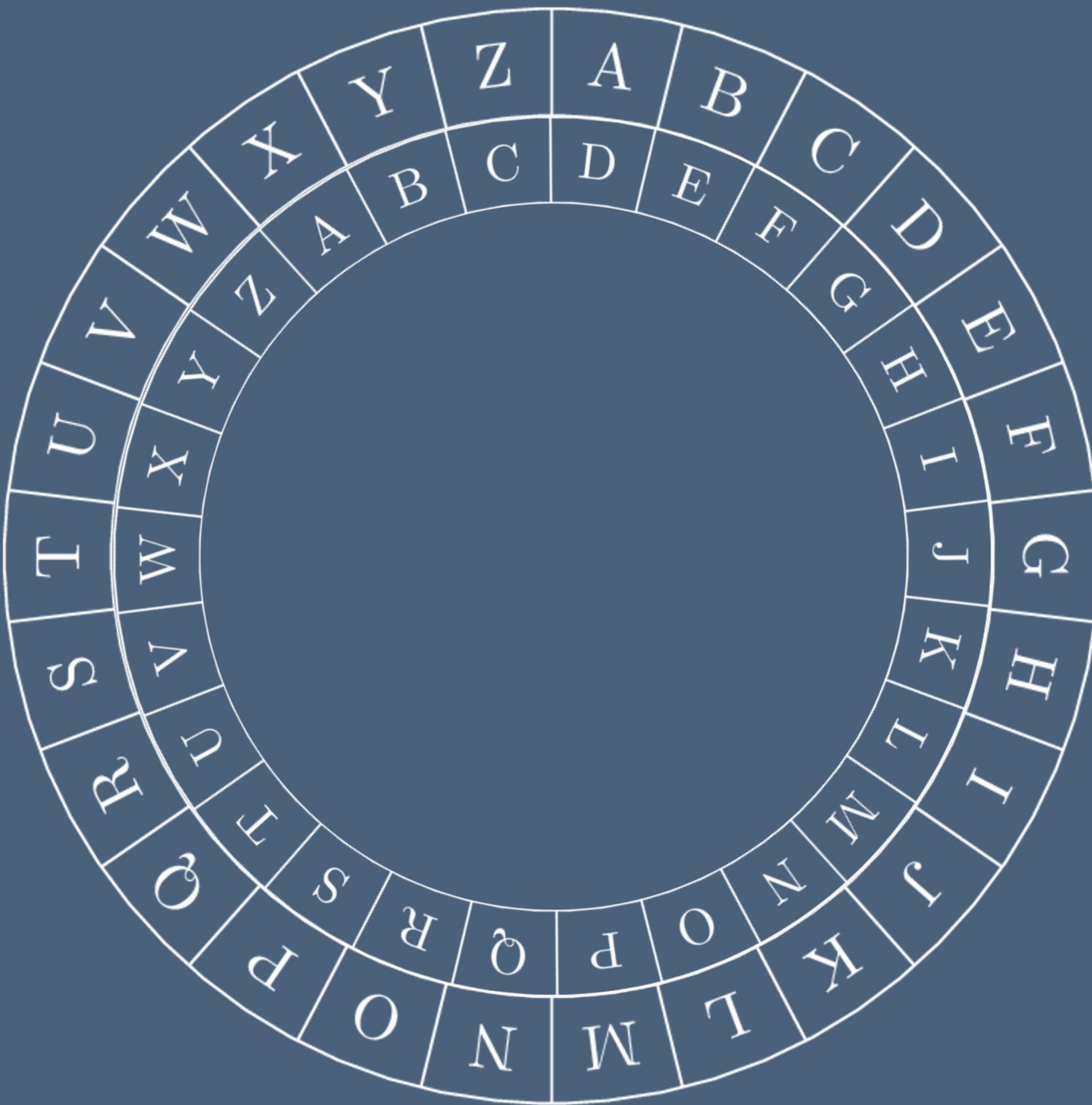
**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**SUHQGV**

# *Historique*

Chiffrement de César (50 av. J.-C.)



**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**SUHQGV JDUGH DXA LGHV GH PDUV**

# *Historique*

Chiffrement de César (50 av. J.-C.)



**PRENDS GARDE AUX IDES DE MARS**

est chiffré par

**SUHQGV JDUGH DXA LGHV GH PDUV**

# *Historique*

## Chiffrement par décalage



26 clés possibles

Sécurité basée (à l'époque) sur la  
méconnaissance de l'alphabet grec et  
l'illettrisme

Sécurité nulle de nos jours (brute force)

# *Historique*

## Chiffrement par décalage



26 clés possibles

Sécurité basée (à l'époque) sur la  
méconnaissance de l'alphabet grec et  
l'illettrisme

Sécurité nulle de nos jours (brute force)

# *Historique*

## Chiffrement par décalage



26 clés possibles

Sécurité basée (à l'époque) sur la  
méconnaissance de l'alphabet grec et  
l'illettrisme

Sécurité nulle de nos jours (brute force)

# *Historique - Chiffrement par substitution*

Chiffrement **mono**alphabétique - Cryptographie

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- A chaque élément de l'alphabet de départ est associé un élément de l'alphabet de destination

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- A chaque élément de l'alphabet de départ est associé un élément de l'alphabet de destination
- Nombre de clés : 26 possibilités de permutation pour A, 25 possibilités de permutation pour B, ..., 2 possibilités de permutation pour Y, 1 possibilité de permutation pour Z.

$26 \times 25 \times 24 \times \dots \times 2 \times 1 = 26! = 403291461126605635584000000$  clés possibles.

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- A chaque élément de l'alphabet de départ est associé un élément de l'alphabet de destination
- Nombre de clés : 26 possibilités de permutation pour A, 25 possibilités de permutation pour B, ..., 2 possibilités de permutation pour Y, 1 possibilité de permutation pour Z.

$$26 \times 25 \times 24 \times \dots \times 2 \times 1 = 26! = 403291461126605635584000000 \text{ clés possibles.}$$

- Ces deux alphabets peuvent être identiques:

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- A chaque élément de l'alphabet de départ est associé un élément de l'alphabet de destination
- Nombre de clés : 26 possibilités de permutation pour A, 25 possibilités de permutation pour B, ..., 2 possibilités de permutation pour Y, 1 possibilité de permutation pour Z.

$26 \times 25 \times 24 \times \dots \times 2 \times 1 = 26! = 403291461126605635584000000$  clés possibles.

- Ces deux alphabets peuvent être identiques:

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- A chaque élément de l'alphabet de départ est associé un élément de l'alphabet de destination
- Nombre de clés : 26 possibilités de permutation pour A, 25 possibilités de permutation pour B, ..., 2 possibilités de permutation pour Y, 1 possibilité de permutation pour Z.

$26 \times 25 \times 24 \times \dots \times 2 \times 1 = 26! = 403291461126605635584000000$  clés possibles.

- Ces deux alphabets peuvent être identiques:

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

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

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- Ou bien ce peut être deux alphabets différents (exemple : chiffre des francs-maçons) :

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- Ou bien ce peut être deux alphabets différents (exemple : chiffre des francs-maçons) :

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	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

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptographie

- Ou bien ce peut être deux alphabets différents (exemple : chiffre des francs-maçons) :

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	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R

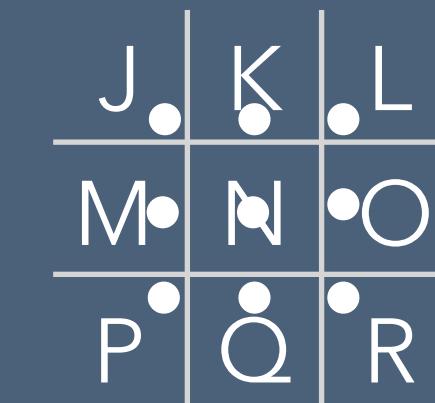
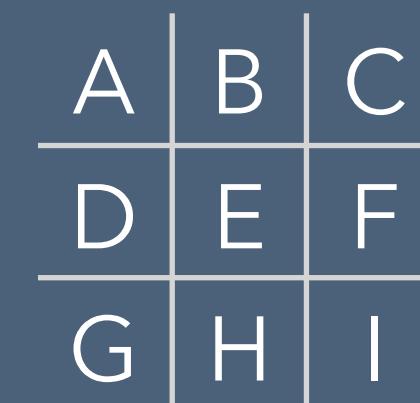
S  
T  
U  
V

W  
X  
Y  
Z

J U L C O C T T P

# *Historique - Chiffrement par substitution*

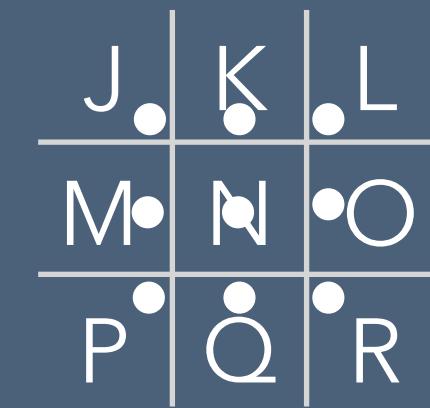
# Chiffrement monoalphabétique - Cryptographie



# Historique - Chiffrement par substitution

# Chiffrement monoalphabétique - Cryptographie

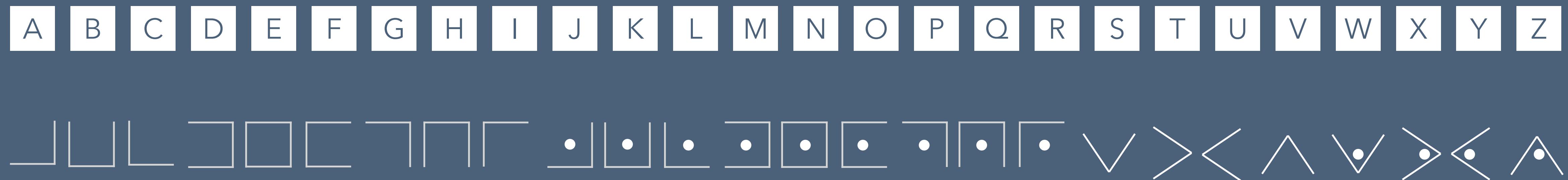
- Ou bien ce peut être deux alphabets différents (exemple : chiffre des francs-maçons) :



A diagram on a blue background featuring four white points arranged in a cross. The top point is labeled 'W' above it. The bottom point is labeled 'Z' below it. The left point is labeled 'X' to its left. The right point is labeled 'Y' to its right. Two thick white lines extend from the center through each of the four points.

# *Historique - Chiffrement par substitution*

# Chiffrement monoalphabétique - Cryptographie



Gamla- åfwen kallad Tyska stilen.

Er 336 376 Ky 37 K L M N D J Y K 57

U Z Z Y Z E E O

Er ub q d n p y f i j x l m n o y y r y g s t u w w y y j z i v o

## Rumorna eller Rumstafven

3<sup>o</sup> vilken Oden, Sigge den 1<sup>te</sup> Fridulfsson införde här i norrden  
med den hedniska tidervarfroet. Skilen ägde i begynnelsen endast  
16 figurer, som utgjorde 20 bokstäfver, hvilka ej gick i alfabet-  
isk ordning. Av ursprunget till den skriften och av detta

ΨΝΑΡΞΙΡΥΡ\*ΤΙΧΤΛΤΒΒΓΨΗΦ \*

F U Y D O R K G H N Y A E S T B P L M W Ed. M.W.  
Men sedan tiden blev mera känd uppkom ett fullständigt alfabet,

som af okänd orsak förändras till följande utseende.

A B C D E F G H Y K L M N O P Z R S T U Y X Y Z Ä Å Ö  
Sist af dessa sortes bokstäfver införes Lönstilen, som säges vara

den fästa i Verlden och var skrifven på lagens Tafflor

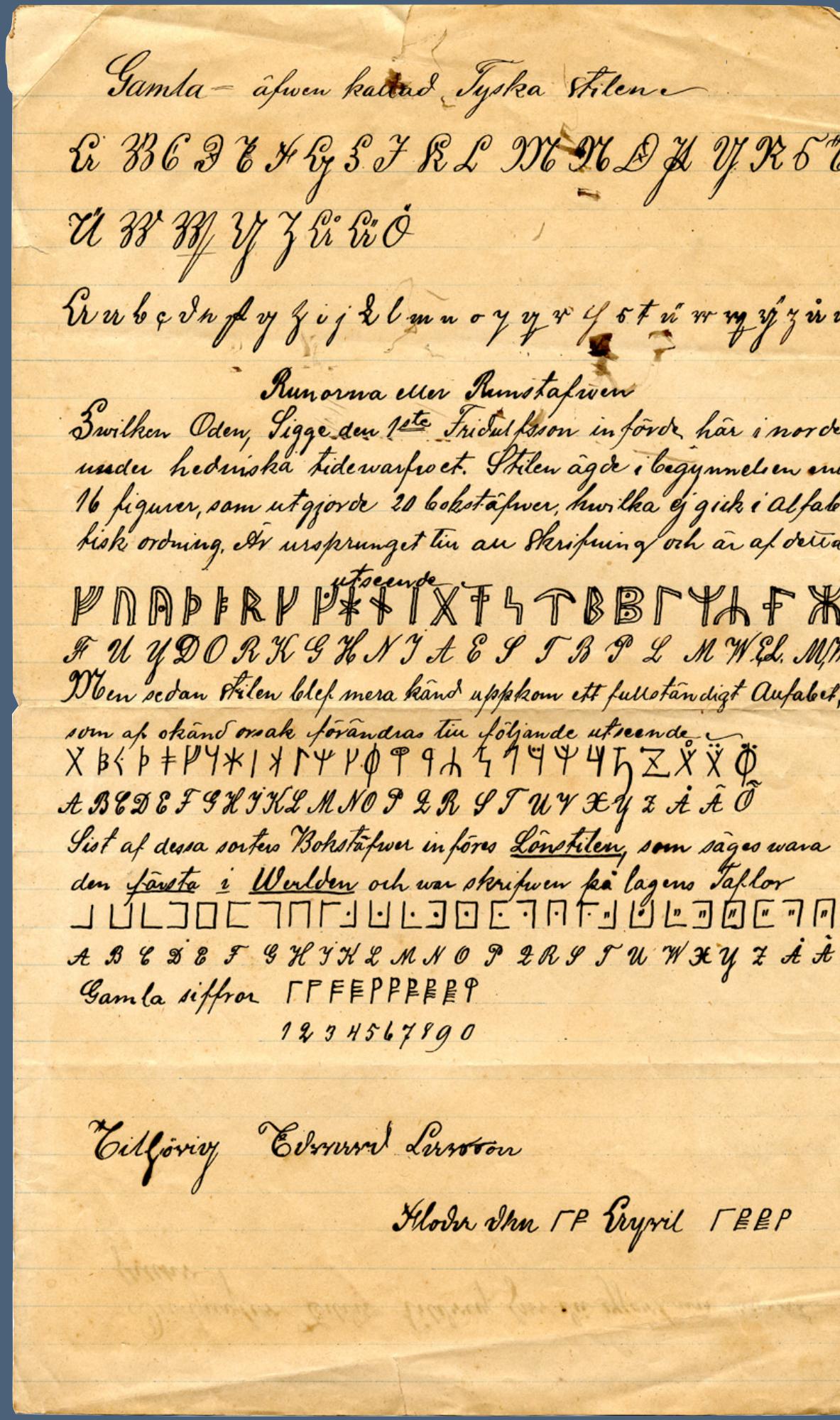
A B C D E F G H Y K L M N O P Q R S T U W X Y Z Å Ä Ö  
Gamla sifferor ΓΡΦΕΠΡΡΡΡΡΦ

1234567890

Tilförsel till världen

Hlover John RP Eryvill RP RP

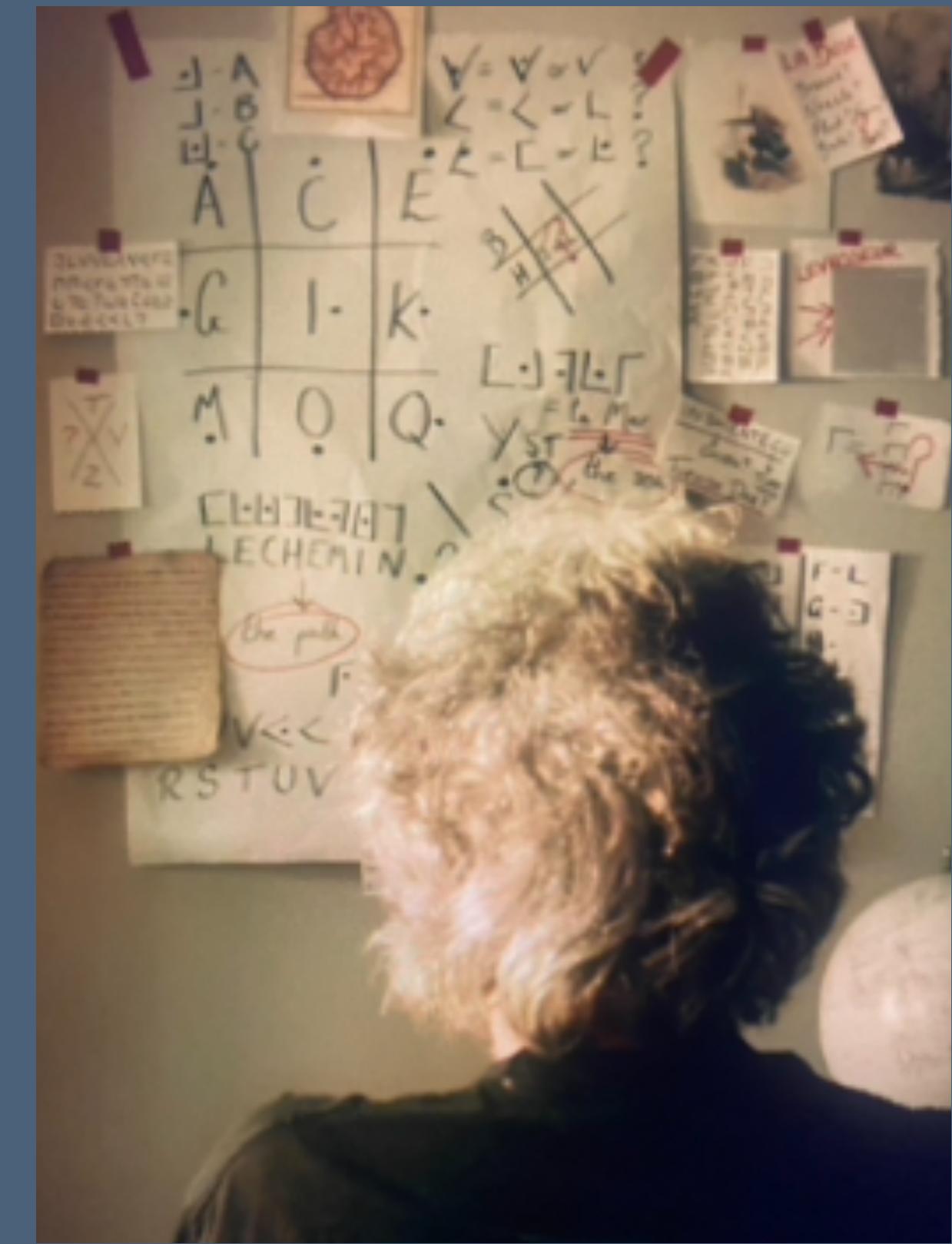
# Lettre datée de 1885 contenant une liste de glyphes dont fait partie le chiffre des francs-maçons



Lettre datée de 1885 contenant une liste de glyphes dont fait partie le chiffre des francs-maçons

F P F E D F L A C T E U P G U E U N B O A T V O G U E V  
 Z U R L E G T G V F E V E L O V L E V E A C E F L A T L E A G V  
 L O C V V B L A B C A L V A M C O T E A D T H E C C B E F  
 U L T B E C C E L L A C V G U L A P U L A V E L A T B V E  
 A F E L R E T A V A L V A T L A P U L A V E L A T B V E  
 T E V V E A V G E E P U N V B E U C P U L G V A V V B V E  
 C A S S E L A P E L C A P U G A T E A S C E V H A V A C E  
 L T B T B C L J A V F A L V V V A B A F A B V A B U P C E L  
 P A C G T P U N E A L G A T L L L E T T E U C E U V A C E  
 F A I C R A V V A T G E F U A J A J A H E J A V U M A G C E .  
 T E F F E V N P A G E P A T E C E P C E C E O C C E V G C A F  
 E B C O T R A G C J B G E P B V E L G A T H A B E R V A P F C E  
 C E L T E J U L E S E G U N D A L T V I H O L L V A E T T E  
 T C A C C E L F A B C L B A V E B A U L E 4 4 7 U L E 7 7 T F  
 B C L E V V E L J B G E U A G T C E V V A V U E V E X U K  
 U A L V U A C E B A A C F U A R G F B G L A R F F  
 E V V A U L C E E / P E L J A V T G E T U G E E U C F  
 4 4 7 U B O L L E G F E B O L L E L G V U E V C E V E

Le « Cryptogramme du forban », (à gauche) tel qu'il a été publié en 1934 dans *Le flibustier mystérieux, histoire d'un trésor caché*, aux éditions du Masque à Paris, fictivement déchiffré dans un épisode de  
*The Grand Tour*



*Historique - Chiffrement par substitution*

Chiffrement **mono**alphabétique - Cryptanalyse

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptanalyse

- Nombre de clés possibles :  $26! = 403291461126605635584000000 \approx 2^{88}$

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Cryptanalyse

- Nombre de clés possibles :  $26! = 403291461126605635584000000 \approx 2^{88}$
- Bruteforce : Au rythme d'**un milliard de clés testées par seconde**, il faudrait en moyenne **plus de 6 milliards d'années** pour trouver la bonne clé.

# *Historique - Chiffrement par substitution*

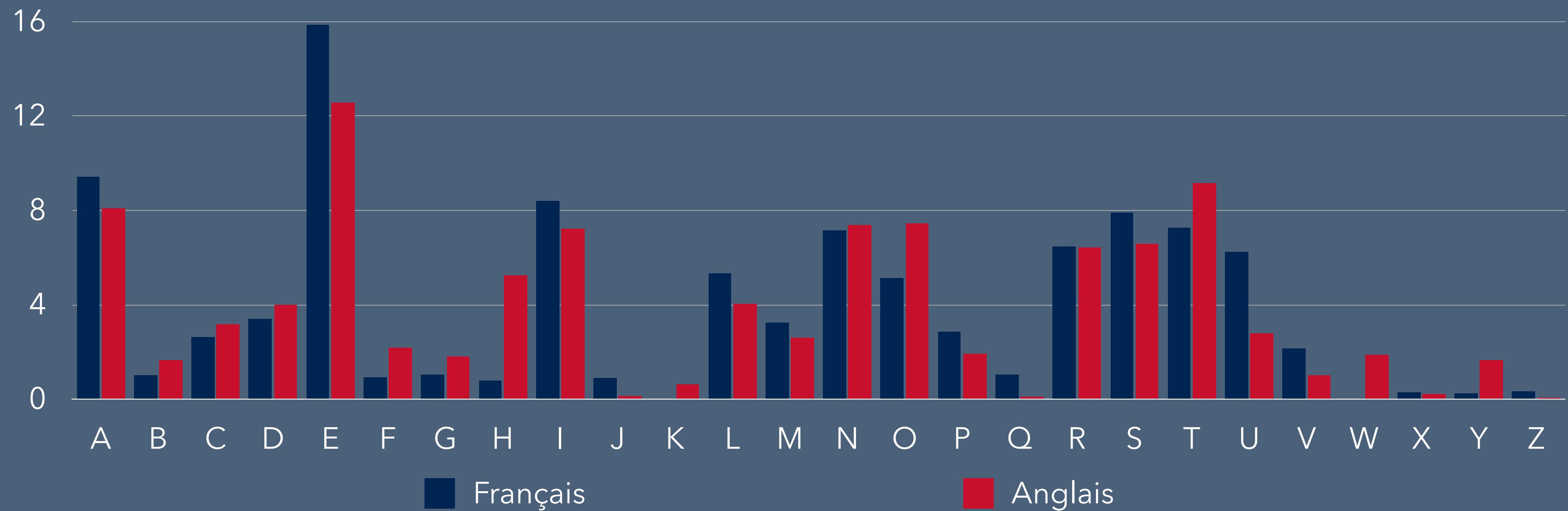
## Chiffrement **mono**alphabétique - Cryptanalyse

- Nombre de clés possibles :  $26! = 403291461126605635584000000 \approx 2^{88}$
  - Bruteforce : Au rythme d'**un milliard de clés testées par seconde**, il faudrait en moyenne **plus de 6 milliards d'années** pour trouver la bonne clé.
- ➔ Cryptanalyse par **analyse fréquentielle**

# *Historique - Chiffrement par substitution*

Chiffrement **mono**alphabétique - Analyse fréquentielle

Répartition de fréquence des lettres



# *Historique - Chiffrement par substitution*

Chiffrement **mono**alphabétique - Analyse fréquentielle - Exemple

Tgxo octzu, hgy mz dz skgyo qco ix'yj l cyn az pgddz gx az hcxtcyoz oynxcnygd. Hgy, oy mz aztcyo kzoxhzk hc tyz cxmgxka'wxy ctzs tgxo, mz aykcyo ixz s'zon a'cpgka azo kzdsgdnkzo. Azo vzdo ixy h'gdn nzdax jc hcyd, qzxn-znkz c xd hghzdn gx mz dz qgxtcyo qco, gx m'zncyo ozxj swzu hgy. Zn s'zon coozu sxkyzxe az oz aykz ixz jzo wcockao, jzo kzdsgdnkzo rgkvzdn xdz azonydzz... Qcksz ixz ixcda gd c jz vgxn az jc swgoz, ixcda gd c jz vgxn az jc swgoz pyzd rcynz, jz pzcx vzonz, qckrgyo gd dz nkgxtz qco j'ydndzkjgsxnzxk zd rcsz mz aykcyo, jz hykgyk ixy tgxo cyaz c ctcdszk. Cjgko sc d'zon qco hgd sco, sghhz mz ayocyo jc, qxyoixz hgy cx sgdnkcykz, m'cy qx ; zn mz ayo hzksy c jc tyz, mz jxy ayo hzksy, mz swcdnz jc tyz, mz acdoz jc tyz... mz dz oxyo ix'chgxr ! Zn rydcjzhzdn, ixcda azo vzdo hz ayozdn « Hcyo sghhzdn rcyo-nx qgxr ctgyk szñnz wxhcdynz ? », mz jzxk kzqgdao nkzo oyhqjzhzdn ixz s'zon sz vgxn az j'chgxr, sz vgxn agds ixy h'c qgxooz cxmgxka'wxy c zdnkzqkzdakz xdz sgdonkxsnygd hzscdyixz... hcyo azhcyd ixy ocyn ? Qzxn-znkz oyhqjzhzdn c hz hznnkz cx ozktysz az jc sghhxdcxz, c rcyrkz jz agd, jz agd az ogy.

# *Historique - Chiffrement par substitution*

Chiffrement **mono**alphabétique - Analyse fréquentielle - Exemple

Lettre	z	c	o	y	x	d	g	n	k	h	a	s
Fréquence	138	74	66	66	64	55	53	50	45	37	37	32
Pourcentage	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %

Lettre	j	q	t	m	i	w	v	r	p	u	l	e
Fréquence	27	17	16	16	15	8	8	7	4	3	1	1
Pourcentage	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %

Lettre	<b>z</b>	<b>c</b>	<b>o</b>	<b>y</b>	<b>x</b>	<b>d</b>	<b>g</b>	<b>n</b>	<b>k</b>	<b>h</b>	<b>a</b>	<b>s</b>
Fréquence	138	74	66	66	64	55	53	50	45	37	37	32
Pourcentage	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %

Lettre	<b>j</b>	<b>q</b>	<b>t</b>	<b>m</b>	<b>i</b>	<b>w</b>	<b>v</b>	<b>r</b>	<b>p</b>	<b>u</b>	<b>l</b>	<b>E</b>
Fréquence	27	17	16	16	15	8	8	7	4	3	1	1
Pourcentage	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %

tgxo octzu, hgy mz dz skgyo qco ix'yyj l cyn az pgddz gx az hcxtcyoz oynxcnygd. hgy, oy mz aztcyo kzoxhzk hc tyz cxmgxka'wxy ctzs tgxo, mz aykcyo ixz s'zon a'cpgka azo kzdsgdnkzo. azo vzdo ixy h'gdn nzdax jc hcyd, qzxn-znkz c xd hghdn gx mz dz qgxtcyo qco, gx m'zncyo ozxj swzu hgy. zn s'zon coozu sxkyzxe az oz aykz ixz jzo wcockao, jzo kzdsgdnkzo rgkvzdn xdz azonydzz... qcksz ixz ixcda gd c jz vgxn az jc swgoz, ixcda gd c jz vgxn az jc swgoz pyzd rcynz, jz pzcx vzonz, qckrgyo gd dz nkgxtz qco j'ydnzkjgsxnzxk zd rcsz mz aykcyo, jz hykgyk ixy tgxo cyaz c ctcdszk. c jgko sc d'zon qco hgd sco, sghhz mz ayocyo jc, qxyoixz hgy cx sgdnkcykz, m'cy qx ; zn mz ayo hzksy c jc tyz, mz jxy ayo hzksy, mz swcdnz jc tyz, mz acdoz jc tyz... mz dz oxyo ix'chgwk ! zn rydcjzhzdn, ixcda azo vzdo hz ayozdn « hcyo sghhzdn rcyo-nx qgwk ctgyk sznnz wxhcdynz ? », mz jzxk kzqgdao nkzo oyhqjzhzdn ixz s'zon sz vgxn az j'chgwk, sz vgxn agds ixy h'c qgxooz cxmgxka'wxy c zdnkzqkzdakz xdz sgdonkxsnygd hzscdyixz... hcyo azhcyd ixy ocyn ? qzxn-znkz oyhqjzhzdn c hz hznnkz cx ozktysz az jc sghhxdcxz, c rcykz jz agd, jz agd az ogy.

Lettre	<b>z</b>	<b>c</b>	<b>o</b>	<b>y</b>	<b>x</b>	<b>d</b>	<b>g</b>	<b>n</b>	<b>k</b>	<b>h</b>	<b>a</b>	<b>s</b>
<b>Fréquence</b>	138	74	66	66	64	55	53	50	45	37	37	32
<b>Pourcentage</b>	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
<b>Correspondance</b>	E											

Lettre	<b>j</b>	<b>q</b>	<b>t</b>	<b>m</b>	<b>i</b>	<b>w</b>	<b>v</b>	<b>r</b>	<b>p</b>	<b>u</b>	<b>l</b>	<b>E</b>
<b>Fréquence</b>	27	17	16	16	15	8	8	7	4	3	1	1
<b>Pourcentage</b>	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
<b>Correspondance</b>												

tgxo octEu, hgy mE dE skgyo qco ix'yj l cyn aE pgddE gx aE hcxtcyoE oynxcnygd. hgy, oy mE aEtcyo kEoxhEk hc tyE cxmgxka'wxy ctEs tgxo, mE aykcyo ixE s'Eon a'cpgka aEo kEdsgdnkEo. aEo vEdo ixy h'gdn nEdax jc hcyd, qExn-EnkE c xd hghEdn gx mE dE qgxtcyo qco, gx m'Encyo oExj swEu hgy. En s'Eon cooEu sxkyExe aE oE aykE ixE jEo wcockao, jEo kEdsgdnkEo rgkvEdn xdE aEonydEE... qcksE ixE ixcda gd c jE vgxn aE jc swgoE, ixcda gd c jE vgxn aE jc swgoE pyEd rcynE, jE pEcx vEonE, qckrgyo gd dE nkgxtE qco j'ydnEkjgsxnExk Ed rcsE mE aykcyo, jE hykgyk ixy tgxo cyaE c ctcdsEk. c jgko sc d'Eon qco hgd sco, sghhE mE ayocyo jc, qxyoixE hgy cx sgdnkcykE, m'cy qx ; En mE ayo hEksy c jc tyE, mE jxy ayo hEksy, mE swcdnE jc tyE, mE acdoE jc tyE... mE dE oxyo ix'chgwk ! En rydcjEhEdn, ixcda aEo vEdo hE ayoEdn « hcyo sghhEdn rcyo-nx qgwk ctgyk sEnnE wxhcdynE ? », mE jExk kEqgdao nkEo oyhqjEhEdn ixE s'Eon sE vgxn aE j'chgwk, sE vgxn agds ixy h'c qgxooE cxmgxka'wxy c EdnkEpkEdakE xdE sgdonkxsnygd hEscdyixE... hcyo aEhcyd ixy ocyn ? qExn-EnkE oyhqjEhEdn c hE hEnnKE cx oEktysE aE jc sghhxdcxnE, c rcykE jE agd, jE agd aE ogy.

Lettre	<b>z</b>	<b>c</b>	<b>o</b>	<b>y</b>	<b>x</b>	<b>d</b>	<b>g</b>	<b>n</b>	<b>k</b>	<b>h</b>	<b>a</b>	<b>s</b>
<b>Fréquence</b>	138	74	66	66	64	55	53	50	45	37	37	32
<b>Pourcentage</b>	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
<b>Correspondance</b>	E	A										

Lettre	<b>j</b>	<b>q</b>	<b>t</b>	<b>m</b>	<b>i</b>	<b>w</b>	<b>v</b>	<b>r</b>	<b>p</b>	<b>u</b>	<b>l</b>	<b>E</b>
<b>Fréquence</b>	27	17	16	16	15	8	8	7	4	3	1	1
<b>Pourcentage</b>	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
<b>Correspondance</b>												

tgxo oAtEu, hgy mE dE skgyo qAo ix'yj l Ayn aE pgddE gx aE hAxtAyoE oynxAnygd. hgy, oy mE aEtAyo kEoxhEk hA tyE Axmgxka'wxy AtEs tgxo, mE aykAyo ixE s'Eon a'Apgrka aEo kEdsgdnkEo. aEo vEdo ixy h'gdn nEdax jA hAyd, qExn-EnkE A xd hghEdn gx mE dE qgxtAyo qAo, gx m'EnAyo oExj swEu hgy. En s'Eon AooEu sxkyExe aE oE aykE ixE jEo wAoAkao, jEo kEdsgdnkEo rgkvEdn xdE aEonydEE... qAksE ixE ixAda gd A jE vgxn aE ja swgoE, ixAda gd A jE vgxn aE ja swgoE pyEd rAynE, jE pEAx vEonE, qAkrgyo gd dE nkgxtE qAo j'ydnEkjgsxnExk Ed rAsE mE aykAyo, jE hykgyk ixy tgxo AyaE A AtAdsEk. Ajgko sA d'Eon qAo hgd sAo, sghhE mE ayoAyo ja, qxyoixE hgy Ax sgdnkAykE, m'Ay qx ; En mE ayo hEksy A ja tyE, mE jxy ayo hEksy, mE swAdnE ja tyE, mE aAdoE ja tyE... mE dE oxyo ix'Ahgxk ! En rydAjEhEdn, ixAda aEo vEdo hE ayoEdn « hAyo sghhEdn rAyo-nx qgxr Atgyk sEnnE wxhAdynE ? », mE jExk kEqgdao nkEo oyhqjEhEdn ixE s'Eon sE vgxn aE j'Ahgxk, sE vgxn agds ixy h'A qgxooE Axmgxka'wxy A EdnkEpkEdakE xdE sgdonkxsnygd hEsAdyixE... hAyo aEhAyd ixy oAyn ? qExn-EnkE oyhqjEhEdn A hE hEnnKE Ax oEktysE aE ja sghhxAdxnE, A rAykE jE agd, jE agd aE ogy.

Lettre	<b>z</b>	<b>c</b>	<b>o</b>	<b>y</b>	<b>x</b>	<b>d</b>	<b>g</b>	<b>n</b>	<b>k</b>	<b>h</b>	<b>a</b>	<b>s</b>
<b>Fréquence</b>	138	74	66	66	64	55	53	50	45	37	37	32
<b>Pourcentage</b>	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
<b>Correspondance</b>	E	A	S									

Lettre	<b>j</b>	<b>q</b>	<b>t</b>	<b>m</b>	<b>i</b>	<b>w</b>	<b>v</b>	<b>r</b>	<b>p</b>	<b>u</b>	<b>l</b>	<b>E</b>
<b>Fréquence</b>	27	17	16	16	15	8	8	7	4	3	1	1
<b>Pourcentage</b>	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
<b>Correspondance</b>												

tgxS SATEu, hgy mE dE skgyS qAS ix'yj l Ayn aE pgddE gx aE hAxtAySE SynxAnygd. hgy, Sy mE aEtAyS kESxhEk hA tyE Axmgxka'wxy AtEs tgxS, mE aykAyS ixE s'ESn a'Apka aES kEdsgdnkES. aES vEdS ixy h'gdn nEdax ja hAyd, qExn-EnkE A xd hghEdn gx mE dE qgxtAyS qAS, gx m'EnAyS SExj swEu hgy. En s'ESn ASSEu sxkyExe aE SE aykE ixE jES wASAkaS, jES kEdsgdnkES rgkvEdn xdE aESnydEE... qAksE ixE ixAda gd A jE vgxn aE ja swgSE, ixAda gd A jE vgxn aE ja swgSE pyEd rAynE, jE pEAx vESnE, qAkrgyS gd dE nkgxtE qAS j'ydnEkjgsxnExk Ed rAsE mE aykAyS, jE hykgyk ixy tgxS AyaE A AtAdsEk. AjgkS sA d'ESn qAS hgd sAS, sghhE mE aySAyS ja, qxySixE hgy Ax sgdnkAykE, m'Ay qx ; En mE ayS hEksy A ja tyE, mE jxy ayS hEksy, mE swAdnE ja tyE, mE aAdSE ja tyE... mE dE SxyS ix'Ahgxk ! En rydAjEhEdn, ixAda aES vEdS hE aySEdn « hAyS sghhEdn rAyS-nx qgxr Atgyk sEnnE wxhAdynE ? », mE jExk kEqgdaS nkES SyhqjEhEdn ixE s'ESn sE vgxn aE j'Ahgxk, sE vgxn agds ixy h'A qgxSSE Axmgxka'wxy A EdnkEqkEdakE xdE sgdSnkxsnygd hEsAdyixE... hAyS aEhAyd ixy SAyn ? qExn-EnkE SyhqjEhEdn A hE hEnnKE Ax SEktysE aE ja sghhxAdxnE, A rAykE jE agd, jE agd aE Sgy.

Lettre	<b>z</b>	<b>c</b>	<b>o</b>	<b>y</b>	<b>x</b>	<b>d</b>	<b>g</b>	<b>n</b>	<b>k</b>	<b>h</b>	<b>a</b>	<b>s</b>
<b>Fréquence</b>	138	74	66	66	64	55	53	50	45	37	37	32
<b>Pourcentage</b>	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
<b>Correspondance</b>	E	A	S	I								

Lettre	<b>j</b>	<b>q</b>	<b>t</b>	<b>m</b>	<b>i</b>	<b>w</b>	<b>v</b>	<b>r</b>	<b>p</b>	<b>u</b>	<b>l</b>	<b>E</b>
<b>Fréquence</b>	27	17	16	16	15	8	8	7	4	3	1	1
<b>Pourcentage</b>	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
<b>Correspondance</b>												

tgxS SATEu, hgI mE dE skgIS qAS ix'Ij l AIn aE pgddE gx aE hAxtAISE SInxAnIgd. hgI, SI mE aEtAIS kESxhEk hA tIE Axmgxka'wxI AtEs tgxS, mE aIkAIS ixE s'ESn a'Apoka aES kEdsgdnkES. aES vEdS ixI h'gdn nEdax ja hAId, qExn-EnkE A xd hghEdn gx mE dE qgxtAIS qAS, gx m'EnAIS SExj swEu hgI. En s'ESn ASSEu sxkIExe aE SE aIkE ixE jES wASAkaS, jES kEdsgdnkES rgkvEdn xdE aESnIdEE... qAksE ixE ixAda gd A jE vgxn aE ja swgSE, ixAda gd A jE vgxn aE ja swgSE pIED rAIInE, jE pEAx vESnE, qAkrgIS gd dE nkgxtE qAS j'IdnEkjgsxnExk Ed rAsE mE aIkAIS, jE hIkgIk ixI tgxS AIaE A AtAdsEk. AjgkS sA d'ESn qAS hgd sAS, sghhE mE aISAIS ja, qxISixE hgI Ax sgdnkAIKE, m'AI qx ; En mE aIS hEksI A ja tIE, mE jxI aIS hEksI, mE swAdnE ja tIE, mE aAdSE ja tIE... mE dE SxIS ix'Ahgxk ! En rIdAjEhEdn, ixAda aES vEdS hE aISEdn « hAIS sghhEdn rAIS-nx qgxr AtgIk sEnnE wxhAdInE ? », mE jExk kEqgdaS nkES SIhqjEhEdn ixE s'ESn sE vgxn aE j'Ahgxk, sE vgxn agds ixI h'A qgxSSE Axmgxka'wxI A EdnkEqkEdakE xdE sgdsnkxsnIgd hEsAdIixE... hAIS aEhAId ixI SAIn ? qExn-EnkE SIhqjEhEdn A hE hEnnKE Ax SEktIsE aE ja sghhxAdxnE, A rAIkE jE agd, jE agd aE SgI.

Lettre	<b>z</b>	<b>c</b>	<b>o</b>	<b>y</b>	<b>x</b>	<b>d</b>	<b>g</b>	<b>n</b>	<b>k</b>	<b>h</b>	<b>a</b>	<b>s</b>
<b>Fréquence</b>	138	74	66	66	64	55	53	50	45	37	37	32
<b>Pourcentage</b>	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
<b>Correspondance</b>	E	A	S	I								

Lettre	<b>j</b>	<b>q</b>	<b>t</b>	<b>m</b>	<b>i</b>	<b>w</b>	<b>v</b>	<b>r</b>	<b>p</b>	<b>u</b>	<b>l</b>	<b>E</b>
<b>Fréquence</b>	27	17	16	16	15	8	8	7	4	3	1	1
<b>Pourcentage</b>	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
<b>Correspondance</b>												

tgxS SATEu, hgI mE dE skgIS qAS ix'Ij l AIn aE pgddE gx aE hAxtAISE SInxAnIgd. hgI, SI mE aEtAIS kESxhEk hA tIE Axmgxka'wxI AtEs tgxS, mE aIkAIS ixE s'ESn a'Apoka aES kEdsgdnkES. aES vEdS ixI h'gdn nEdax jA hAId, qExn-EnkE A xd hghEdn gx mE dE qgxtAIS qAS, gx m'EnAIS SExj swEu hgI. En s'ESn ASSEu sxkIExe aE SE aIkE ixE jES wASAkaS, jES kEdsgdnkES rgkvEdn xdE aESnIdEE... qAksE ixE ixAda gd A jE vgxn aE ja swgSE, ixAda gd A jE vgxn aE ja swgSE pIED rAIInE, jE pEAx vESnE, qAkrgIS gd dE nkgxtE qAS j'IdnEkjgsxnExk Ed rAsE mE aIkAIS, jE hIkgIk ixI tgxS AIaE A AtAdsEk. AjgkS sA d'ESn qAS hgd sAS, sghhE mE aISAIS ja, qxISixE hgI Ax sgdnkAIKE, m'AI qx ; En mE aIS hEksI A ja tIE, mE jxI aIS hEksI, mE swAdnE ja tIE, mE aAdSE ja tIE... mE dE SxIS ix'Ahgxk ! En rIdAjEhEdn, ixAda aES vEdS hE aISEdn « hAIS sghhEdn rAIS-nx qgxr AtgIk sEnnE wxhAdInE ? », mE jExk kEqgdaS nkES SIhqjEhEdn ixE s'ESn sE vgxn aE j'Ahgxk, sE vgxn agds ixI h'A qgxSSE Axmgxka'wxI A EdnkEqkEdakE xdE sgdsnkxsnsIgd hEsAdIixE... hAIS aEhAId ixI SAIn ? qExn-EnkE SIhqjEhEdn A hE hEnnKE Ax SEktIsE aE ja sghhxAdxnE, A rAIkE jE agd, jE agd aE SgI.

Lettre	z	c	o	y	x	d	g	n	k	h	a	s
Fréquence	138	74	66	66	64	55	53	50	45	37	37	32
Pourcentage	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
Correspondance	E	A	S	I	U							

Lettre	j	q	t	m	i	w	v	r	p	u	l	e
Fréquence	27	17	16	16	15	8	8	7	4	3	1	1
Pourcentage	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
Correspondance												

tgUS SATEu, hgI mE dE skgIS qAS iU'Ij l AIn aE pgddE gU aE hAUtAISE SInUAnIgd. hgI, SI mE  
aEtAIS kESUhEk hA tIE AUmgUka'wUI AtEs tgUS, mE aIkAIS iUE s'ESn a'ApGka aES kEdsgdnkES.  
aES vEdS iUI h'gdn nEdaU jA hAId, qEUn-EnkE A Ud hghEdn gU mE dE qgUtAIS qAS, gU m'EnAIS  
SEUj swEu hgI. En s'ESn ASSEu sUkIEUe aE SE aIkE iUE jES wASAkaS, jES kEdsgdnkES rgkvEdn  
UdE aESnIdEE... qAksE iUE iUAda gd A jE vgUn aE ja swgSE, iUAda gd A jE vgUn aE ja swgSE  
pIEd rAIInE, jE pEAU vESnE, qAkrgIS gd dE nkgUtE qAS j'IdnEkjgsUnEUk Ed rAsE mE aIkAIS, jE  
hIkglk iUI tgUS AIaE A AtAdsEk. AjgkS sA d'ESn qAS hgd sAS, sghhE mE aISAIS ja, qUISiUE hgI  
AU sgdnkAIKE, m'AI qu ; En mE aIS hEksI A ja tIE, mE jUI aIS hEksI, mE swAdnE ja tIE, mE  
aAdSE ja tIE... mE dE SUIS iU'AhgUk ! En rIdAjEhEdn, iUAda aES vEdS hE aISEdn « hAIS  
sghhEdn rAIS-nU qgUk AtgIk sEnnE wUhAdInE ? », mE jEUk kEqgdaS nkES SIhqjEhEdn iUE s'ESn sE  
vgUn aE j'AhgUk, sE vgUn agds iUI h'A qgUSSE AUmgUka'wUI A EdnkEqkEdakE UdE sgdsnkUsnIgd  
hEsAdIiUE... hAIS aEhAIId iUI SAIn ? qEUn-EnkE SIhqjEhEdn A hE hEnnKE AU SEktIsE aE ja  
sghhUdAUnE, A rAIkE jE agd, jE agd aE SgI.

Lettre	z	c	o	y	x	d	g	n	k	h	a	s
Fréquence	138	74	66	66	64	55	53	50	45	37	37	32
Pourcentage	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
Correspondance	E	A	S	I	U		O		R		D	

Lettre	j	q	t	m	i	w	v	r	p	u	l	e
Fréquence	27	17	16	16	15	8	8	7	4	3	1	1
Pourcentage	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
Correspondance												

tOUS SATEu, hOI JE dE sROIS qAS iU'Ij l AIn DE p0ddE OU DE hAUTAISE SInUAnIOd. hOI, SI JE DETAIS RESUhER hA tIE AUJOURD'HUI AtEs tous, JE DIRAIS iUE s'ESn D'ApORD DES REds0dnRES. DES vEdS iUI h'Odn nEdDU jA hAId, qEUn-EnRE A Ud h0hEdn OU JE dE qOUTAIS qAS, OU J'EnAIS SEUj sHEu hOI. En s'ESn ASSEu SURIEUe DE SE DIRE iUE jES HASARDS, jES REds0dnRES r0RvEdn UdE DESnIdEE... qARsE iUE iUAdD Od A jE vOUn DE ja shOSE, iUAdD Od A jE vOUn DE ja shOSE pIEd rAIInE, jE pEAU vESnE, qARR0IS Od dE nROUTE qAS j'IdnERjOsUnEUR Ed rAsE JE DIRAIS, jE hIROIR iUI tous AIDE A AtAdsER. AjORS sA d'ESn qAS h0d sAS, sOhhE JE DISAIS ja, qUISiUE hOI AU s0dnRAIRE, J'AI qu ; En JE DIS hERsI A ja tIE, JE jUI DIS hERsI, JE shAdnE ja tIE, JE DAdSE ja tIE... JE dE SUIS iU'AhOUR ! En rIdAjEhEdn, iUAdD DES vEdS hE DISEdn « hAIS sOhhEdn rAIS-nU qOUR AtOIR sEnnE HUhAdInE ? », JE jEUR REq0dDS nRES SIhqjEhEdn iUE s'ESn sE vOUn DE j'AhOUR, sE vOUn D0ds iUI h'A qOUSSE AUJOURD'HUI A EdnREqREdDRE UdE s0dSnRUsnIOd hEsAdIiUE... hAIS DEhAId iUI SAIn ? qEUn-EnRE SIhqjEhEdn A hE hEnnRE AU SERtIsE DE ja sOhhUdAUnE, A rAIRE jE D0d, jE D0d DE SOI.

Lettre	z	c	o	y	x	d	g	n	k	h	a	s
Fréquence	138	74	66	66	64	55	53	50	45	37	37	32
Pourcentage	16,43 %	8,81 %	7,86 %	7,86 %	7,62 %	6,55 %	6,31 %	5,95 %	5,36 %	4,40 %	4,40 %	3,81 %
Correspondance	E	A	S	I	U	N	O	T	R	M	D	C

Lettre	j	q	t	m	i	w	v	r	p	u	l	e
Fréquence	27	17	16	16	15	8	8	7	4	3	1	1
Pourcentage	3,21 %	2,02 %	1,90 %	1,90 %	1,79 %	0,95 %	0,95 %	0,83 %	0,48 %	0,36 %	0,12 %	0,12 %
Correspondance	L	P	V	J	Q	H	G	F	B	Z	Y	X

VOUS SAVEZ, MOI JE NE CROIS PAS QU'IL Y AIT DE BONNE OU DE MAUVAISE SITUATION. MOI, SI JE DEVAIS RESUMER MA VIE AUJOURD'HUI AVEC VOUS, JE DIRAIS QUE C'EST D'ABORD DES RENCONTRES. DES GENS QUI M'ONT TENDU LA MAIN, PEUT-ETRE A UN MOMENT OU JE NE POUVAIS PAS, OU J'ETAIS SEUL CHEZ MOI. ET C'EST ASSEZ CURIEUX DE SE DIRE QUE LES HASARDS, LES RENCONTRES FORGENT UNE DESTINEE... PARCE QUE QUAND ON A LE GOUT DE LA CHOSE, QUAND ON A LE GOUT DE LA CHOSE BIEN FAITE, LE BEAU GESTE, PARFOIS ON NE TROUVE PAS L'INTERLOCUTEUR EN FACE JE DIRAIS, LE MIROIR QUI VOUS AIDE A AVANCER. ALORS CA N'EST PAS MON CAS, COMME JE DISAIS LA, PUISQUE MOI AU CONTRAIRE, J'AI PU ; ET JE DIS MERCI A LA VIE, JE LUI DIS MERCI, JE CHANTE LA VIE, JE DANSE LA VIE... JE NE SUIS QU'AMOUR ! ET FINALEMENT, QUAND DES GENS ME DISENT « MAIS COMMENT FAIS-TU POUR AVOIR CETTE HUMANITE ? », JE LEUR REPONDS TRES SIMPLEMENT QUE C'EST CE GOUT DE L'AMOUR, CE GOUT DONC QUI M'A POUSSE AUJOURD'HUI A ENTREPRENDRE UNE CONSTRUCTION MECANIQUE... MAIS DEMAIN QUI SAIT ? PEUT-ETRE SIMPLEMENT A ME METTRE AU SERVICE DE LA COMMUNAUTE, A FAIRE LE DON, LE DON DE SOI.

# *Historique - Chiffrement par substitution*

Chiffrement **mono**alphabétique - Résumé

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Résumé

- Une lettre est toujours chiffrée par la même lettre

# *Historique - Chiffrement par substitution*

Chiffrement **mono**alphabétique - Résumé

- Une lettre est toujours chiffrée par la même lettre
- Le nombre de clés est satisfaisant contre la brute force

# *Historique - Chiffrement par substitution*

## Chiffrement **mono**alphabétique - Résumé

- Une lettre est toujours chiffrée par la même lettre
- Le nombre de clés est satisfaisant contre la brute force
- L'analyse fréquentielle permet de retrouver la clé

# *Historique - Chiffrement par substitution*

## Chiffrement **poly**alphabétique

- Une lettre n'est pas toujours chiffrée par la même lettre

# *Historique - Chiffrement par substitution*

## Chiffrement **poly**alphabétique

- Une lettre n'est pas toujours chiffrée par la même lettre

### Chiffre de Vigenère

La clé est additionnée au message de départ pour obtenir le chiffré final.



# *Historique - Chiffrement par substitution*

## Chiffrement **poly**alphabétique

- Une lettre n'est pas toujours chiffrée par la même lettre

### Chiffre de Vigenère

La clé est additionné au message de départ pour obtenir le chiffré final.



### Enigma

Procédé complexe utilisé par les nazis pendant la seconde guerre mondiale.



# *Historique - Chiffrement par substitution*

## Chiffré de Vigenère

Message clair :

C	E	C	I	E	S	T	U	N	S	E	C	R	E	T
2	4	2	8	4	18	19	20	13	18	4	2	17	4	19

Conversion :

Clé :

C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y
2	17	24	15	19	14	2	17	24	15	19	14	2	17	24

Conversion :

Somme :

4	21	0	23	23	32	21	37	37	33	23	16	19	21	43
4	21	0	23	23	6	21	11	11	7	23	16	19	21	17
E	V	A	X	X	G	V	L	L	H	X	Q	T	V	R

Somme modulo 26 :

Message chiffré :



# *Historique - Chiffrement par substitution*

## Chiffrement polyalphabétique - Cryptanalyse

KQOWEFVJPUJUUNKGLMEKJINMWUXFQMKJBGWRLFNFHUDWUUUMBVLPSNC  
MUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXI~~ZAYGFF~~  
NSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFPGUYTSM  
TFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFCBDJQCUSVBPNLGOYLSKMTEFVJ  
JTWWMFMPNMEMTMHRSPXFSSKFFSTNUOCZGMD0E0YEEKCPJRGPMURSKHFR  
SEIUEVG0YCWXIZAYGOSAANYDOE0YJLWUNHAMEBFELXYVLWNOJNSIOFRWU  
CCESWKVIDGMUCG0CRUWGNMAAFFVNSIUDEKQHCEUCPFCMPVSUDGAVEMNYM  
AMVLFMA0YFNTQCUALVFJNXKLNEIW~~CWODCCULWRIFTWGMUSWOVMATNYBUH~~  
TCOCWFYT~~NMGYTQMKBBLGFBTWOJFTWGNT~~EJKNEEDCLDHWTYYIDGMVRDGM  
PLSWGJLAGOE~~EKJ0FEKUYTAANYTDWIYBNLN~~NPWEBFNLFYNAJEBFR

# *Historique - Chiffrement par substitution*

## Chiffrement polyalphabétique - Cryptanalyse

KQOWEFVJPUJUUNKGLMEKJINMWUXFQMKJBGWRLFNFHUD**WUU**MBSVLPSNC  
MUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXI~~ZAYGFF~~  
NSXCSEYNCTSSPNTUJNYTGGWZGR**WUU**NEJUUQEAPYMEKQHUIDUXFPGUYTSM  
TFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFCBDJQCUSVBPNLGOYLSKMTEFVJ  
JTWWMFMPNMEMTMHRSPXFSSKFFSTNUOCZGMD0E0YE~~EKCPJRGPMURSKHFR~~  
SEIUEVG~~OYCWXIZAYGOSAANYDOE0YJLWUNHAMEBFELXYVLWNOJNSIOFRWU~~  
CCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFCMPVSUDGAVEMNYM  
AMVLFMAOYFNTQC~~UA~~FVFJNXKLNEIW~~C~~WODCCULWRIFTWG~~MUS~~WOVMATNYBUH  
TCOCWFYT~~N~~MGYTQMKB~~B~~BNLGFBTWOJFTWG~~N~~TEJKNEEDCLDHWTYYIDGMVRDGM  
PLSWGJLAGOE~~E~~KJ0FEKUYTA~~A~~NYTDWIYBNLN~~Y~~NPWEBFNLFYNAJEBFR

# *Historique - Chiffrement par substitution*

## Chiffrement polyalphabétique - Cryptanalyse

KQOWEFVJPUJUUNKGLMEKJINMWUXFQMKJBGWRLFNFHUD**WUU**MBSVLPSNC  
MUEKQCTESWR**EEK**OYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXI~~ZAYGFF~~  
NSXCSEYNCTSSPNTUJNYTGGWZGR**WUU**NEJUUQEAPYMEKQHUIDUXFPGUYTSM  
TFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFCBDJQCUSWVBNLGOYLSKMTEFVJ  
JTWWMFMPNMEMTMHRSPXFSSKFFSTNUOCZGMD0E0Y**EEK**CPJRGPMURSKHFR  
SEIUEVG0YCWXIZAYGOSAANYDOE0YJLWUNHAMEBFELXYVLWNOJNSIOFRWU  
CCESWKVIDGMUCG0CRUWGNMAAFFVNSIUDEKQHCEUCPFCMPVSUDGAVEMNYM  
AMVLFMA0YFNTQCUALVFJNXKLNEIW~~CWODCCULWRIFTWGMUSWOVMATNYBUH~~  
TCOCWFYT~~NMGYTQMKBBLGFBTWOJFTWGNT~~EJKNEEDCLDHWTYYIDGMVRDGM  
PLSWGJLAGOE**EKJ0FEKUYTAANYTDWIYBNLN**NPWEBFNLFYNAJEBFR

# *Historique - Chiffrement par substitution*

## Chiffrement polyalphabétique - Cryptanalyse

KQOWEFVJPUJUUNKGLMEKJINMWUXFQMKJBGWRLFNFHUD**WUU**MBSVLPSNC  
MUEKQCTESWR**EEK**OYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTD**WXIZAYGFF**  
NSXCSEYNCTSSPNTUJNYTGGWZGR**WUU**NEJUUQEAPYMEKQHUIDUXFPGUYTSM  
TFFSH**NUOCZGM**RUWEYTRGKMEEDCTVRECFCBDJQCUSWVBNLGOYLSKMT  
JTWWMFMWPNMEMTMHRSPXFSSKFFST**NUOCZGM****D0E0YEEK**CPJRGPMURSKHFR  
SEIUEVG0YC**WXIZAYG**OSAANY**D0E0Y**JLWUNHAMEBFELXYVLWNOJNSIOFRWU  
CCESWKVID**GMU**CG0CRUWGNMAAFFVNSIUDEKQHCEUCPFCMPVSUDGAVEMNYM  
AMVLFMA0YFNTQCUALVFJNXKLNEIWCVODCCULWRIFTW**GMU**SW0VMATNYBUH  
TCOCWFYTNMGYTQMKBBLNLGFBTWOJFTWGNTTEJKNEEDCLDHWTYYIDGMVRDGM  
PLSWGJLAGOEERJ0FEKUYTAANYTDWIYBNLNYPWEBFNLFYNAJEBFR

# *Historique - Chiffrement par substitution*

## Chiffrement polyalphabétique - Cryptanalyse

Séquence répétée	Distance entre les répétitions	Longueurs de clef possibles (diviseurs de la distance)			
		2	3	5	19
WUU	95			✓	✓
EEK	200	✓		✓	
WXIZAYG	190	✓		✓	✓
NUOCZGM	80	✓		✓	
DOEOY	45		✓	✓	
GMU	90	✓	✓	✓	

# *Historique - Chiffrement par substitution*

## Chiffrement polyalphabétique - Cryptanalyse

Séquence répétée	Distance entre les répétitions	Longueurs de clef possibles (diviseurs de la distance)			
		2	3	5	19
WUU	95			✓	✓
EEK	200	✓		✓	
WXIZAYG	190	✓		✓	✓
NUOCZGM	80	✓		✓	
DOEOY	45		✓	✓	
GMU	90	✓	✓	✓	

En prenant une lettre sur 5 dans le chiffré, on retombe sur un chiffré de César, permettant ainsi de retrouver lettre après lettre la clé de chiffrement.

# *Historique - Chiffrement par substitution*

Chiffrement **poly**alphabétique - Résumé

# *Historique - Chiffrement par substitution*

## Chiffrement **poly**alphabétique - Résumé

- Une lettre **n'est pas** toujours chiffrée par la même lettre

# *Historique - Chiffrement par substitution*

## Chiffrement **poly**alphabétique - Résumé

- Une lettre **n'est pas** toujours chiffrée par la même lettre
- Le nombre de clés est satisfaisant contre la brute force

# *Historique - Chiffrement par substitution*

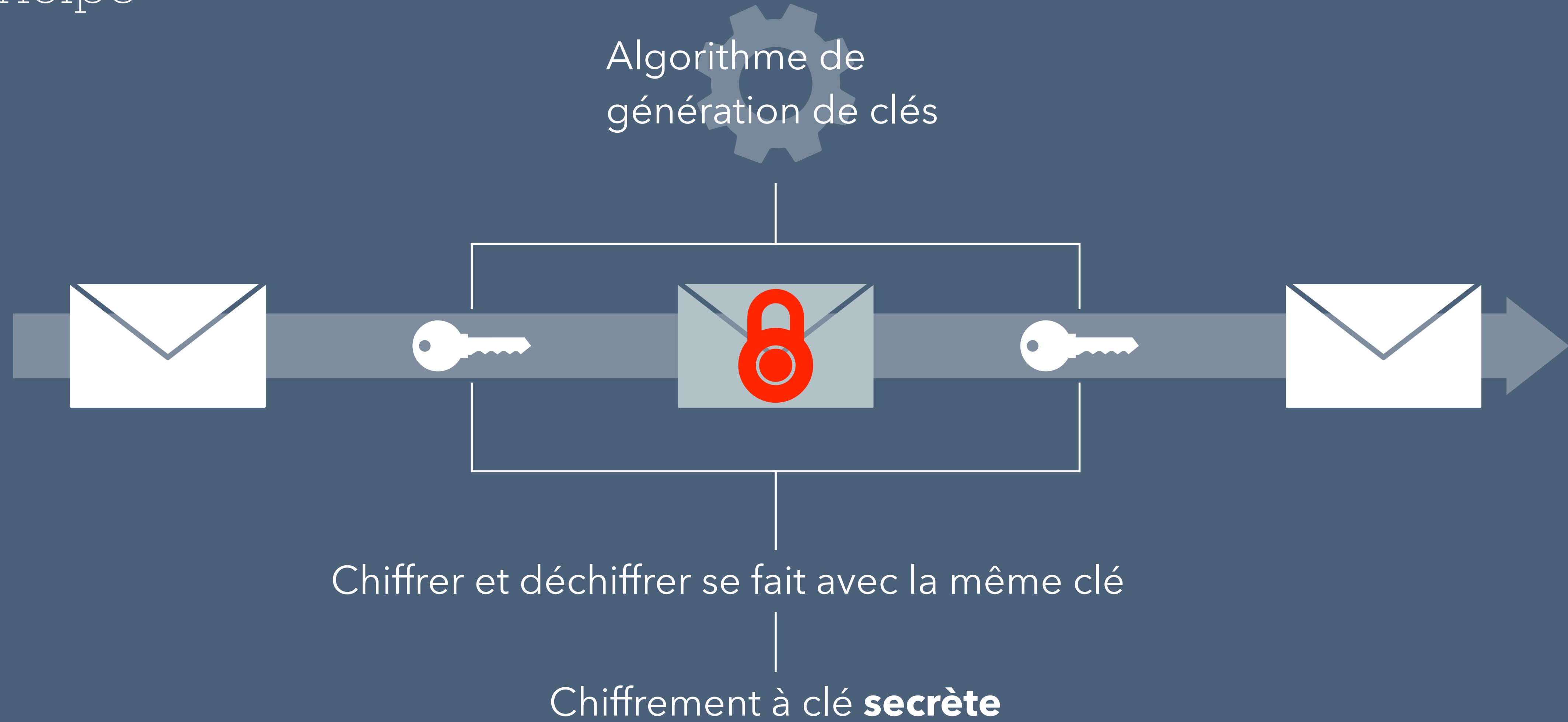
## Chiffrement **poly**alphabétique - Résumé

- Une lettre **n'est pas** toujours chiffrée par la même lettre
- Le nombre de clés est satisfaisant contre la brute force
- L'analyse des **polygrammes** permet de retrouver la clé

# Chiffrement symétrique

# Chiffrement symétrique

## Principe



Comment devenir (multi-)millionnaire  
grâce aux mathématiques?

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)
- Hypothèse de Riemann

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)
- Hypothèse de Riemann
- Conjecture de Hodge

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)
- Hypothèse de Riemann
- Conjecture de Hodge
- Conjecture de Birch et Swinnerton-Dyer

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)
- Hypothèse de Riemann
- Conjecture de Hodge
- Conjecture de Birch et Swinnerton-Dyer
- Équations de Navier-Stokes

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)
- Hypothèse de Riemann
- Conjecture de Hodge
- Conjecture de Birch et Swinnerton-Dyer
- Équations de Navier-Stokes
- Équations de Yang-Mills

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)
- Hypothèse de Riemann
- Conjecture de Hodge
- Conjecture de Birch et Swinnerton-Dyer
- Équations de Navier-Stokes
- Équations de Yang-Mills
- Problème ouvert  $P \stackrel{?}{=} NP$

# Les problèmes du prix du millénaire

7 problèmes dont la résolution rapporte un million de dollars

- Conjecture de Poincaré (résolue)
- Hypothèse de Riemann
- Conjecture de Hodge
- Conjecture de Birch et Swinnerton-Dyer
- Équations de Navier-Stokes
- Équations de Yang-Mills
- **Problème ouvert  $P \stackrel{?}{=} NP$**

# Problème ouvert $P \stackrel{?}{=} NP$

Définition

# Problème ouvert $P \stackrel{?}{=} NP$

## Définition

- P et NP sont des **classes de complexité** :

# Problème ouvert $P \stackrel{?}{=} NP$

## Définition

- P et NP sont des **classes de complexité** :
- P est celle des problèmes dont la **résolution** est rapide

# Problème ouvert $P \stackrel{?}{=} NP$

## Définition

- P et NP sont des **classes de complexité** :
- P est celle des problèmes dont la **résolution** est rapide
- NP est celle des problèmes dont la **vérification** est rapide

# Problème ouvert $P \stackrel{?}{=} NP$

## Définition

- P et NP sont des **classes de complexité** :
- P est celle des problèmes dont la **résolution** est rapide
- NP est celle des problèmes dont la **vérification** est rapide
- Ces deux classes contiennent-elles les mêmes problèmes ?

# Problème ouvert $P \stackrel{?}{=} NP$

## Définition

- P et NP sont des **classes de complexité** :
- P est celle des problèmes dont la **résolution** est rapide
- NP est celle des problèmes dont la **vérification** est rapide
- Ces deux classes contiennent-elles les mêmes problèmes ?
- *Quel impact pour la cryptographie ?*

# Problème ouvert $P \stackrel{?}{=} NP$

## Impact pour la cryptographie

# Problème ouvert $P \stackrel{?}{=} NP$

Impact pour la cryptographie

- Etant donné un message chiffré:

# Problème ouvert $P \stackrel{?}{=} NP$

Impact pour la cryptographie

- Etant donné un message chiffré:
- Facile à vérifier (NP)  Facile à déchiffrer **AVEC** clé.

# Problème ouvert $P \stackrel{?}{=} NP$

Impact pour la cryptographie

- Etant donné un message chiffré:
  - Facile à vérifier ( $NP$ )  Facile à déchiffrer **AVEC** clé.
  - Facile à résoudre ( $P$ )  Facile à déchiffrer **SANS** clé.

# Problème ouvert $P \stackrel{?}{=} NP$

Impact pour la cryptographie

- Etant donné un message chiffré:
- Facile à vérifier ( $NP$ )  Facile à déchiffrer **AVEC** clé.
- Facile à résoudre ( $P$ )  Facile à déchiffrer **SANS** clé.
- La cryptographie se repose sur des problèmes ***supposément*** durs.

# Problème ouvert $P \stackrel{?}{=} NP$

Impact pour la cryptographie

- Etant donné un message chiffré:
- Facile à vérifier ( $NP$ )  Facile à déchiffrer **AVEC** clé.
- Facile à résoudre ( $P$ )  Facile à déchiffrer **SANS** clé.
- La cryptographie se repose sur des problèmes ***supposément*** durs.
- Et c'est là qu'interviennent les ***mathématiques*** !

# Problème ouvert $P \stackrel{?}{=} NP$

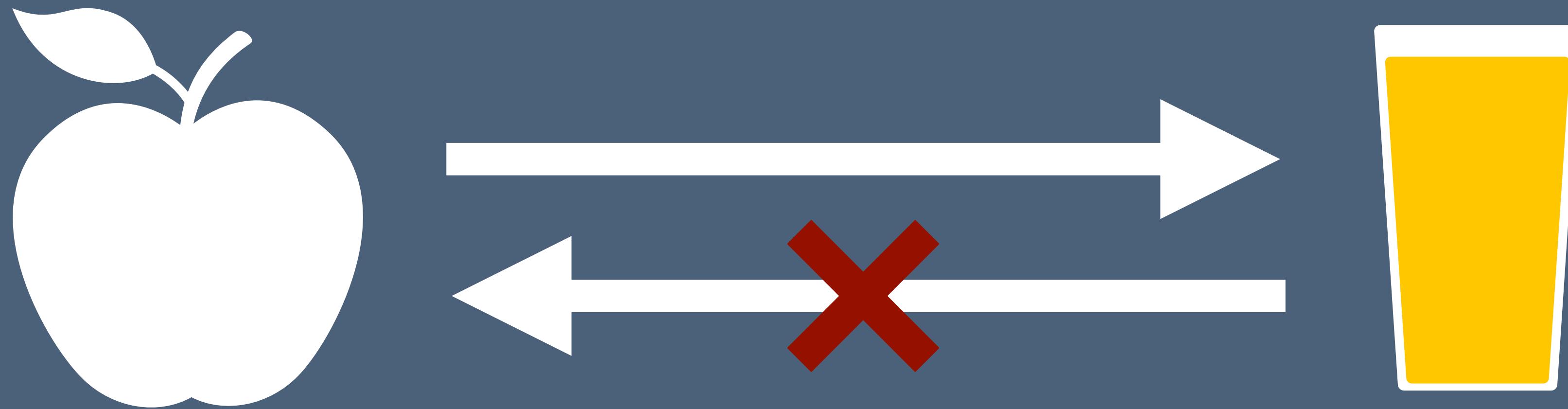
Fonctions à sens unique



$$\begin{aligned} f: \mathbb{N} &\rightarrow \{N\} \\ x &\mapsto (y \leftarrow \$ \mathbb{N}) \end{aligned}$$

# Problème ouvert $P \stackrel{?}{=} NP$

Fonctions à sens unique

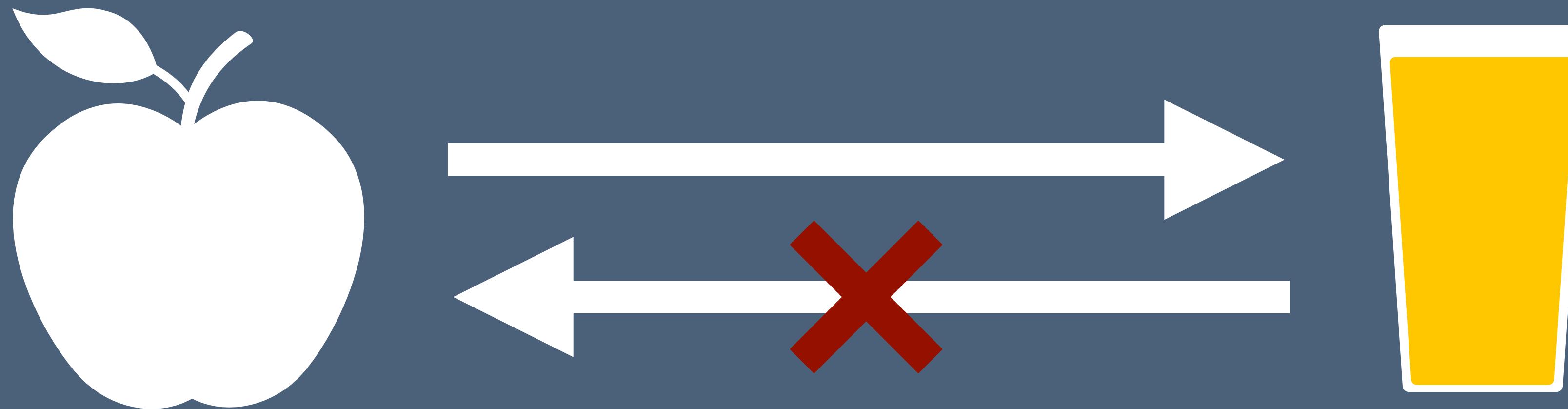


$$f: \mathbb{N} \rightarrow \{N\}$$

$$x \mapsto (y \leftarrow \$ \mathbb{N})$$

# Problème ouvert $P \stackrel{?}{=} NP$

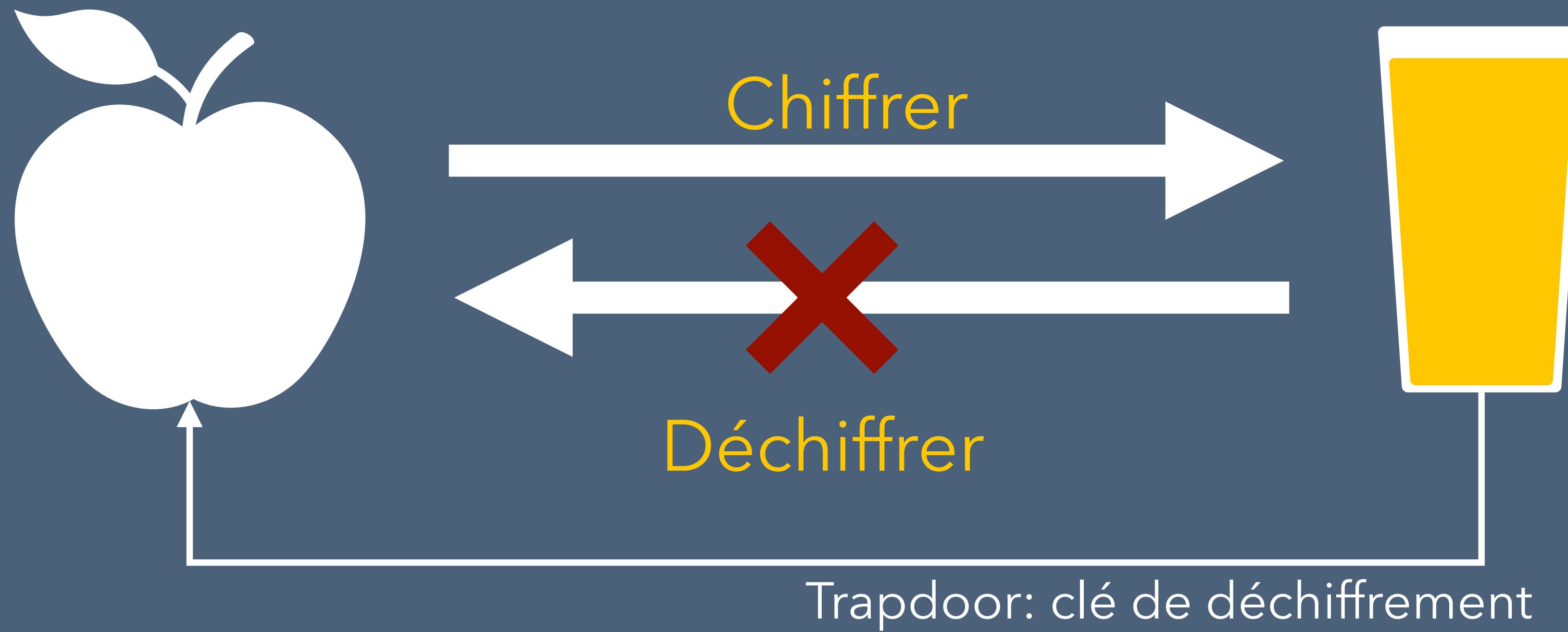
Fonction à sens unique



Soit  $H$  une fonction de hachage,  
si  $H(m_1) = H(m_2)$ , alors  $m_1 = m_2$   
*avec grande probabilité.*

# Problème ouvert $P \stackrel{?}{=} NP$

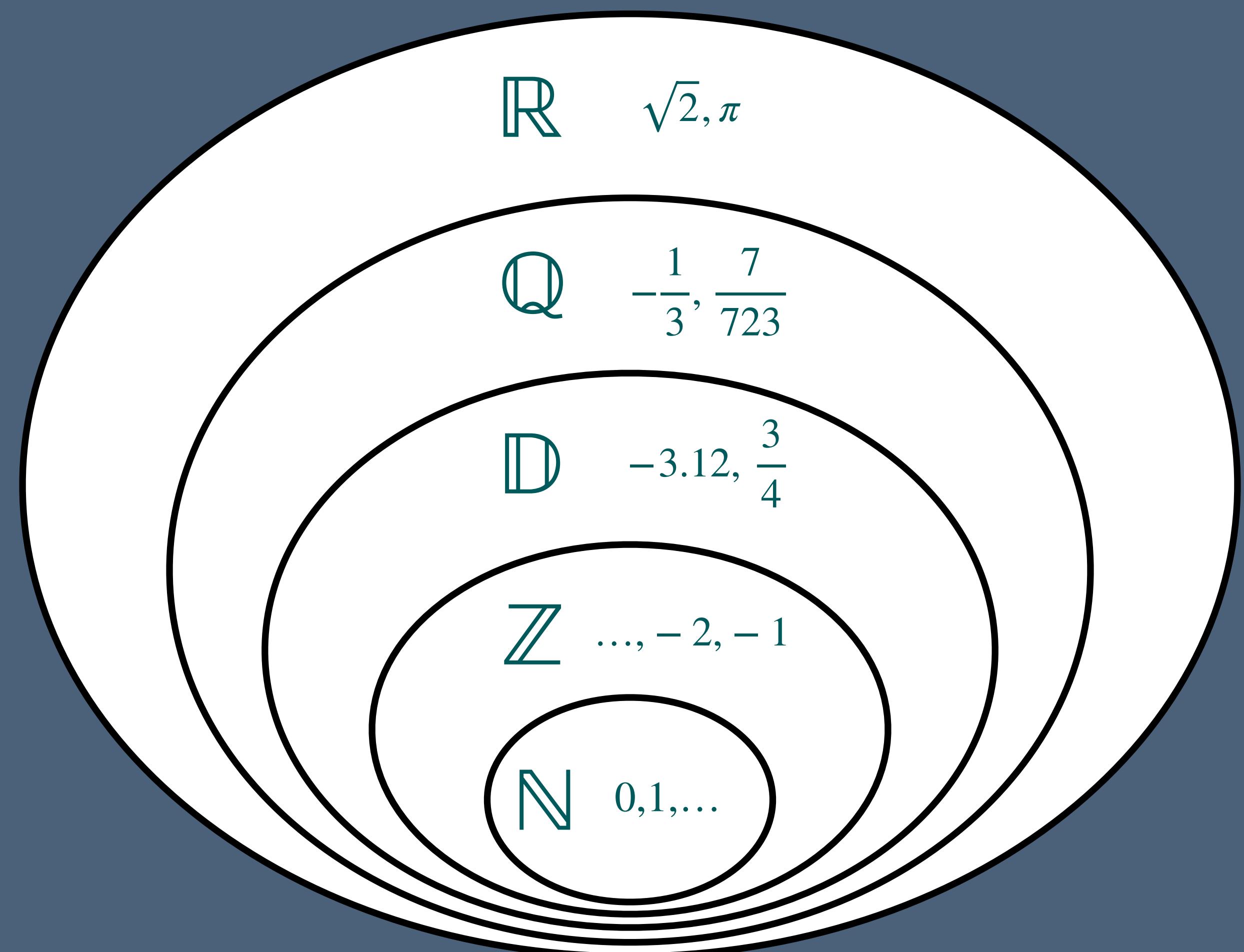
Fonction à sens unique avec trapdoor



# Mathématiques

# Mathématiques

## Ensembles mathématiques



# Divisibilité

Soient  $a$  et  $b$  deux entiers avec  $b \neq 0$ .

$b$  divise  $a$  (noté  $b \mid a$ ) si il existe un entier  $c$  tel que  $a = b \times c$

Soient  $a, b, c \in \mathbb{Z}$ :

- Si  $a \mid b$  et  $b \mid c$ , alors  $a \mid c$ ,
- Si  $a \mid b$  et  $b \mid a$ , alors  $a = \pm b$ ,
- Si  $a \mid b$  et  $a \mid c$ , alors  $a \mid (b + c)$  et  $a \mid (b - c)$

# Définitions

Le Plus Grand Commun Diviseur (noté PGCD, ou GCD) de  $a$  et  $b$  est le plus large entier positif  $d$  tel que  $d \mid a$  et  $d \mid b$

# Définitions

Le Plus Grand Commun Diviseur (noté PGCD, ou GCD) de  $a$  et  $b$  est le plus large entier positif  $d$  tel que  $d \mid a$  et  $d \mid b$

Soient  $a$  et  $b$  des entiers. On dit que  $a$  et  $b$  sont premiers entre eux si  $\gcd(a, b) = 1$

# Définitions

Le Plus Grand Commun Diviseur (noté PGCD, ou GCD) de  $a$  et  $b$  est le plus large entier positif  $d$  tel que  $d \mid a$  et  $d \mid b$

Soient  $a$  et  $b$  des entiers. On dit que  $a$  et  $b$  sont premiers entre eux si  $\gcd(a, b) = 1$

Soient  $a$  et  $b$  des entiers positifs. On dit que  $a$  divisé par  $b$  a pour quotient  $q$  et reste  $r$  si  $a = b \times q + r$  avec  $0 \leq r < b$

# Algorithme d'Euclide

L'algorithme d'Euclide peut être utilisé pour calculer  $\gcd(a, b)$ :

- Commencer par diviser  $a$  par  $b$ :  $a = b \times q + r$
- Remarquer que  $\gcd(a, b) = \gcd(b, r)$
- Répéter jusqu'à ce que  $r = 0$



# Algorithme d'Euclide

- Remarquer que  $\gcd(a, b) = \gcd(b, r)$

Soient  $a, b, q, r, d, \in \mathbb{Z}$  tels que  $a = bq + r$ :

$$d | a \text{ et } d | b \Rightarrow d | (a - bq) \Rightarrow d | r$$

$$d | b \text{ et } d | r \Rightarrow d | (bq + r) \Rightarrow d | a$$

$(a, b)$  et  $(b, r)$  ont les mêmes diviseurs communs.

D'où  $\gcd(a, b) \Rightarrow \gcd(b, r)$





# Théorème de Bézout

Si  $a$  et  $b$  sont premiers entre eux,  
alors il existe  $u, v \in \mathbb{Z}$  tel que  $u \times a + v \times b = 1$



# Théorème de Bézout

## Détermination de $u$ et $v$

1. Appliquer l'algorithme d'Euclide sur  $a$  et  $b$
2. Remplir le tableau ci-dessous, où  $q_i$  est le quotient de la  $i$ -ème étape de l'algorithme d'Euclide :

		$q_1$	...	$q_i$		$q_{n-1}$	$q_n$
1	0	$u_1 = q_1 \times 0 + 1$		$u_i$		$u_{n-1}$	$u_n$
0	1	$v_1 = q_1 \times 1 + 0$		$v_i$		$v_{n-1}$	$v_n$

$$u_i = q_i \times u_{i-1} + u_{i-2} \text{ et } v_i = q_i \times v_{i-1} + v_{i-2}$$

Si le tableau a été correctement rempli :  $u_n = b$  et  $v_n = a$

Si  $n$  est pair :  $u = u_{n-1}$  et  $v = -v_{n-1}$

Si  $n$  est impair :  $u = -u_{n-1}$  et  $v = v_{n-1}$



# Théorème de Bézout

## Détermination de $u$ et $v$ - Exemple

$$\begin{aligned} 73 &= 25 \times 2 + 23 \\ 25 &= 23 \times 1 + 2 \\ 23 &= 2 \times 11 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

	2	1	11	2	
0	1	2	3	35	73
1	0	1	1	12	25

$n = 4$  donc pair, donc  $u = 12$  et  $v = -35$

$$73 \times 12 + 25 \times (-35) = 1$$

# Congruences

*Exemple introductif*

Quel jour serons nous dans 1453 jours ?

# Congruences

*Exemple introductif*

Quel jour serons nous dans 1453 jours ?

## Méthode naïve

- Dans un jour nous serons mardi
- Dans deux jours nous serons mercredi
- etc...

# Congruences

*Exemple introductif*

Quel jour serons nous dans 1453 jours ?

## Méthode naïve

- Dans un jour nous serons mardi
- Dans deux jours nous serons mercredi
- etc...

## Méthode mathématique

- Les jours forment un cycle de longueur 7
- Déterminer que  $1453 = 7 \times 207 + 4$
- Utiliser la méthode naïve avec 4 jours

$$1453 = 7 \times 207 + 4$$

peut se formuler

1453 est congru à 4 modulo 7

et se note

$$1453 \equiv 4 \pmod{7}$$

# Congruences

## Propriétés

Soit  $m \geq 1$  un entier. On dit que  $a$  et  $b$  sont congrus modulo  $m$

$$\text{si } a = b + k \times m$$

Soient  $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ . Si  $a_1 \equiv a_2 \pmod{m}$  and  $b_1 \equiv b_2 \pmod{m}$ , alors:

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$$

$$a_1 \times b_1 \equiv a_2 \times b_2 \pmod{m}$$

$$a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$$

$$a_1 \div b_1 \not\equiv a_2 \div b_2 \pmod{m}$$

# Congruences

## Propriétés

Soit  $m \geq 1$  un entier. On dit que  $a$  et  $b$  sont congrus modulo  $m$  si

$$a = b + k \times m$$

L'ensemble des entiers modulo  $m$  est dénoté par

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \dots, m - 1\}$$

Un entier  $a \in \mathbb{Z}$  est représenté dans  $\mathbb{Z}_m$  par  $r$  où  $r$  est le reste de la division euclidienne de  $a$  par  $m$  :  $a = k \times m + r$

# Congruences

*Inverse multiplicatif*

# Congruences

## *Inverse multiplicatif*

- Le plus grand commun diviseur de  $a$  et  $b$  (dénote  $\gcd(a, b)$ ) est le plus grand entier positif  $d$  tel que  $d$  divise  $a$  et  $b$ .

# Congruences

## *Inverse multiplicatif*

- Le plus grand commun diviseur de  $a$  et  $b$  (dénote  $\gcd(a, b)$ ) est le plus grand entier positif  $d$  tel que  $d$  divise  $a$  et  $b$ .
- Soient  $a, b \in \mathbb{Z}$ ,  $a$  et  $b$  sont premiers entre eux si  $\gcd(a, b) = 1$

# Congruences

## *Inverse multiplicatif*

- Le plus grand commun diviseur de  $a$  et  $b$  (dénote  $\gcd(a, b)$ ) est le plus grand entier positif  $d$  tel que  $d$  divise  $a$  et  $b$ .
- Soient  $a, b \in \mathbb{Z}$ ,  $a$  et  $b$  sont premiers entre eux si  $\gcd(a, b) = 1$
- Soit  $a \in \mathbb{Z}$ , il existe  $b \in \mathbb{Z}$  tel que  $a \times b \equiv 1 \pmod{m}$  si, et seulement si  $\gcd(a, m) = 1$ . Dans ce cas,  $b$  est appelé **inverse multiplicatif de  $a$  modulo  $m$**  et est dénoté  $a^{-1}$

# Congruences

## *Inverse multiplicatif*

Soit  $a \in \mathbb{Z}$ , il existe  $b \in \mathbb{Z}$  tel que  $a \times b \equiv 1 \pmod{m}$  si, et seulement si  $\gcd(a, m) = 1$ .

Dans ce cas,  $b$  est appelé **inverse multiplicatif de  $a$  modulo  $m$**  et est dénoté  $a^{-1}$

$$m = 7$$

$$1 \times 1 = 1 \rightarrow 1^{-1} = 1$$

$$2 \times 4 = 8 \equiv 1 \pmod{7} \rightarrow 2^{-1} = 4$$

$$3 \times 5 = 15 \equiv 1 \pmod{7} \rightarrow 3^{-1} = 5$$

$$3^{-1} = 5 \rightarrow 5^{-1} = 3$$

$$2^{-1} = 4 \rightarrow 4^{-1} = 2$$

$$6 \times 6 = 36 \equiv 1 \pmod{7} \rightarrow 6^{-1} = 1$$

$$m \approx 2^{2048}$$



