Cégep Sainte-Foy
Québec, Qc.

Cryptographie et sécurité informatique

JEAN-LOU DE CARUFEL

LSFM
Département d'informatique et de génie logiciel
FACULTÉ DES SCIENCES ET DE GÉNIE
UNIVERSITÉ LAVAL

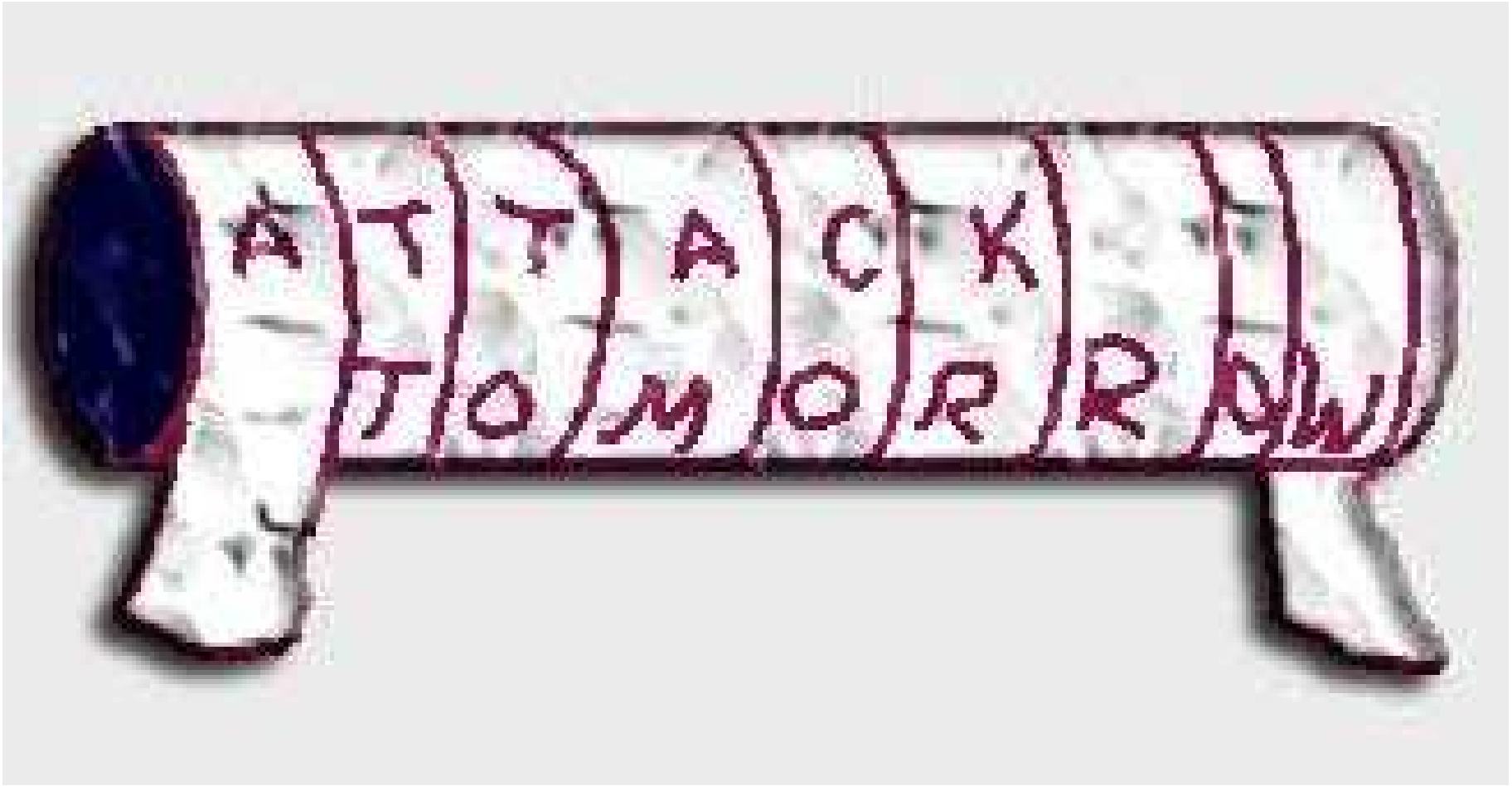
Qu'est-ce que la cryptographie ?

Quelles sont les applications ?

La bataille entre crypteurs et décrypteurs

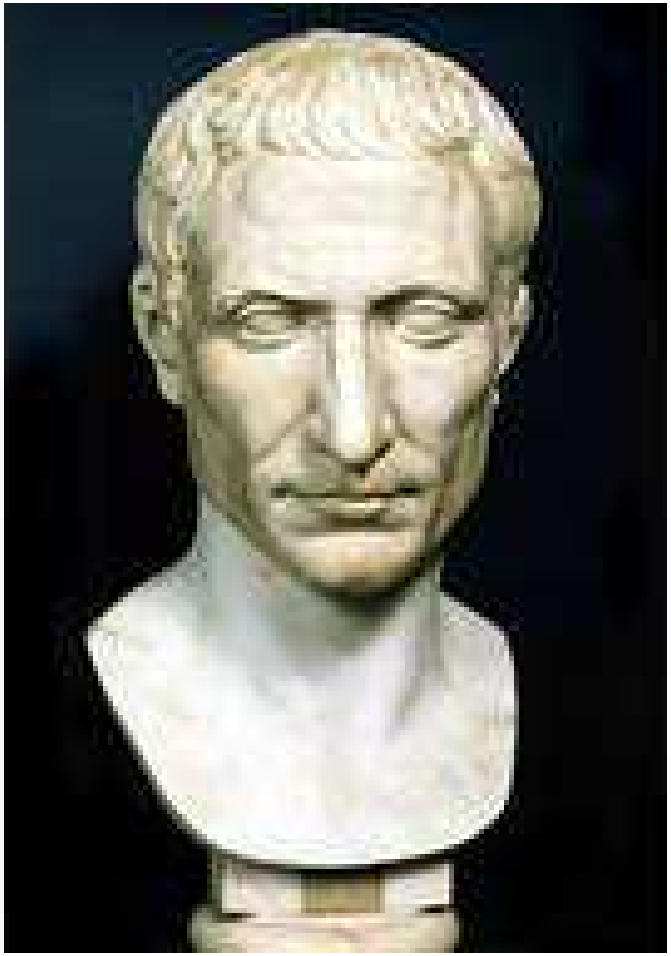
Les premières méthodes

1. Histaïaeus souhaitait encourager Aristagoras de Milet à se soulever contre le roi de Perse...
2. Tablette de bois gravée et recouverte de cire
3. La scytale



Une scytale

Mélanger les lettres



Jules César (101 av. J.-C. - 44 av. J.-C.)

La cryptographie selon Jules César

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

La cryptographie selon Jules César

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

Rome $\longrightarrow$ Urph

Combien de possibilités ?

$$\begin{aligned} 26! &= 26 \times 25 \times 24 \times ... \times 3 \times 2 \times 1 \\ &= 403\ 291\ 461\ 126\ 605\ 635\ 584\ 000\ 000 \end{aligned}$$

403 quadrillons, 291 trilliards, 461 trillions, 126 billiards, 605 billions, 635 milliards, 584 millions

Est-ce sécuritaire ?

Est-ce sécuritaire ?

Que feriez-vous avec ce message ?

TILUQLIKTCGGLVCSTIEKLTOPTCGTCRLHEGJNLELGGLS
JCGGLLGGLPTCILSJCSMJRUQKRRLLISKTSAKHHLTIKLT
OLIVCLTRLRLSLINLSRLIOGLLSRLSQJVJCGGLMKTQLUJ
GLQGJICHJGLIUQKRRLTQNCRJISQLUJQNLZECLIHJRKLT
QLRSALJRRLZNCSLRHKCIYRTCRDLMKCISLIAKQLILIICH
YVKCACNKIAMKCISNTSKTSHYVKCGJVKTRILIJMMQKAB
LZMKCISGJABLSCVLMLAKQLRLIOGJRCECLIPTLGGLAQL
VJGLHKINLLRSMGLCINLULIRPTCILRKISMJRMGTRRJULR
SKTSEKTQULKCRVLTSEJSCQAKHHLGLRUQJINRRLCUIL
TQRSKTSMQCIALJNLRJHEJRRJNLTQRSKTSHJQPTCRV
LTSJVKCQNLRMJULR

Y a-t-il une façon de décrypter ce message ?

Y a-t-il une façon de décrypter ce message ?

IX^{e} siècle

Abu Yusuf Ya'qub ibn Is-haq ibn as Sabbah ibn Oòmran ibn Ismaïl al-Kindi (pour les intimes : al-Kindi)

Les statistiques !

Al-Kindi (801 - 873)

Distribution des lettres de l'alphabet

E	15,87%	O	5,14%	F	0,95%
A	9,42%	D	3,39%	J	0,89%
I	8,41%	M	3,24%	H	0,77%
S	7,90%	P	2,86%	Z	0,32%
T	7,26%	C	2,64%	X	0,30%
N	7,15%	V	2,15%	Y	0,24%
R	6,46%	Q	1,06%	W	0,00%
U	6,24%	G	1,04%	K	0,00%
L	5,34%	B	1,02%		

	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		0,2	0,4	0,1		0,1	0,3		1,2			0,5	0,2	1,3		0,3		0,9	0,5	0,6	0,6	0,4			0,1	
B	0,1				0,1				0,1			0,2			0,1			0,1								
C	0,2		0,1		1			0,4	0,3			0,1			0,9			0,1	0,1	0,1	0,1					
D	0,4				2,2				0,3						0,2			0,1			0,4					
E	0,5	0,1	1	1	0,7	0,3	0,1		0,2	0,1		1,4	1,1	2,4	0,2	0,8	0,3	1,6	3,1	1,4	0,9	0,2		0,2		0,1
F	0,2				0,1	0,1			0,2			0,1			0,1			0,2								
G	0,1				0,5				0,1			0,1		0,1				0,1			0,1					
H	0,1				0,3				0,1						0,1											
I	0,1		0,2	0,2	0,9	0,1	0,1					0,7	0,4	0,9	0,5	0,1	0,2	0,5	1	1,1		0,1		0,1		
J					0,1																					
K																										
L	1			0,1	2,5				0,5			0,7			0,4				0,1	0,1	0,4					
M	0,6	0,2			1				0,3				0,2		0,2	0,3										
N	0,3		0,6	0,8	1,2	0,1	0,3		0,2			0,1	0,1	0,2	0,4	0,2	0,1		0,8	2	0,1	0,1		0,1		
O			0,1			0,1			0,5			0,3	0,4	1,6		0,2		0,5	0,2	0,1	1,2				0,1	
P	0,8				0,5				0,1			0,4			0,5	0,2		0,5			0,2					
Q																					1,3					
R	0,9		0,3	0,2	2,1		0,1		0,7			0,4	0,1	0,2	0,6	0,1	0,1	0,2	0,4	0,4	0,1	0,1		0,1		
S	0,8	0,1	0,4	0,6	1,6	0,2	0,1		0,6			0,4	0,1	0,1	0,6	0,4	0,4	0,1	0,7	0,6	0,4	0,1		0,1		
T	0,9		0,2	0,5	1,6	0,1			1			0,3		0,1	0,4	0,3	0,2	0,9	0,4	0,3	0,1	0,2				
U	0,2		0,2	0,2	0,9				0,7			0,2	0,1	0,6		0,2		0,9	0,8	0,6				0,2		
V	0,3				0,4				0,2						0,2			0,1								
W																										
X	0,1			0,1												0,2										
Y	0,1				0,1																					
Z																										

UNE GRENOUILLE VIT UN BOEUF QUI LUI SEMBLA DE BELLE TAILLE ELLE QUI N'ETAIT PAS GROSSE EN TOUT COMME UN OEUF ENVIEUSE SE TEND ET S'ENFLE ET SE TRAVAILLE POUR EGALER L'ANIMAL EN GROSSEUR DISANT REGARDEZ BIEN MA SOEUR EST-CE ASSEZ DITES MOI N'Y SUIS-JE POINT ENCORE NENNI M'Y VOICI DONC POINT DU TOUT M'Y VOILA VOUS N'EN APPROCHEZ POINT LA CHETIVE PECORE S'ENFLA SI BIEN QU'ELLE CREVA LE MONDE EST PLEIN DE GENS QUI NE SONT PAS PLUS SAGES TOUT BOURGEOIS VEUT BATIR COMME LES GRANDS SEIGNEURS TOUT PRINCE A DES AMBASSADEURS TOUT MARQUIS VEUT AVOIR DES PAGES

Ce n'est pas infaillible

Augustus dut fournir un travail colossal pour qu'Haig s'inculquât d'un savoir plus satisfaisant. Il s'y adonna non sans application ; mais, tantôt pion, tantôt prof, il accablait l'ignorant garçon d'un discours fort trapu mais surtout fort obscur où il n'y avait jamais lourd à saisir. Haig avalait tout ça, soumis, souriant, sans aucun mauvais vouloir, mais il apparut, moins d'un mois plus tard, qu'à coup sûr s'il avait appris, il n'avait pas compris : nul pour tout savoir touchant aux maths, à la philo, au latin, il avait cinq ou six notions d'anglais, mais pas plus ; quant au français, il s'y donnait plus à fond : il avait, grosso modo, saisi la signification d'accords grammaticaux plus ou moins incongrus ; il distinguait, disons cinq fois sur huit, un son fricatif d'un son labial, un substantif d'un pronom, un nominatif d'un accusatif, un actif d'un passif ou d'un pronominal, un indicatif d'un optatif, un imparfait d'un futur, un attribut d'apposition d'un partitif d'attribution, un ithos d'un pathos, chiasma d'un anticlimax.

Ayant compris qu'il divaguait quand il croyait concourir à la formation d'un grand savant futur, Augustus s'agaçait du pouvoir quasi nul qu'il paraissait avoir sur la vocation du garçon. Puis, modifiant sont tir, il constata, surpris, mais aussitôt ravi, qu'Haig trouvait dans l'art musical un plaisir toujours vrai. On l'avait surpris crachotant dans un tuba dont il tira un son pas tout à fait discordant. Il harmonisait non sans intuition. Il avait surtout pour la chanson un goût distinctif. Il n'oubliait aucun air pourvu qu'on lui jouât ou qu'on lui chantât trois fois.

Augustus, qu'Iturbi jadis honora d'un cours, installa donc aussitôt un piano crapaud (un Graf aux sons parfois nasillards, mais aux accords parfaits, construit pour Brahms qui y composa, dit-on, l'impromptu opus vingt-huit) dans un salon où il y avait aussi un billard (billard sur quoi, on l'a appris jadis, il avait failli raccourcir à coup d'hachoir Haig alors tout bambin).

Georges Pérec (1936 - 1982)

La substitution polyalphabétique

Léon Battista Alberti (1404-1472)

Blaise de Vigenère (1523 - 1596)


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

Exemple

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
D	**E**	**P**	**L**	**A**	**C**	**E**	**Z**	**V**	**O**	**S**	**T**	**R**	**O**	**U**	**P**	**E**	**S**
V	I	R	C	E	V	W	D	X	F	W	M	J	S	W	G	I	L

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
V	**E**	**R**	**S**	**L**	**E**	**N**	**O**	**R**	**D**	**D**	**E**	**M**	**A**	**I**	**N**	**E**	**N**
N	I	T	J	P	X	F	S	T	U	H	X	E	E	K	E	I	G

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
F	**I**	**N**	**D**	**A**	**V**	**A**	**N**	**T**	**M**	**I**	**D**	**I**	**V**	**O**	**U**	**S**	**T**
X	M	P	U	E	O	S	R	V	D	M	W	A	Z	Q	L	W	M

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
R	**O**	**U**	**V**	**E**	**R**	**E**	**Z**	**U**	**N**	**N**	**O**	**U**	**V**	**E**	**A**	**U**	**S**
J	S	W	M	I	K	W	D	W	E	R	H	M	Z	G	R	Y	L

Est-ce sécuritaire ?

Est-ce sécuritaire ?

Regardez bien...

V I R C E V W D X F W M J S W G I L

N I T J P X F S T U H X E E K E I G

X M P U E O S R V D M W A Z Q L W M

J S W M I K W D W E R H M Z G R Y L

L S E B H X E Y P Z X B G R U R P T

V I R C E V W D X F **W M J S W** G I L

N I T J P X F S T U **H X E** E K E I G

X M P U E O S R V D M W A Z Q L **W M**

J S W M I K W D W E R H M Z G R Y L

L S E B **H X E** Y P Z X B G R U R P T

D E P L A C E Z V O **S T R O U** P E S
V I R C E V W D X F **W M J S W** G I L

V E R S L E N O R D **D E M** A I N E N
N I T J P X F S T U **H X E** E K E I G

F I N D A V A N T M I D I V O U **S T**
X M P U E O S R V D M W A Z Q L **W M**

R O U V E R E Z U N N O U V E A U S
J S W M I K W D W E R H M Z G R Y L

T O C K **D E M** U N I T I O N S A L A
L S E B **H X E** Y P Z X B G R U R P T

D E P L A C E Z V O **S T R O U** P E S
V I R C E V W D X F **W M J S W** G I L

V E R S L E N O R D **D E M** A I N E N
N I T J P X F S T U **H X E** E K E I G

F I N D A V A N T M I D I V O U **S T**
X M P U E O S R V D M W A Z Q L **W M**

R O U V E R E Z U N N O U V E A U S
J S W M I K W D W E R H M Z G R Y L

T O C K **D E M** U N I T I O N S A L A
L S E B **H X E** Y P Z X B G R U R P T

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
D	E	P	L	A	C	E	Z	V	O	S	T	R	O	U	P	E	S
V	I	R	C	E	V	W	D	X	F	W	M	J	S	W	G	I	L

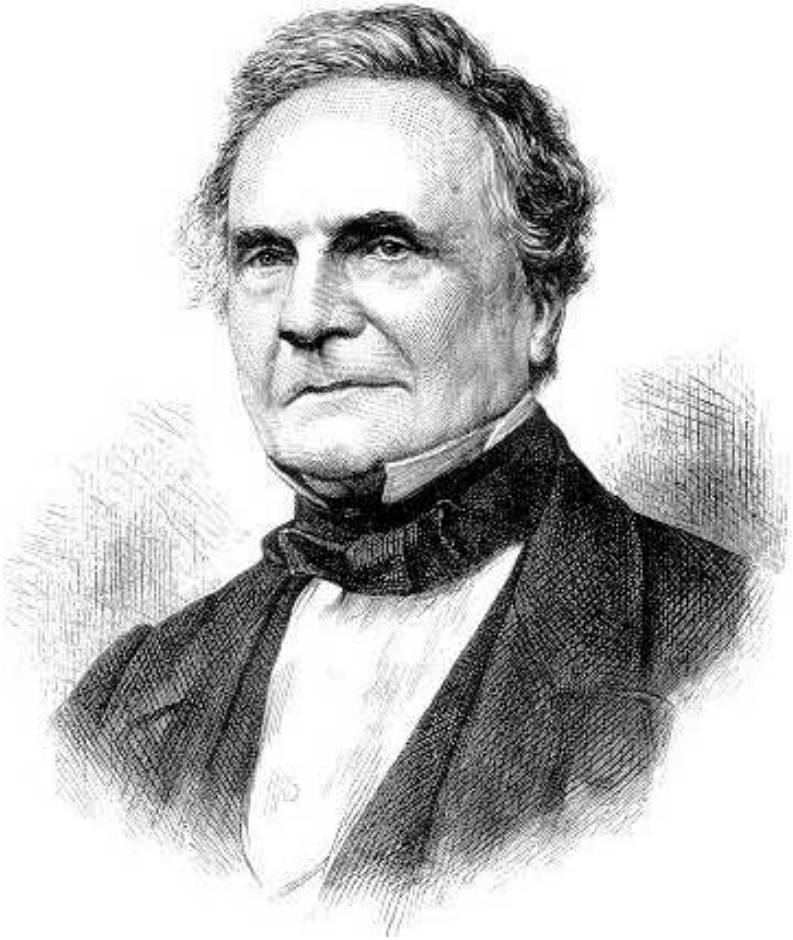
S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
V	E	R	S	L	E	N	O	R	D	D	E	M	A	I	N	E	N
N	I	T	J	P	X	F	S	T	U	H	X	E	E	K	E	I	G

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
F	I	N	D	A	V	A	N	T	M	I	D	I	V	O	U	S	T
X	M	P	U	E	O	S	R	V	D	M	W	A	Z	Q	L	W	M

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

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

L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6
V	I	R	C	E	V	W	D	X	F	W	M	J	S	W	G	I	L
L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6
N	I	T	J	P	X	F	S	T	U	H	X	E	E	K	E	I	G
L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6
X	M	P	U	E	O	S	R	V	D	M	W	A	Z	Q	L	W	M
L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6
J	S	W	M	I	K	W	D	W	E	R	H	M	Z	G	R	Y	L
L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6	L_1	L_2	L_3	L_4	L_5	L_6
L	S	E	B	H	X	E	Y	P	Z	X	B	G	R	U	R	P	T



Charles Babbage (1791 - 1871)

La morale de l'histoire

Les mathématiques au service de la cryptographie et de l'informatique

La méthode RSA

Les mathématiques au service de la cryptographie et de l'informatique

La méthode RSA

Pour comprendre RSA, nous avons besoin de trois résultats mathématiques.

Premier résultat

Quelle est la factorisation du nombre suivant ?

$$182670290573621134331325592091141224133279168 9$$

$$1826702905736211343313255920911412241332791689$$
$$= 124218091799 \cdot 225899827463 \cdot 233826604493 \cdot 278402572429$$

En **pratique**, c'est impossible de factoriser (rapidement) un grand nombre.

Deuxième résultat

Trouver une solution à l'équation

$$1978x - 2007y = 1$$

telle que $x, y \in \mathbf{Z}$.

$$2007 \quad = \quad 1 \cdot 1978 + 29$$

$$2007 = 1 \cdot 1978 + 29$$

$$1978 = 68 \cdot 29 + 6$$

$$
\begin{aligned}
2007 &= 1 \cdot 1978 + 29 \\
1978 &= 68 \cdot 29 + 6 \\
29 &= 4 \cdot 6 + 5
\end{aligned}
$$

$$
\begin{aligned}
2007 &= 1 \cdot 1978 + 29 \\
1978 &= 68 \cdot 29 + 6 \\
29 &= 4 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1
\end{aligned}
$$

$$\begin{array}{rcl} 2007 & = & 1 \cdot 1978 + 29 \\ 1978 & = & 68 \cdot 29 + 6 \\ 29 & = & 4 \cdot 6 + 5 \\ 6 & = & 1 \cdot 5 + 1 \end{array} \Bigg\| \quad 1 \;=\; 6 - 5$$

$$
\begin{aligned}
2007 &= 1 \cdot 1978 + 29 \\
1978 &= 68 \cdot 29 + 6 \\
29 &= 4 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1
\end{aligned}
\quad \Bigg\| \quad
\begin{aligned}
&\\
&\\
1 &= 6 - (29 - 4 \cdot 6) \\
1 &= 6 - 5
\end{aligned}
$$

$$
\begin{array}{rcl}
2007 & = & 1 \cdot 1978 + 29 \\
1978 & = & 68 \cdot 29 + 6 \\
29 & = & 4 \cdot 6 + 5 \\
6 & = & 1 \cdot 5 + 1
\end{array}
\quad \Bigg\| \quad
\begin{array}{rcl}
1 & = & 5 \cdot 6 - 29 \\
1 & = & 6 - (29 - 4 \cdot 6) \\
1 & = & 6 - 5
\end{array}
$$

$$
\begin{array}{rcl}
2007 & = & 1 \cdot 1978 + 29 \\
\\
1978 & = & 68 \cdot 29 + 6 \\
\\
29 & = & 4 \cdot 6 + 5 \\
\\
6 & = & 1 \cdot 5 + 1
\end{array}
\quad \Bigg\| \quad
\begin{array}{rcl}
\\
\\
1 & = & 5 \cdot (1978 - 68 \cdot 29) - 29 \\
1 & = & 5 \cdot 6 - 29 \\
1 & = & 6 - (29 - 4 \cdot 6) \\
\\
1 & = & 6 - 5
\end{array}
$$

$$
\begin{array}{rcl}
2007 & = & 1 \cdot 1978 + 29 \\
 & & \\
1978 & = & 68 \cdot 29 + 6 \\
 & & \\
29 & = & 4 \cdot 6 + 5 \\
 & & \\
6 & = & 1 \cdot 5 + 1
\end{array}
\quad \Bigg\| \quad
\begin{array}{rcl}
 & & \\
1 & = & 5 \cdot 1978 - 341 \cdot 29 \\
1 & = & 5 \cdot (1978 - 68 \cdot 29) - 29 \\
1 & = & 5 \cdot 6 - 29 \\
1 & = & 6 - (29 - 4 \cdot 6) \\
 & & \\
1 & = & 6 - 5
\end{array}
$$

$$
\begin{array}{rcl}
2007 &=& 1 \cdot 1978 + 29 \\
1978 &=& 68 \cdot 29 + 6 \\
29 &=& 4 \cdot 6 + 5 \\
6 &=& 1 \cdot 5 + 1
\end{array}
\quad\Bigg\|\quad
\begin{array}{rcl}
1 &=& 5 \cdot 1978 - 341 \cdot (2007 - 1978) \\
1 &=& 5 \cdot 1978 - 341 \cdot 29 \\
1 &=& 5 \cdot (1978 - 68 \cdot 29) - 29 \\
1 &=& 5 \cdot 6 - 29 \\
1 &=& 6 - (29 - 4 \cdot 6) \\
1 &=& 6 - 5
\end{array}
$$

$$
\begin{aligned}
2007 &= 1 \cdot 1978 + 29 \\
1978 &= 68 \cdot 29 + 6 \\
29 &= 4 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1
\end{aligned}
\qquad \Vert \qquad
\begin{aligned}
1 &= 346 \cdot 1978 - 341 \cdot 2007 \\
1 &= 5 \cdot 1978 - 341 \cdot (2007 - 1978) \\
1 &= 5 \cdot 1978 - 341 \cdot 29 \\
1 &= 5 \cdot (1978 - 68 \cdot 29) - 29 \\
1 &= 5 \cdot 6 - 29 \\
1 &= 6 - (29 - 4 \cdot 6) \\
1 &= 6 - 5
\end{aligned}
$$

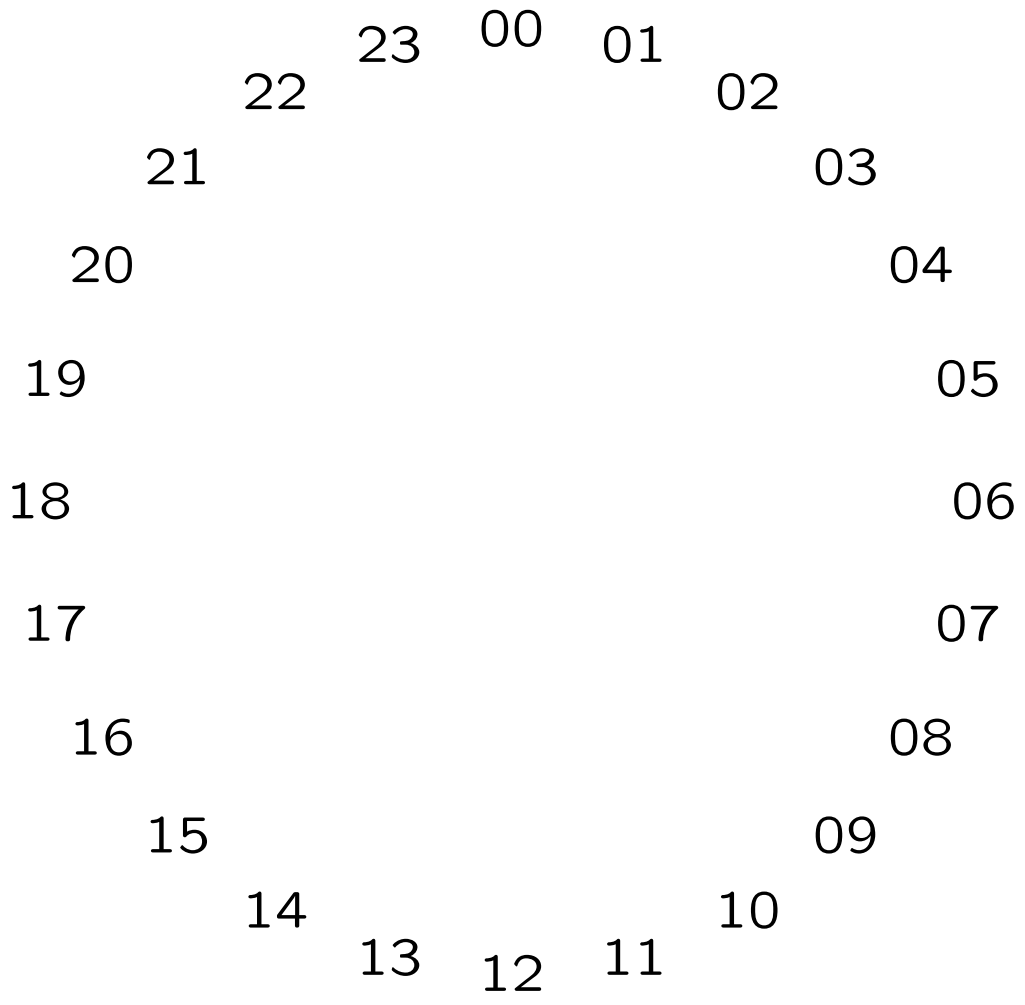
$$
\begin{array}{rcl}
2007 &=& 1 \cdot 1978 + 29 \\
1978 &=& 68 \cdot 29 + 6 \\
29 &=& 4 \cdot 6 + 5 \\
6 &=& 1 \cdot 5 + 1
\end{array}
\quad \Vert \quad
\begin{array}{rcl}
1 &=& 346 \cdot 1978 - 341 \cdot 2007 \\
1 &=& 5 \cdot 1978 - 341 \cdot (2007 - 1978) \\
1 &=& 5 \cdot 1978 - 341 \cdot 29 \\
1 &=& 5 \cdot (1978 - 68 \cdot 29) - 29 \\
1 &=& 5 \cdot 6 - 29 \\
1 &=& 6 - (29 - 4 \cdot 6) \\
\\
1 &=& 6 - 5
\end{array}
$$

Donc $(x, y) = (346, 341)$ est une solution de $1978x - 2007y = 1$ où $x, y \in \mathbf{Z}$.

Ce truc fonctionne toujours, pourvu que les deux nombres (ici 1978 et 2007) n'aient pas de diviseur commun.

Troisième résultat

Arithmétique circulaire



« Notation scientifique »

$$25 \equiv 1 \pmod{24}$$

$$24 \equiv 0 \pmod{24}$$

$$36 \equiv 12 \pmod{24}$$

$$-10 \equiv 14 \pmod{24}$$

« Notation et calcul scientifiques »

$$25 \equiv 1 \pmod{24}$$

$$17 + 13 \equiv 6 \pmod{24}$$

$$7 + 7 + 7 + 7 + 7 \equiv 5 \cdot 7 \equiv 11 \pmod{24}$$

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \equiv 2^6 \equiv 16 \pmod{24}$$

Si x est tel que $x \equiv 0 \pmod{24}$, que pouvons-nous dire de x ?

Le théorème d'Euler

Théorème 1 (Euler) *Soient p et q deux nombres premiers et a un entier tels que a n'est pas divisible par p ni par q. Alors*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq},$$

autrement dit $a^{(p-1)(q-1)} - 1$ est divisible par pq.

Le théorème d'Euler

Théorème 2 (Euler) *Soient p et q deux nombres premiers et a un entier tels que a n'est pas divisible par p ni par q. Alors*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq},$$

autrement dit $a^{(p-1)(q-1)} - 1$ est divisible par pq.

Exemples

$9^{(2-1)(5-1)} - 1$ est divisible par $2 \cdot 5$

$4^{(3-1)(7-1)} - 1$ est divisible par $3 \cdot 7$

$2^{(5-1)(7-1)} - 1$ est divisible par $5 \cdot 7$

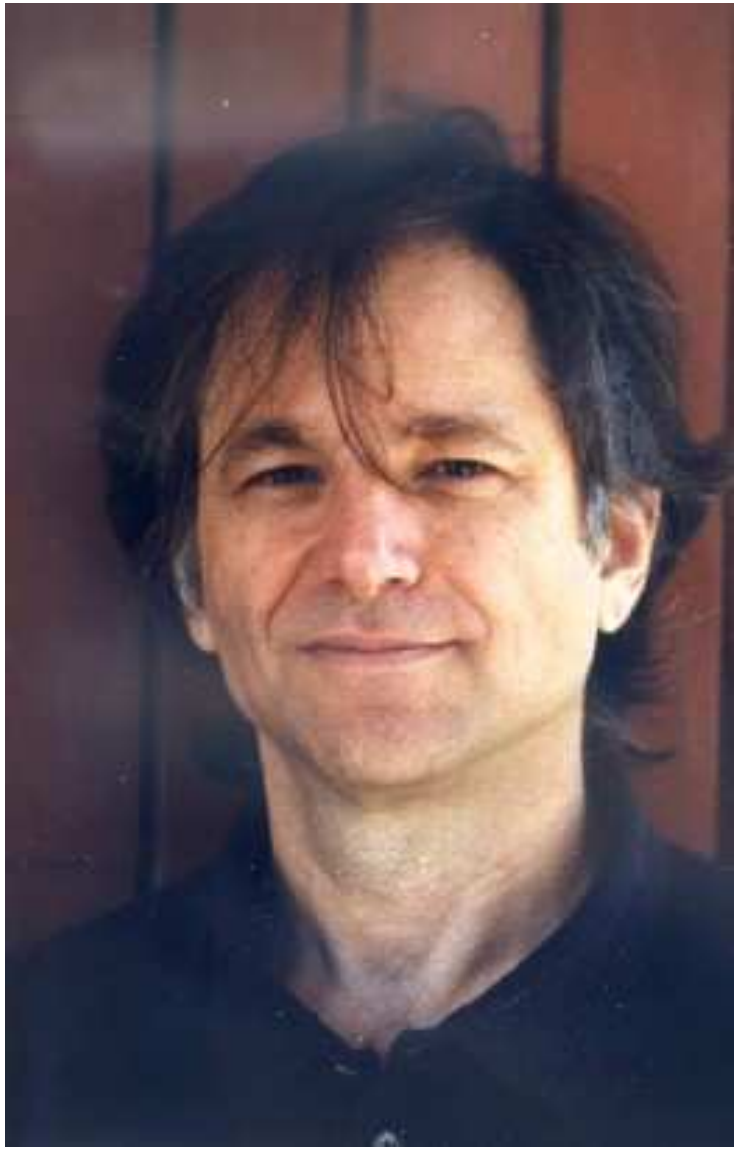
Leonhard Euler (1707-1783)

RSA

L'algorithme de cryptographie RSA a été mis au point en 1977 par Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman.

Ron **R**ivest (né en 1947 à New-York (États-Unis))

Adi **S**hamir (né en 1952 à Tel Aviv (Israël))



Leonard **A**dleman (né en 1945 en Californie (États-Unis))

Comment fonctionne l'algorithme ?

1. D'abord, le bottin suivant est rendu public.

	n	a
Lily	3452346509	17
Marco	5078078569	13
Sophie	2418737527	11
Jean	4730645749	17
Mario	1651907011	23
Lyne	8245778143	19

Le nombre a n'a pas de diviseur commun avec $p-1$ ni avec $q-1$.
Chacun de ces nombres n est de la forme $n = pq$, pour des nombres premiers p et q. Seul le propriétaire d'un n connaît son p et son q. Pour les autres, c'est impossible à trouver parce que...

2. À titre d'exemple, voyons ce que Sophie a entre les mains. Puisqu'elle connaît p et q tels que $n = pq$, elle connaît aussi x et y tels que $ax - (p-1)(q-1)y = 1$ parce que...

   Dans son cas, $x = 1539134011$ et $y = 7$.

3. Si nous décidons de lui envoyer le message « Salut », nous utilisons la table suivante.

A $\rightarrow$ 01	J $\rightarrow$ 10	S $\rightarrow$ 19
B $\rightarrow$ 02	K $\rightarrow$ 11	T $\rightarrow$ 20
C $\rightarrow$ 03	L $\rightarrow$ 12	U $\rightarrow$ 21
D $\rightarrow$ 04	M $\rightarrow$ 13	V $\rightarrow$ 22
E $\rightarrow$ 05	N $\rightarrow$ 14	W $\rightarrow$ 23
F $\rightarrow$ 06	O $\rightarrow$ 15	X $\rightarrow$ 24
G $\rightarrow$ 07	P $\rightarrow$ 16	Y $\rightarrow$ 25
H $\rightarrow$ 08	Q $\rightarrow$ 17	Z $\rightarrow$ 26
I $\rightarrow$ 09	R $\rightarrow$ 18	espace $\rightarrow$ 27

Le message est donc représenté par le nombre $M = 1901122120$.

Nous calculons

$$\begin{aligned} C &\equiv M^a \pmod{2418737527} \\ &\equiv 1901122120^{11} \pmod{2418737527} \\ &\equiv 250061500 \pmod{2418737527} \end{aligned}$$

Nous envoyons C à Sophie.

4. Que fait Sophie lorsqu'elle reçoit C ? Elle calcule

$$\begin{aligned} C^x &\equiv 250061500^{1539134011} \pmod{2418737527} \\ &\equiv 1901122120 \pmod{2418737527} \\ &\equiv M \pmod{2418737527} \end{aligned}$$

Elle retrouve le message !

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$C^x \equiv (M^a)^x \pmod{n}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned} C^x &\equiv (M^a)^x \pmod{n} \\ &\equiv M^{ax} \pmod{n} \end{aligned}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned} C^x &\equiv (M^a)^x \pmod{n} \\ &\equiv M^{ax} \pmod{n} \\ &\equiv M^{(ax-1)+1} \pmod{n} \end{aligned}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned} C^x &\equiv (M^a)^x \pmod{n} \\ &\equiv M^{ax} \pmod{n} \\ &\equiv M^{(ax-1)+1} \pmod{n} \\ &\equiv M^{ax-1} \cdot M^1 \pmod{n} \end{aligned}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned} C^x &\equiv (M^a)^x \pmod{n} \\ &\equiv M^{ax} \pmod{n} \\ &\equiv M^{(ax-1)+1} \pmod{n} \\ &\equiv M^{ax-1} \cdot M^1 \pmod{n} \\ &\equiv M^{ax-1} \cdot M \pmod{n} \end{aligned}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned} C^x &\equiv (M^a)^x \pmod{n} \\ &\equiv M^{ax} \pmod{n} \\ &\equiv M^{(ax-1)+1} \pmod{n} \\ &\equiv M^{ax-1} \cdot M^1 \pmod{n} \\ &\equiv M^{ax-1} \cdot M \pmod{n} \\ &\equiv M^{(p-1)(q-1)y} \cdot M \pmod{n} \end{aligned}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned}
C^x &\equiv (M^a)^x \pmod{n} \\
&\equiv M^{ax} \pmod{n} \\
&\equiv M^{(ax-1)+1} \pmod{n} \\
&\equiv M^{ax-1} \cdot M^1 \pmod{n} \\
&\equiv M^{ax-1} \cdot M \pmod{n} \\
&\equiv M^{(p-1)(q-1)y} \cdot M \pmod{n} \\
&\equiv (M^y)^{(p-1)(q-1)} \cdot M \pmod{n}
\end{aligned}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned}
C^x &\equiv (M^a)^x \pmod{n} \\
&\equiv M^{ax} \pmod{n} \\
&\equiv M^{(ax-1)+1} \pmod{n} \\
&\equiv M^{ax-1} \cdot M^1 \pmod{n} \\
&\equiv M^{ax-1} \cdot M \pmod{n} \\
&\equiv M^{(p-1)(q-1)y} \cdot M \pmod{n} \\
&\equiv (M^y)^{(p-1)(q-1)} \cdot M \pmod{n} \\
&\equiv 1 \cdot M \pmod{n}
\end{aligned}$$

Pourquoi ça fonctionne ?

Le message codé est $C \equiv M^a \pmod{n}$. Lorsque Sophie calcule $C^x \pmod{n}$, elle obtient le résultat suivant.

$$\begin{aligned}
C^x &\equiv (M^a)^x \pmod{n} \\
&\equiv M^{ax} \pmod{n} \\
&\equiv M^{(ax-1)+1} \pmod{n} \\
&\equiv M^{ax-1} \cdot M^1 \pmod{n} \\
&\equiv M^{ax-1} \cdot M \pmod{n} \\
&\equiv M^{(p-1)(q-1)y} \cdot M \pmod{n} \\
&\equiv (M^y)^{(p-1)(q-1)} \cdot M \pmod{n} \\
&\equiv 1 \cdot M \pmod{n} \\
&\equiv M \pmod{n}
\end{aligned}$$

Conclusion