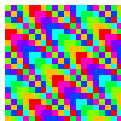


MATHÉMATIQUES ET CRYPTOGRAPHIE

Michel Rigo

Département de Mathématiques, Université de Liège
<http://www.discmath.ulg.ac.be/>



CRYPTOGRAPHIE. N. F.

Art d'écrire en chiffres ou d'une façon secrète quelconque.

Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données, afin d'en préserver la confidentialité et l'authenticité.

EXEMPLE

“Mon numéro de carte VISA est le 1234-3552-1209-7633”



“XFHEBBCASKOIUUSBCKKQHDGGDDSJQQIEUEU”

Applications

- ▶ Armée, gouvernement
- ▶ Banques, transactions bancaires, bancontact, ...
- ▶ Internet, paiement en ligne par carte de crédit, ...
- ▶ Vote électronique
- ▶ GSM (identification, code PIN)
- ▶ Télévision payante (à la carte)
- ▶ Signatures électroniques, recommandés électroniques, ...
- ▶ Mots de passe informatiques, ...

COMPTER MODULO...



“ 17 heures = 5 heures de l'après-midi ! ”

COMPTER MODULO...



“ 17 heures = 5 heures de l'après-midi ! ”

$$17=5\dots$$

DÉFINITION

Deux nombres x et y sont **congrus modulo 12** s'ils ont même reste après division par 12. (Ou si leur différence est un multiple de 12.)

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59
⋮											

On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



On peut alors calculer modulo 12

17	$=$	5	$(\text{mod } 12)$	car	$17 = 1.12 + 5$
$7 + 9$	$=$	4	$(\text{mod } 12)$	car	$16 = 1.12 + 4$
3.11	$=$	9	$(\text{mod } 12)$	car	$33 = 2.12 + 9$
5^2	$=$	1	$(\text{mod } 12)$	car	$25 = 2.12 + 1$
-3	$=$	9	$(\text{mod } 12)$	car	$-3 = (-1).12 + 9$



UN PREMIER CRYPTOSYSTÈME

On peut compter modulo 2,3,4,..., **26**, ..., 723, ...

$67 = 7 \pmod{20}$, $67 = 4 \pmod{21}$, $12+19 = 7 \pmod{24}$, ...

A	B	C	...	X	Y	Z
0	1	2	...	23	24	25

CRYPTOSYSTÈME DE JULES CESAR

BONJOUR

1, 14, 13, 9, 14, 20, 17

↓ +3

4, 17, 16, 12, 17, 23, 20

ERQMRXU

UN PREMIER CRYPTOSYSTÈME

On peut compter modulo 2,3,4,..., **26**, ..., 723, ...

$67 = 7 \pmod{20}$, $67 = 4 \pmod{21}$, $12+19 = 7 \pmod{24}$, ...

A	B	C	...	X	Y	Z
0	1	2	...	23	24	25

CRYPTOSYSTÈME DE JULES CESAR

BONJOUR

1, 14, 13, 9, 14, 20, 17

↓ +3

4, 17, 16, 12, 17, 23, 20

ERQMRXU

UN PREMIER CRYPTOSYSTÈME

On peut compter modulo 2,3,4,..., **26**, ..., 723, ...

$67 = 7 \pmod{20}$, $67 = 4 \pmod{21}$, $12+19 = 7 \pmod{24}$, ...

A	B	C	...	X	Y	Z
0	1	2	...	23	24	25

CRYPTOSYSTÈME DE JULES CESAR

BONJOUR

1, 14, 13, 9, 14, 20, 17

↓ +3

4, 17, 16, 12, 17, 23, 20

ERQMRXU

UN PREMIER CRYPTOSYSTÈME

On peut compter modulo 2,3,4,..., 26, ..., 723, ...

$67 = 7 \pmod{20}$, $67 = 4 \pmod{21}$, $12+19 = 7 \pmod{24}$, ...

A	B	C	...	X	Y	Z
0	1	2	...	23	24	25

CRYPTOSYSTÈME DE JULES CESAR

BONJOUR

1, 14, 13, 9, 14, 20, 17

↓ +3

4, 17, 16, 12, 17, 23, 20

ERQMRXU

UN PREMIER CRYPTOSYSTÈME

On peut compter modulo 2,3,4,..., 26, ..., 723, ...

$67 = 7 \pmod{20}$, $67 = 4 \pmod{21}$, $12+19 = 7 \pmod{24}$, ...

A	B	C	...	X	Y	Z
0	1	2	...	23	24	25

CRYPTOSYSTÈME DE JULES CESAR

BONJOUR

1, 14, 13, 9, 14, 20, 17

↓ +3

4, 17, 16, 12, 17, 23, 20

ERQMRXU

UN PREMIER CRYPTOSYSTÈME

On peut compter modulo 2,3,4,..., 26, ..., 723, ...

$67 = 7 \pmod{20}$, $67 = 4 \pmod{21}$, $12+19 = 7 \pmod{24}$, ...

A	B	C	...	X	Y	Z
0	1	2	...	23	24	25

CRYPTOSYSTÈME DE JULES CESAR

BONJOUR

1, 14, 13, 9, 14, 20, 17

↓ +3

4, 17, 16, 12, 17, 23, 20

ERQMRXU



HAL
IBM



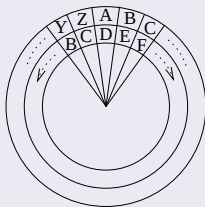
HAL
IBM

REMARQUE

Le cryptosystème de J.C. est un cryptosystème à **clé secrète**.

DES VARIANTES

$x \mapsto x + k \pmod{26}$, $k = 1, 2, \dots, 25$



D'AUTRES VARIANTES ?

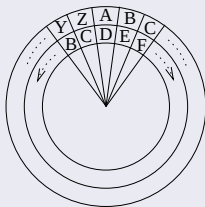
$x \mapsto k.x \pmod{26} \dots$

REMARQUE

Le cryptosystème de J.C. est un cryptosystème à **clé secrète**.

DES VARIANTES

$x \mapsto x + k \pmod{26}$, $k = 1, 2, \dots, 25$



D'AUTRES VARIANTES ?

$x \mapsto k.x \pmod{26} \dots$

$$x \mapsto 5x \pmod{26}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
0	5	10	15	20	25	4	9	14	19	24	3	8
A	F	K	P	U	Z	E	J	O	T	Y	D	I

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
13	18	23	2	7	12	17	22	1	6	11	16	21
N	S	X	C	H	M	R	W	B	G	L	Q	V

BONJOUR $\longrightarrow$ FSNTSWH

$$x \mapsto 5x \pmod{26}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
0	5	10	15	20	25	4	9	14	19	24	3	8
A	F	K	P	U	Z	E	J	O	T	Y	D	I

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
13	18	23	2	7	12	17	22	1	6	11	16	21
N	S	X	C	H	M	R	W	B	G	L	Q	V

BONJOUR $\longrightarrow$ FSNTSWH

$$x \mapsto 5x \pmod{26}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
0	5	10	15	20	25	4	9	14	19	24	3	8
A	F	K	P	U	Z	E	J	O	T	Y	D	I

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
13	18	23	2	7	12	17	22	1	6	11	16	21
N	S	X	C	H	M	R	W	B	G	L	Q	V

BONJOUR $\longrightarrow$ FSNTSWH

$$x \mapsto 2 \cdot x \pmod{26}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	2	4	6	8	10	12	14	16	18	20	22	24	0
A	C	E	G	I	K	M	O	Q	S	U	W	Y	A

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25
2	4	6	8	10	12	14	16	18	20	22	24
C	E	G	I	K	M	O	Q	S	U	W	Y

$$\text{OUI} \rightarrow 14, 20, 8 \xrightarrow{\times 2} 2, 14, 16 \rightarrow \text{COQ} \rightarrow \left\{ \begin{array}{l|l} \text{OUI} & \text{BUI} \\ \text{OUV} & \text{BUV} \\ \text{OHI} & \text{BHI} \\ \text{OHV} & \text{BHV} \end{array} \right.$$

$$x \mapsto 2x \pmod{26}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	2	4	6	8	10	12	14	16	18	20	22	24	0
A	C	E	G	I	K	M	O	Q	S	U	W	Y	A

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25
2	4	6	8	10	12	14	16	18	20	22	24
C	E	G	I	K	M	O	Q	S	U	W	Y

$$\text{OUI} \rightarrow 14, 20, 8 \xrightarrow{\times 2} 2, 14, 16 \rightarrow \text{COQ} \rightarrow \left\{ \begin{array}{l|l} \text{OUI} & \text{BUI} \\ \text{OUV} & \text{BUV} \\ \text{OHI} & \text{BHI} \\ \text{OHV} & \text{BHV} \end{array} \right.$$

$$x \mapsto 2x \pmod{26}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	2	4	6	8	10	12	14	16	18	20	22	24	0
A	C	E	G	I	K	M	O	Q	S	U	W	Y	A

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25
2	4	6	8	10	12	14	16	18	20	22	24
C	E	G	I	K	M	O	Q	S	U	W	Y

$$\text{OUI} \rightarrow 14, 20, 8 \xrightarrow{\times 2} 2, 14, 16 \rightarrow \text{COQ} \rightarrow \left\{ \begin{array}{l|l} \text{OUI} & \text{BUI} \\ \text{OUV} & \text{BUV} \\ \text{OHI} & \text{BHI} \\ \text{OHV} & \text{BHV} \end{array} \right.$$

Notion mathématique d'inverse...

THÉORÈME

x possède un inverse modulo m , i.e, $x.y = 1 \pmod{m}$,
si et seulement si x est premier avec m .

COROLLAIRE

Les “bons” multiplicateurs (modulo 26) sont

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14,

15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25

CODAGE PAR BLOCS



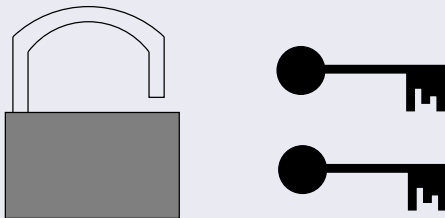
AA	AB	AC	...	AX	AY	AZ
0	1	2	...	23	24	25
BA	BB	BC	...	BX	BY	BZ
26	27	28	...	49	50	51
⋮						⋮
ZA	ZB	ZC	...	ZX	ZY	ZZ
650	651	652	...	673	674	675

modulo $26^2 = 676$

CLÉ SECRÈTE VS. CLÉ PUBLIQUE

CRYPTOSYSTÈME À CLÉ SECRÈTE

Alice & Bob : un jeu de 2 clés identiques

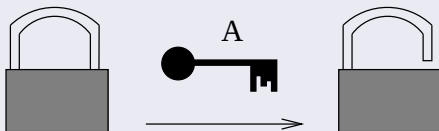
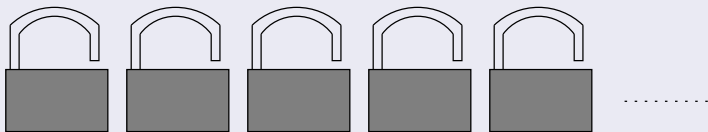


INCONVÉNIENT

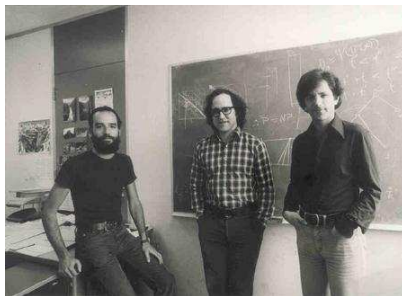
Alice & Bob doivent échanger la clé. . .

CRYPTOSYSTÈME À CLÉ PUBLIQUE

Alice produit des cadenas qu'elle seule pourra ouvrir !



Le RSA est un exemple de cryptosystème à clé publique



Ron Rivest, Adi Shamir et Leonard Adleman (1977)

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

LES NOMBRES PREMIERS

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE

Tout nombre entier se décompose de manière unique (à l'ordre des facteurs près) comme produit de nombres premiers.



$$84 = 2^2 \cdot 3 \cdot 7$$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131,
137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193,
197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263,
269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337,
347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, ...

ALICE CONSTRUIT “SON” RSA

- ▶ Alice choisit p et q .
- ▶ Elle calcule le produit $n = p \cdot q$
- ▶ Elle calcule $\varphi(n) = (p - 1) \cdot (q - 1)$
- ▶ Alice choisit e et d tels que $d \cdot e = 1 \pmod{\varphi(n)}$. Pour ce faire, elle choisit e tel que

$$1 < e < \varphi(n) \quad \text{et} \quad \text{pgcd}(e, \varphi(n)) = 1.$$

$$y = x^e \pmod{n}$$

$$y^d \pmod{n} = x$$

$$p_{1100} \times p_{1000}$$

$$8831 \times 7919 = ?$$

$$\begin{array}{r}
 8831 \\
 \times 7919 \\
 \hline
 79479 \\
 8831 \\
 79479 \\
 61817 \\
 \hline
 69932689
 \end{array}$$

$$p_{1100} \times p_{1000}$$

$$8831 \times 7919 = ?$$

$$\begin{array}{r}
 8 8 3 1 \\
 7 9 1 9 \\
 \hline
 7 9 4 7 9 \\
 8 8 3 1 \\
 7 9 4 7 9 \\
 6 1 8 1 7 \\
 \hline
 6 9 9 3 2 6 8 9
 \end{array}$$

$$103724581 = ? \times ?$$

divisible par 2 ? NON

divisible par 3 ? NON

divisible par 5 ? NON

divisible par 7 ? NON

⋮

divisible par 9733 ? OUI !

$$103724581 = 9733 \times 10657 \quad p_{1200} \times p_{1300}$$

$$103724581 = ? \times ?$$

divisible par 2 ? **NON**

divisible par 3 ? **NON**

divisible par 5 ? **NON**

divisible par 7 ? **NON**

⋮

divisible par 9733 ? **OUI !**

$$103724581 = 9733 \times 10657 \quad p_{1200} \times p_{1300}$$

$$103724581 = ? \times ?$$

divisible par 2 ? **NON**

divisible par 3 ? **NON**

divisible par 5 ? **NON**

divisible par 7 ? **NON**

⋮

divisible par 9733 ? **OUI !**

$$103724581 = 9733 \times 10657 \quad p_{1200} \times p_{1300}$$

$$103724581 = ? \times ?$$

divisible par 2 ? **NON**

divisible par 3 ? **NON**

divisible par 5 ? **NON**

divisible par 7 ? **NON**

⋮

divisible par 9733 ? **OUI!**

$$103724581 = 9733 \times 10657 \quad p_{1200} \times p_{1300}$$

$$103724581 = ? \times ?$$

divisible par 2 ? **NON**

divisible par 3 ? **NON**

divisible par 5 ? **NON**

divisible par 7 ? **NON**

⋮

divisible par 9733 ? **OUI !**

$$103724581 = 9733 \times 10657 \quad p_{1200} \times p_{1300}$$

$$103724581 = ? \times ?$$

divisible par 2 ? **NON**

divisible par 3 ? **NON**

divisible par 5 ? **NON**

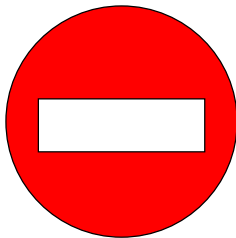
divisible par 7 ? **NON**

⋮

divisible par 9733 ? **OUI!**

$$103724581 = 9733 \times 10657 \quad p_{1200} \times p_{1300}$$

Principe d'une fonction à sens unique



Si on dispose de n et e , il est (supposé) très difficile de

- ▶ retrouver p et q
- ▶ retrouver d .

FONCTION INDICATRICE D'EULER

$\varphi(n)$ compte le nombre de nombres $< n$ et premiers avec n .

$$\begin{array}{l} \varphi(2) = 1 \mid 1 \\ \varphi(3) = 2 \mid 1, 2 \\ \varphi(4) = 2 \mid 1, 3 \end{array} \parallel \begin{array}{l} \varphi(5) = 4 \mid 1, 2, 3, 4 \\ \varphi(6) = 2 \mid 1, 5 \\ \varphi(7) = 6 \mid 1, 2, 3, 4, 5, 6 \end{array}$$

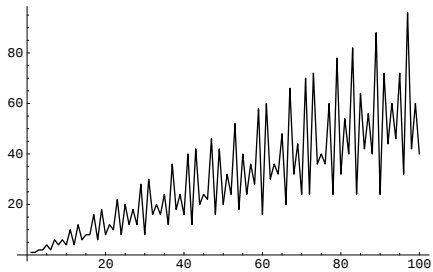
THÉORÈME D'EULER

Soient $n \geq 2$ un entier et a un entier premier avec n , alors

$$a^{\varphi(n)} = 1 \pmod{n}.$$

En effet, si x est premier avec n , alors

$$y^d = x^{ed} = x^{1+k\varphi(n)} = x \cdot x^{k\varphi(n)} = x \cdot (x^{\varphi(n)})^k = x \cdot 1 \pmod{n}.$$



UN MINI RSA

$$p = 11, q = 23, n = p.q = 253, e = 3.$$

Puisque $220 = 3.73 + 1$, $3.(-73) + 220 = 1$ et

$$d = -73 = 147 \pmod{220}.$$

Alice publie $k = (3, 253)$.

Si Bob veut envoyer le texte clair $x = 165$ à Alice, il calcule

$$y = 165^3 \pmod{253} = 110.$$

Si Alice reçoit le message $y = 110$, il lui suffit de calculer

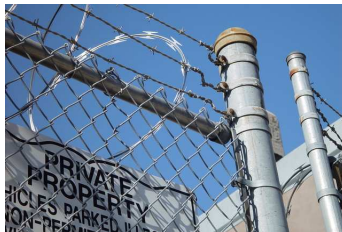
$$110^{147} = 165 \pmod{253}.$$

LE RSA EST-IL SÛR ?

$$p, q \sim 2^{512}$$

$$\begin{array}{ccc} p, q & \longrightarrow & n = p \times q \\ n & \not\longrightarrow & p, q \end{array}$$

facile
supposé difficile



*RSA Challenge number RSA-640, factorisé le 5/11/2005
plusieurs mois sur des centaines d'ordinateurs en réseau !*

3107418240490043721350750035888567930037346022842727545720
1619488232064405180815045563468296717232867824379162728380
3341547107310850191954852900733772482278352574238645401469
1736602477652346609

LE RSA EST-IL SÛR ?

$$p, q \sim 2^{512}$$

$$\begin{array}{ccc} p, q & \longrightarrow & n = p \times q \\ n & \not\longrightarrow & p, q \end{array}$$

facile
supposé difficile



RSA Challenge number RSA-640, factorisé le 5/11/2005
plusieurs mois sur des centaines d'ordinateurs en réseau !

3107418240490043721350750035888567930037346022842727545720
1619488232064405180815045563468296717232867824379162728380
3341547107310850191954852900733772482278352574238645401469
1736602477652346609

FACTORISATION NAÏVE

$$n \sim 2^{1024} \sim 10^{300}$$

tous les nombres impairs jusqu'à $\sqrt{n} \sim 10^{150}$

Supposons tester 10^{10} diviseurs à la seconde...

Temps nécessaire : $\frac{1}{2}10^{140} \sim 5.10^{139}$ secondes !

Age de l'univers : 15.10^9 années $\sim 5.10^{17}$ secondes !

REMARQUE

La sécurité du RSA dépend donc des avancées de la recherche en mathématique.

REMARQUE

La construction même du RSA repose sur un théorème (Euler) de théorie des nombres.

pictures taken from [http ://www.morguefile.com/](http://www.morguefile.com/) id : 142947, 135868, 101161, 142562, 139702