

$$\begin{array}{r} 43 \\ - 37 \\ \hline 301 \\ - 129 \\ \hline 1581 \end{array}$$

$$\begin{array}{r} 7 \\ \times 7 \\ \hline 1 \end{array}$$

cible d'Eratosthène

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	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

25 nb premiers ≤ 100
(26 avec le 1)

→ le nb de nb 1^{er} est infini

Car $\forall n \in \mathbb{N}$; soit $p = n! + 1$ ($n \geq 1$)

$$n! + 1 = n(n-1)! + 1 \not\equiv 0 \pmod{n+1}$$

$$p > n$$

or p n'est pas divisible par $2, 3, 4, \dots, n$

donc soit p est 1^{er} avec $p > n$

Soit p n'est pas 1^{er}, donc divisible par 1
 $nb 1^{er} > n$

comment trouver un nombre 1^{er}?

Euler $f(n) = n^2 + n + 41$ avec $0 \leq n \leq 39$ est 1^{er}

$n \rightarrow 10\ 000\ 000$ 1/3 des $f(n)$ sont 1^{er}

Mersenne Abbe français du début du 17^e

$$M_k = 2^p - 1 \quad \text{avec } p \text{ premier}$$

M_k est premier pour $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$
~~25 864 351~~

18/02/2005	$M_{42} = 2^{25\ 964\ 951} - 1$	+ 816 230 chiffres
24/12/2005	$M_{43} = 2^{30402457} - 1$	8 152 052
4/08/2006	$M_{44} = 2^{32582657} - 1$	9 808 358
23/08/2008	$M_{46} = 2^{43\ 112\ 609} - 1$	12 978 109
10/09/2008	$M_{45} = 2^{37\ 156\ 667} - 1$	11 185 275

$f(n) = 2 + (2(n!) [n+1])$ génère tous les premiers dans l'ordre

$$f(1) = 2 + (2 \cdot 2! [3]) = 2 \text{ premier}$$

$$f(2) = 2 + (2 \cdot 3! [4]) = 3 \text{ premier}$$

$$f(3) = 2 + (2 \cdot 3! [4]) = 2$$

$$f(4) = 2 + (2 \cdot 4! [5]) = 5 \text{ premier}$$

GIMPS

VI.6 Factorisation première

Soit $a \geq 2$ $a \in \mathbb{N}$

Soit p_1 ~~soit~~ plus petit diviseur

$$a = p_1 \cdot a_1 \quad a_1 < a$$

Si $a_1 \geq 2$ il a un plus petit diviseur p_2

$$a_1 = p_2 \cdot a_2 \quad a_2 < a_1$$

$$a_{n-1} = p_n \cdot a_n \quad \text{avec } a_n = 1$$

$$a = p_1 p_2 \dots p_n \quad p_i \text{ sont les } i^{\text{èmes}} \text{ diviseurs}$$

$$\text{alors } a = \prod_{i=1}^n q_i^{d_i} \quad \text{où les } q_i$$

factorisation première de a

Elle est unique dans $\mathbb{N}$

ex

756	2
378	2
189	3
63	3
21	3
7	7
1	

$$756 = 2^2 \cdot 3^3 \cdot 7^1$$

Si $a = \prod_{i=1}^k q_i^{d_i}$ tout diviseur d de a

est de la forme $d = \prod_{i=1}^k q_i^{\beta_i}$

$0 \leq \beta_i \leq d_i$ donc β_i a $d_i + 1$

choix possible

Le nb de diviseurs de a est $(d_1 + 1)(d_2 + 1) \dots (d_k + 1)$

ex 756 a donc $(2+1)(3+1)(1+1) = 3 \times 4 \times 2 = 24$ diviseurs allant de 1 à 756

VI.7 PGCD et PPCM

$$a = \prod_{j=1}^k q_j^{d_j}$$

$$b = \prod_{j=1}^k q_j^{\beta_j}$$

$$d_j \geq 0$$

$$\beta_j \geq 0$$

$$\text{PGCD}(a, b) = a \wedge b = \prod_{j=1}^k q_j^{\min(d_j, \beta_j)}$$

$$\text{PPCM}(a, b) = a \vee b = \prod_{j=1}^k q_j^{\max(d_j, \beta_j)}$$

VI.8 Théorèmes sur la divisibilité

VI.8.1 Théorèmes de Bézout

a et $b \in \mathbb{N}^*$ $a \geq b > 0$

$\forall (u, v) \in \mathbb{Z}$ si c/a et c/b alors $c/au + bv$

Soit $I = \{c = au + bv, \forall u, v \in \mathbb{Z}\}$

I contient des entiers positifs

- Soit $I^+ = \{i \in I, i > 0\} \neq \emptyset$

Soit d le plus petit élément de I^+

$\rightarrow d$ divise a :

car diviser a par d : $a = dq + r$ $0 \leq r < d$

donc $r = a - dq$

or $q \in I^+$ donc $\exists (u, v) \in \mathbb{Z}^2$ tq $d = au + bv$

d'où $r = a - (au + bv)q = a \underbrace{(1 - uq)}_{\in \mathbb{Z}} - b \underbrace{qv}_{\in \mathbb{Z}}$

dc $r \in I$
et $r \geq 0$ $\left. \begin{array}{l} \\ r < d \end{array} \right\} r = 0$

de $\hat{m} d/b$; dc d divise a, b

or $a/b/a$ et $a/b/b$ donc $a/b/au + bv = d$
donc $d = a/b$

♥ 1^{re} forme de Bezout $d = a/b \Rightarrow \exists (u, v) \in \mathbb{Z}^2$ tq $d = au + bv$

de plus si $a/b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tq $au + bv = 1$
mais de plus si $\exists (u, v) / au + bv = 1$ alors
 $a/b/1$ donc $a/b = 1$

♥ 2^{de} forme $a/b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2$ tq $au + bv = 1$

VI 8.2

♥ Théorème de Gauss $a/b/c$ et $a/b = 1 \Rightarrow a/c$

car $a/bc \Rightarrow \exists d \in \mathbb{Z} \text{ tq. } bc = ad$
 $a/b = 1 \Rightarrow \exists (u, v) \in \mathbb{Z}^2 \text{ tq. } au + bv = 1$
d'où $ac = u + bc \cdot v = c$
d'où $ac = u + ad \cdot v = c = c(u + dv)$
donc a/c

VI. 8.3 conséquences

$\rightarrow a/b = 1 \text{ et } a/c = 1 \Rightarrow a/bc = 1$
 $\rightarrow a/b = 1 \Rightarrow a^n/b^m = 1 \quad \forall n, m \in \mathbb{N}^*$

VI. 8.4 Algorithme d'Euclide

Soit $(a, b) \in \mathbb{N}^{*2}$ $0 < b < a$
divisons a par b alors $a = bq + r$ $0 \leq r < b$
1^{er} cas $r = 0$ alors $b = a/b$
2^e cas $r > 0$ $r = a - bq$
 $a/b = b/r$

... le pgcd est le dernier diviseur de cette suite de division.

ex $3809, 18459 = ?$

	4	1	5	2
$a = 18459$	$b = 3809$	3223	586	293
3223	586	293	0	

Pour avoir les "Bezout"

$$3223 = a - 4b$$

$$586 = b - 3223 = b - (a - 4b) = -a + 5b$$

$$293 = 3223 - 5(586) = a - 4b - 5(-a + 5b) = 6a - 29b$$

Verif 6

II.8 Equation diophantienne

Soit à résoudre dans $\mathbb{Z}$ l'équation $\boxed{Ax + By = c} \quad (1)$
où $AB \neq 0$

1^{re} étape soit $d = A \wedge B$ (par ex par factorisation première)

1^{er} cas de ne divise pas c ; (1) n'a pas de solution (dans $\mathbb{Z}$)

2^{ème} cas d divise c ; on divise l'équation par d
(1) devient $\boxed{ax + by = c} \quad (2)$ où $a \wedge b = 1$

2^{ème} étape cherchons des (u, v) tq $au + bv = 1$
(par Euclide par ex)

$$\text{alors } a \wedge C u + b \wedge C v = c \quad (3)$$

$$\text{d'où } (2) - (3): a(x - cu) + b(y - cv) = 0$$

$$\text{d'où } a(x - cu) = b(-y + cv)$$

$$\text{d'où } b \mid a(x - cu) \text{ avec } b \wedge a = 1$$

$$\text{donc d'après Gauss } b \mid (x - cu)$$

$$\text{d'où } \exists \lambda \in \mathbb{Z} \text{ tq } x - cu = b\lambda$$

$$\text{alors } a b \lambda = b(-y + cv) \text{ d'où } -y + cv = a \lambda$$

solution de (1) sont

$$\boxed{\begin{matrix} x = cu + b\lambda \\ y = cv - a\lambda \end{matrix} \mid \forall \lambda \in \mathbb{Z}}$$

ex à résoudre dans $\mathbb{Z}$ $8x + 6y = 10 \quad (1)$
 $8 \wedge 6 = 2$

$\mathbb{Z}/10$ de le pb est possible

division (1) par 2

cherchons les Bezout

$$\begin{array}{cc} 1 & 3 \\ 4 & 3 & 1 \\ 1 & 0 \end{array}$$

(2): $4x + 3y = 5$ où $4 \wedge 3 = 1$

$$1 = 4 - 3$$

$$4 \times 1 + 3(-1) = 1$$

$$4 \times 5 + 3(-5) = 5$$

d'où (3)

$$4(x-5) + 3(-y-5) = 0$$

$$4(x-5) = 3(-y-5)$$

donc $3/4(x-5)$ et $3 \wedge 4 = 1$ donc $3/(x-5)$ d'après Gauss
d'où $\exists x \in \mathbb{Z}$ tq $x-5 = 3\lambda$

$$\text{d'où } 4(3\lambda) = 3(-y-5) \text{ d'où } -y-5 = 4\lambda$$

Finalement $\begin{cases} x = 5 + 3\lambda \\ y = -5 - 4\lambda \end{cases} \forall \lambda \in \mathbb{Z}$ vérif: $8x + 6y = 40 + 24\lambda - 30 - 24\lambda = 10$

Rang 1 Si on veut résoudre (1) dans $\mathbb{N}$
on fait le m calcul

$$\begin{aligned} x = 5 + 3\lambda & \begin{cases} x \geq 0 \\ y \geq 0 \end{cases} & \begin{aligned} 3\lambda &\geq -5 & \lambda &\geq -\frac{5}{3} = -1\frac{2}{3} \\ -5 - 4\lambda &\geq 0 & -5/4\lambda &\leq -\frac{5}{4} \end{aligned} \end{aligned}$$

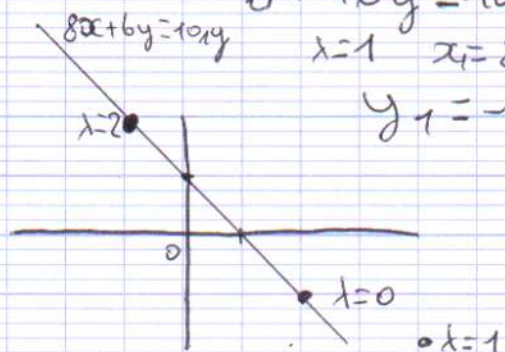
$$\lambda \geq -2$$

$$8x + 6y = 10$$

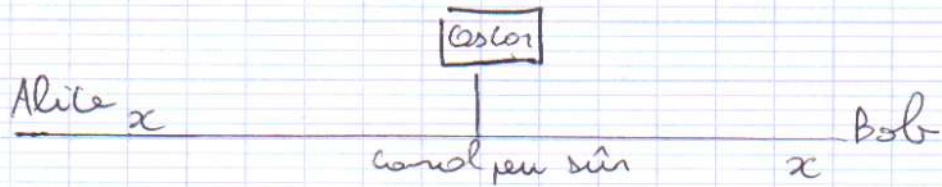
$$\lambda = 1 \quad x = 8$$

$$y = -9$$

Rang 2 interprétation graphique



VI. 10 Applications du Cryptage



$$X = \mathcal{C}_K(x)$$

$$x = d_K(e_K(x)) = x$$

- confidentialité
- intégrité
- authentification

dégonographie

permutation

26! = nb clés

méthode informatique

DES on AES

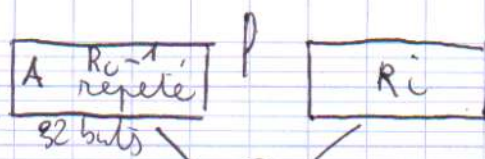
Date en Cryptian Standard | 1975

Advanced, , , /2005

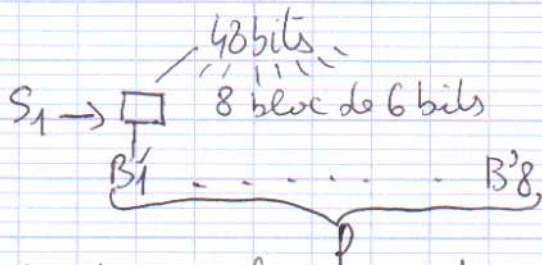
DES clé à 64 bits

x a 64 bits x

$$16 \text{ fois } \begin{cases} L_i = R_i(i-1) \\ R_i = L_{i-1} \oplus f(\underbrace{R_{i-1}}_{16}, \underbrace{K_i}_{16}) \end{cases}$$



K_i sont produits à partir de K_0 par des opérations similaires



K est une clé secrète définie entre Alice et Bob
cryptage symétrique

RSA 1976 Rivest Shamir
procédé asymétrique
factorisation d'un très grand nombre $N=p \cdot q$
(clé publique; clé privée)

PGP

Crypt DE Mathes Applications
Relation
denombrement
Arithmétique