L'arithmétique et la cryptographie

Laurent Debize

Mathématiques appliquées à l'informatique

Nombres premiers

Définition

Un nombre est premier s'il n'admet que deux diviseurs : 1 et lui-même.

Remarque : 1 n'est pas premier. Il n'a qu'un seul diviseur : 1.
Des exemples de nombres premiers : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; etc.
Par contre :

- 4 n'est pas premier : ses diviseurs sont : 1 ; 2 et 4.
- 15 n'est pas premier : ses diviseurs sont : 1 ; 3 ; 5 ; 15

Si un nombre n'est pas premier, on dit qu'il est **composé**.

Nombres premiers

Théorème

Il existe un infinité de nombres premiers (théorème admis).

La course au plus grand nombre premier

Un programme de recherche appelé Great Internet Mersenne Prime Search est constamment à la recherche du plus grand nombre premier possible.
Le plus grand connu à ce jour a été trouvé en 2013
Il a nécessité 360 000 ordinateurs, 150 trillions (10^{18}) opérations par seconde, 17 ans de calcul.
Ce nombre est composé de 17 425 170 caractères. Il faudrait près de 3500 pages pour l'écrire entièrement !
Il peut toutefois s'écrire sous une forme plus courte : $2^{57885161} - 1$

Nombres premiers

Propriété

Soit a un entier naturel strictement supérieur à 1.
a possède au moins un diviseur premier.
Si a n'est pas premier, alors au moins un de ses diviseurs est inférieur à $\sqrt{a}$ (propriété admise).

Méthode pour savoir si un nombre est premier ou non

On appelle cette méthode un test de primalité.

- Si l'un des nombres premiers inférieurs ou égaux à $\sqrt{a}$ divise a, alors a n'est pas premier.
- Si aucun des nombres premiers inférieurs ou égaux à $\sqrt{a}$ ne divise a, alors a est premier.

Nombres premiers

Exemple 1

$a = 871$ est-il premier ?
On calcule $\sqrt{a} = \sqrt{871} \approx 29,51$
Les nombres premiers inférieurs ou égaux à 29,51 sont : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29
On cherche si 871 se divise par un de ces nombres
C'est le cas : 871 se divise par 13 car $871 = 13 \times 67$
Donc 871 n'est pas premier

Exemple 2

$b = 307$ est-il premier ?
$\sqrt{307} \approx 17,52$
Nombres premiers inférieurs à 17,52 : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17
307 n'est divisible par aucun de ces nombres
Donc : 307 est premier

Crible d'Eratosthène

Eratosthène : astronome, géographe, philosophe et mathématicien grec de l'Antiquité (276 av. n.è. - 194 av. n.è.)
Célèbre pour avoir trouvé une méthode permettant de mesurer la circonférence de la Terre
Il a élaboré une méthode (un crible) permettant de trouver, par exemple, tous les nombres premiers entre 1 et 100.

Crible d'Eratosthène

On commence par écrire tous les nombres entre 1 et 100 dans un tableau :

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

Crible d'Eratosthène

On élimine (nombres dans les cases sur fond grisé) :

- 1 qui n'est pas premier
- tous les multiples de 2 (nombres pairs) strictement supérieurs à 2
- tous les multiples de 3 strictement supérieurs à 3
- tous les multiples de 5 strictement supérieurs à 5 (nombres qui se terminent par 0 ou 5)
- tous les multiples de 7 strictement supérieurs à 7

On a $\sqrt{100} = 10$, donc on peut s'arrêter là.
Les nombres restants sont premiers, sinon ils auraient un diviseur premier plus petit que 10.

Crible d'Eratosthène

Inconvénient de cette méthode

Long et fasitidieux, donc envisageable que sur de $\ll$ petits nombres $\gg$...
Mieux vaut implémenter un algorithme.
Mais même dans ce cas, on ne peut pas choisir des nombres trop grands.

Exercice 1

Les nombres suivants sont-ils premiers ? 25 ; 345 ; 659 ; 1023 ;

Le théorème fondamental de l'arithmétique

Théorème

Nous admettrons le théorème suivant :
Tout nombre entier positif strictement plus grand que 1 s'écrit de manière unique sous la forme d'un produit de nombres premiers.

Exemple

La décomposition est à peu près évidente pour de $\ll$ petits nombres $\gg$:

$6 = 2 \times 3$ $\rightarrow$ avec 2 et 3 qui sont premiers

$12 = 2 \times 2 \times 3 = 2^2 \times 3$ $\rightarrow$ avec 2 et 3 qui sont premiers

Le théorème fondamental de l'arithmétique

Méthode

Soit un n un nombre entier.
On cherche à diviser n par tous les nombres premiers, en les prenant dans l'ordre croissant. On divise par chaque nombre premier, tant que c'est possible ; on passe ensuite au nombre premier suivant.

Le théorème fondamental de l'arithmétique

Exemple

Décomposer 9828 en produit de facteurs premiers :

9828	2	9828 se divise par 2 ; le quotient est 4914
4914	2	4914 est encore divisible par 2 ; le quotient est 2457. On ne peut plus diviser par 2 ; on essaie de diviser par 3 :
2457	3	2457 est divisible par 3 ; quotient : 819
819	3	819 est divisible par 3 ; quotient : 273
273	3	273 est divisible par 3 ; quotient : 91 . On ne peut plus diviser par 3 ; on essaie 7 :
91	7	91 est divisible par 7 ; quotient : 13
13	13	13 n'est divisible que par 13 ; quotient : 1 STOP !

On obtient la décomposition en multipliant tous les nombres premiers qui figurent à droite du trait vertical :

$9828 = 2 \times 2 \times 3 \times 3 \times 3 \times 7 \times 13 = 2^2 \times 3^3 \times 7 \times 13$

Exercice 2

1. Décomposer en produit de facteurs premiers les nombres suivants :

$$A = 1080 \qquad B = 63 \times 37 \qquad C = 36^2 \times 38^2$$

$$D = (2 \times 3^2 \times 17)^2 \times (25 \times 24)^5$$

2. On pose $x = 2^4 \times 3^5 \times 5 \times 7^2 \times 11$ et $y = 2^3 \times 3^2 \times 7 \times 11$ Montrer que x est divisible par y. Quel est le quotient de la division de x par y ?

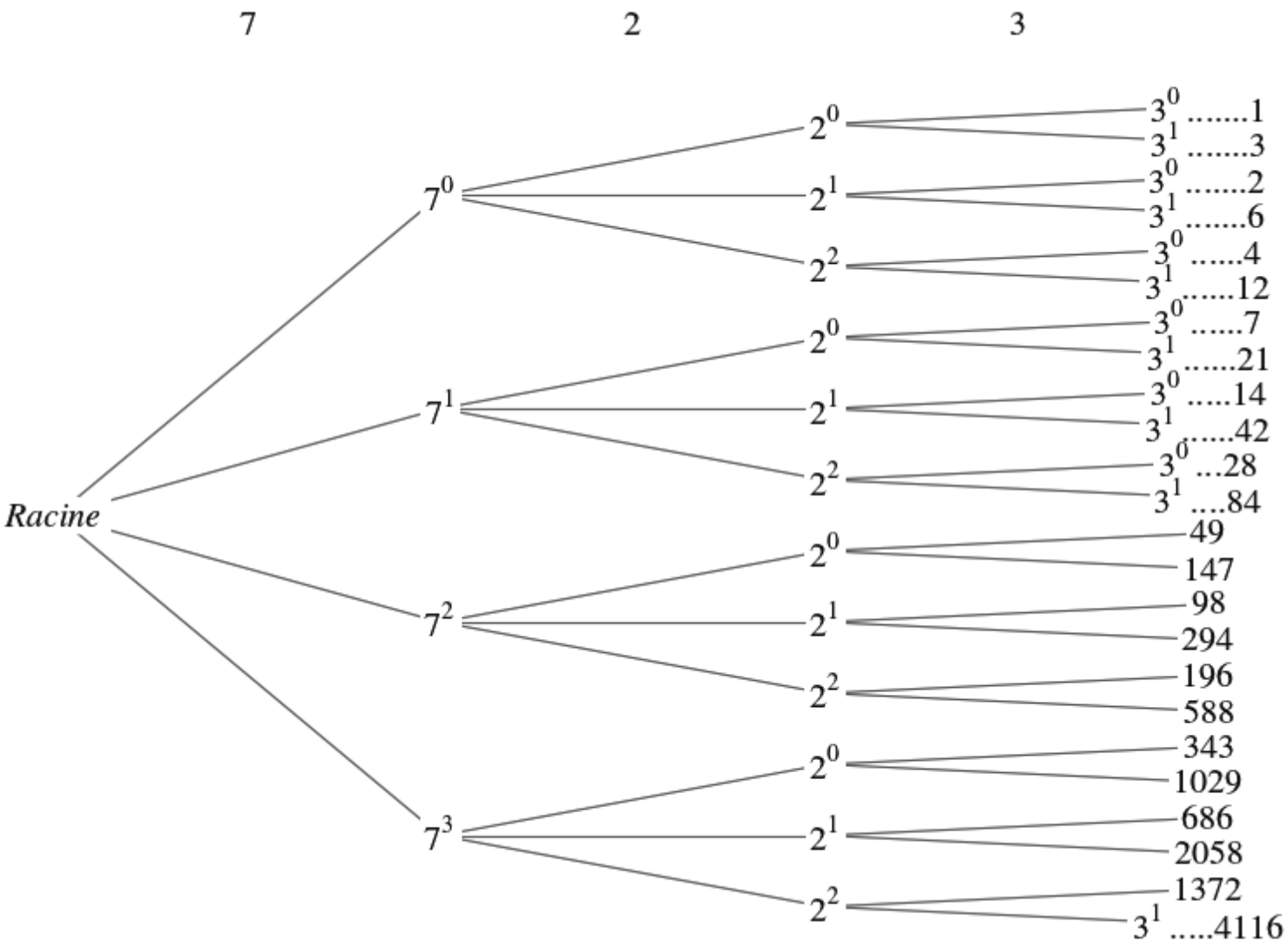
Déterminer les diviseurs d'un nombre

On peut utiliser la décomposition précédente pour obtenir tous les diviseurs d'un nombre

Exemple : $4116 = 2^2 \times 3 \times 7^3$

Utilisons un arbre !

Diviseurs d'un nombre



Déterminer les diviseurs d'un nombre

Conseil : commencer l'arbre par le nombre premier qui a la plus grande puissance.
La lecture et les calculs sur l'arbre se font de gauche à droite.
On met d'abord les puissances de 7 : 7^0, 7^1, 7^2, 7^3 puis les puissances de 2 de 0 à 2 puis les puissances de 3 de 0 à 1.
Les diviseurs s'obtiennent en multipliant les nombres obtenus de la racine de l'arbre jusqu'à la dernière feuille en suivant les branches.
Par exemple pour obtenir 84 on a fait : $7^1 \times 2^2 \times 3^1$.
Remarque : il y a autant de diviseurs que de « branches » de l'arbre soit : $4 \times 3 \times 2 = 24$ diviseurs.

Propriété

Si la décomposition en produit de facteurs premiers du nombre N s'écrit :
$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \ldots \times p_k^{\alpha_k}$, le nombre de diviseurs est égal à : $(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1)\ldots(\alpha_k + 1)$.

PGCD (plus grand commun diviseur)

Définition

Comme son nom l'indique, le *PGCD* de deux entiers a et b est le plus grand nombre entier qui divise à la fois a et b.
On le note : $PGCD(a, b)$

Comment déterminer le PGCD ?

Dans les diapositives suivantes, nous allons donner 4 façons différentes de déterminer le PGCD en étudiant un exemple :
Prenons par exemple : $a = 1636$ et $b = 1128$

1re méthode : trouver les diviseurs

Méthode

Trouvons les diviseurs de $a = 1636$ et $b = 1128$:

$$D_{1636} = \{1, 2, 4, 409, 818, 1636\}$$

$$D_{1128} = \{1, 2, 3, 4, 6, 8, 12, 24, 47, 94, 141, 188, 282, 376, 564, 1128\}$$

Diviseurs **communs** à a et b : 1 ; 2 ; 4.
Le plus grand de ces diviseurs est 4 donc : $PGCD(1636; 1128) = 4$.

Long et fastidieux !

Exercice 3

Calculer le PGCD(246 ; 348) en trouvant tous les diviseurs de chaque nombre.

2e méthode : utiliser la décomposition en produit de facteurs premiers

Règle

Le $PGCD(a, b)$ est égal au produit des facteurs premiers communs aux décompositions de a et de b, chacun d'eux étant affectés du plus petit exposant avec lequel il figure dans la décomposition de a et b.

Exemple

$$1636 = 2^2 \times 409 \qquad \text{et} \qquad 1128 = 2^3 \times 3 \times 47$$

Facteur commun : 2
Plus petit exposant : 2
Donc $PGCD(1636; 1128) = 2^2 = 4$

2e méthode : utiliser la décomposition en produit de facteurs premiers

Autre exemple

$a = 2^2 \times 3^5 \times 7^1 \times 11^2$ et $b = 2^1 \times 3^2 \times 7^4 \times 13$

Facteurs communs :	2	3	7
Plus petits exposants (respectivement) :	1	2	1

Donc $PGCD(a, b) = 2^1 \times 3^2 \times 7^1 = 126$

Exercice 4

Calculer le PGCD(825 ; 168) en décomposant les deux nombres en produit de facteurs premiers.

3e méthode : emploi de l'algorithme d'Euclide

Théorème

Soient a, b, q, r des entiers relatifs non nuls.
Si $a = bq + r$ alors $PGCD(a, b) = PGCD(b, r)$
(Théorème admis)

En pratique

- on divise a par b, on trouve un reste r
- on divise ensuite b par r, ce qui donne un reste r'
- on divise ensuite r par r', ce qui donne un reste r''
- etc.

À chaque étape :

- le dividende de la division est le diviseur de la division précédente
- le diviseur est le reste de la division précédente
- Le PGCD est alors le dernier reste non nul obtenu

3e méthode : emploi de l'algorithme d'Euclide

Exemple : $a = 1636$ et $b = 1128$

Etape	a	b	Reste
1	1636	1128	508
2	1128	508	112
3	508	112	60
4	112	60	52
5	60	52	8
6	52	8	4
7	8	4	0

Dernier reste non nul : $PGCD(1636; 1128) = 4$

Exercice 5

Calculer le PGCD(712 ; 128) avec l'algorithme d'Euclide.

4e méthode : utiliser la calculatrice

Méthode

La plupart des modèles de calculatrices scientifiques donnent directement la réponse.
Sur Texas Instruments : $MenuMATH \rightarrow NUM \rightarrow 9 : gcd$
Puis taper $gcd(1636, 1128)$.
Sur Casio : $OPTN \rightarrow NUM \rightarrow GCD$
Puis taper $GCD(1636, 1128)$
La calculatrice donne directement la réponse : 4.

Nombres premiers entre eux

Définition

On dit que deux nombres sont premiers entre eux si et seulement si leur PGCD est égal à 1

Remarques

Deux nombres **premiers** sont nécessairement **premiers entre eux**.
Par contre, deux nombres premiers entre eux, ne sont pas forcément des nombres premiers.

Exercice 6

Les nombres suivants sont-ils premiers entre eux ? si non quel est leur PGCD ?

4 et 9

44 et 32

13 et 29

30 et 25

23 et 36

Nombres premiers entre eux

Propriété

Propriété du PGCD

Nous admettrons la propriété suivante : si a, b, k sont des entiers :

$$PGCD(ka, kb) = k \times PGCD(a, b)$$

Conséquence

Si $d = PGCD(a, b)$ alors il existe deux nombres a' et b' **premiers entre eux** tels que :

$$a = da' \qquad \text{et} \qquad b = db'$$

En effet : si d est le $PGCD(a, b)$, d est un diviseur de a et de b.
Il existe donc deux nombres a' et b' tels que $a = da'$ et $b = db'$.
On a alors : $d = PGCD(a, b) = PGCD(da', db') = d \times PGCD(a', b')$ (d'après la propriété précédente).
D'où : $d = d \times PGCD(a', b')$ donc $PGCD(a', b') = 1$ et a' et b' sont premiers entre eux.

Exercice 7

Calculer grâce à cette technique : PGCD(30 ; 36)

Congruences - entiers modulo n

Définition

On dit que deux entiers a et b sont congrus modulo n, si a et b ont le même reste dans la division par n.

a et b congrus modulo n se note : $a \equiv b\,(mod\ n)$ ou bien $b \equiv a\,(mod\ n)$
On rencontre aussi cette notation : $a \equiv b\,[n]$ ou $b \equiv a\,[n]$

Exemple

$26 \equiv 15\,(mod\ 11)$ car le reste de la division euclidienne de 26 et 15 par 11 est le même : 4
On peut aussi écrire $26 \equiv 4\,(mod\ 11)$ ou $26 \equiv -7\,(mod\ 11)$
Il y a une infinité de possibilités...

Congruences - entiers modulo n

Autre exemple

2 et 14 sont congrus modulo 12

Un dernier exemple

Si le 4 du mois est un mardi, le prochain mardi sera le 11, puis le 18, le 25

4, 11, 18 et 25 sont congrus à 4 modulo 7

Congruences - entiers modulo n

Propriétés

- $a \equiv b\,(mod\ n)$ équivaut à dire que $a-b$ est un multiple de n
- Si r est le reste de la division de a par n alors : $a \equiv r\,(mod\ n)$
- $n \equiv 0\,(mod\ n)$
- $a \equiv a\,(mod\ n)$
- Si a est un multiple de n alors : $a \equiv 0\,(mod\ n)$
- Transitivité : Si $a \equiv b\,(mod\ n)$ et si $b \equiv c\,(mod\ n)$ alors : $a \equiv c\,(mod\ n)$

Compatibilité des congruences avec les opérations

Soient a, b, c et d des entiers relatifs et p un entier positif.

Compatibilité avec l'addition et la soustraction

- Si $a \equiv b\,(mod\ n)$ alors $a + c \equiv b + c\,(mod\ n)$
- Si $a \equiv b\,(mod\ n)$ alors $a - c \equiv b - c\,(mod\ n)$

Compatibilité avec la multiplication et l'élévation à une puissance

- Si $a \equiv b\,(mod\ n)$ alors $ac \equiv bc\,(mod\ n)$
- Si $a \equiv b\,(mod\ n)$ alors $a^p \equiv b^p\,(mod\ n)$

Autres compatibilités

- Si $a \equiv c\,(mod\ n)$ et $b \equiv d\,(mod\ n)$ alors $a + b \equiv c + d\,(mod\ n)$
- Si $a \equiv c\,(mod\ n)$ et $b \equiv d\,(mod\ n)$ alors $ab \equiv cd\,(mod\ n)$

1 Nombres premiers
- Crible d'Eratosthène

2 Théorème fondamental
- Déterminer les diviseurs d'un nombre

3 PGCD
- Trouver les diviseurs
- Produit de facteurs premiers
- Algorithme d'Euclide
- Calculatrice
- Nombres premiers entre eux

4 Congruences - entiers modulo n

5 Application à la cryptologie
- Le chiffre de César
- Le chiffre affine
- Le chiffre de Vigenère
- Échange de clés Diffie-Hellman

Le chiffre de César

Chiffrement

Jules César utilise un chiffre de substitution monoalphabétique très simple pour transmettre des messages militaires. Chaque lettre du message est remplacée par la lettre venant 3 places après elle dans l'alphabet.

Autrement dit, on associe à chaque lettre de l'alphabet un nombre x entre 0 et 25 à l'aide du tableau :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Nombre	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nombre	13	14	15	16	17	18	19	20	21	22	23	24	25

Puis on calcule $y \equiv x + 3\ [26]$
Ensuite on regarde quelle lettre code y dans le tableau : c'est la lettre chiffrée.

Déchiffrement

Il suffit de faire l'opération inverse : $x \equiv y - 3\ [26]$

Le chiffre de César

Jeu en duo :

1. Ecrire un message, le coder.
2. Le passer à son voisin qui devra le décoder.
3. Vérifiez que vous avez décodé le bon message.

Le chiffre de César

Remarques

- C'est un chiffre de substitution monoalphabétique
- La clé de chiffrement est 3
- La clé de chiffrement est la même que la clé de déchiffrement, il s'agit donc d'un chiffrement symétrique

Le chiffre de César

Décryptement

Je suis un irréductible Gaulois et je veux connaître les intentions de Jules César. J'ai réussi à récupérer un de ses messages militaires et je sais qu'il utilise cette méthode de chiffrage. Comment « casser » son chiffre ?

- Méthode de la force brute : j'essaye toutes les clés possibles ! Combien y en a-t-il ?

Le chiffre affine

Chiffrement

Le chiffre de César étant un peu simple, on peut le compliquer en utilisant deux clés a et b.
Le chiffrement se fait alors en calculant :
$y \equiv ax + b\ [26]$

Exemple

Coder la lettre T avec la clé $(a; b) = (7; 12)$.

Le chiffre affine

Jeu en duo :

1. Ecrire un message, le coder avec la clé (7 ; 12) pour l'un et (5 ; 17) pour l'autre.
2. Passer le message codé à son voisin ainsi que la clé $(a; b)$.
3. Trouver l'inverse de a modulo 26, autrement dit, trouver le nombre c entre 0 et 25 tel que : $a \cdot c \equiv 1\ [26]$
4. Mettre l'équation $y \equiv ax + b\ [26]$ sous la forme $x \equiv cy + d\ [26]$ avec d entre 0 et 25.
5. Décoder le message de votre voisin.

Le chiffre affine

Analyse détaillée

1. Coder à nouveau le message avec la clé (0 ;17). Que se passe-t-il ?
2. Coder à nouveau le message avec la clé (13 ;6). Que se passe-t-il ?
3. Donner les restes de la division euclidienne de $13x + 6$ par 26, pour x allant de 0 à 25.

Le chiffre affine

Analyse détaillée

Un codage est dit acceptable lorsque deux lettres distinctes quelconques sont toujours codées différemment. On admet que les clés $(a; b)$ donnant un codage acceptable sont celles pour lesquelles a est un entier premier avec 26, quel que soit l'entier b compris entre 0 et 25.

1. Donner la liste des nombres entiers compris entre 0 et 25 et premiers avec 26.
2. Déterminer le nombre de clés donnant un codage acceptable.
3. Le mot ABSURDE a été codé à l'aide d'une clé (a ; b) selon le principe décrit ci-dessus et l'on a obtenu VOZLGAT. Déterminer cette clé.

Le chiffre affine

Décryptement

- Méthode de la force brute : j'essaye toutes les clés possibles ! Combien y en a-t-il ?
- Méthode d'analyse des fréquences : dans une langue, toutes les lettres n'ont pas la même fréquence d'apparition. Par exemple, en français, le « e » est beaucoup plus fréquent que les autres lettres. En observant la lettre la plus fréquente dans le texte chiffré, on peut en déduire qu'elle correspond au « e ».

  Cette méthode permet de casser tout chiffrement de substitution monoalphabétique.

Le chiffre de Vigenère

Texte

Clé

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Le chiffre de Vigenère

C'est un chiffremet **polyalphabétique**.
On choisit une clé d'une certaine longueur.

Dans la table de Vigenère, on lit la i^e lettre du texte clair en colonne et la i^e lettre de la clé en ligne : la lettre chiffrée est à l'intersection.

Si le texte est plus long que la clé, on répète la clé

Mathématiquement parlant :
Soient Texte[i] la i^e lettre du texte clair, Clés[i] la i^e lettre de la clé répétée en boucle, Chiffré[i] la i^e lettre du texte chiffré,

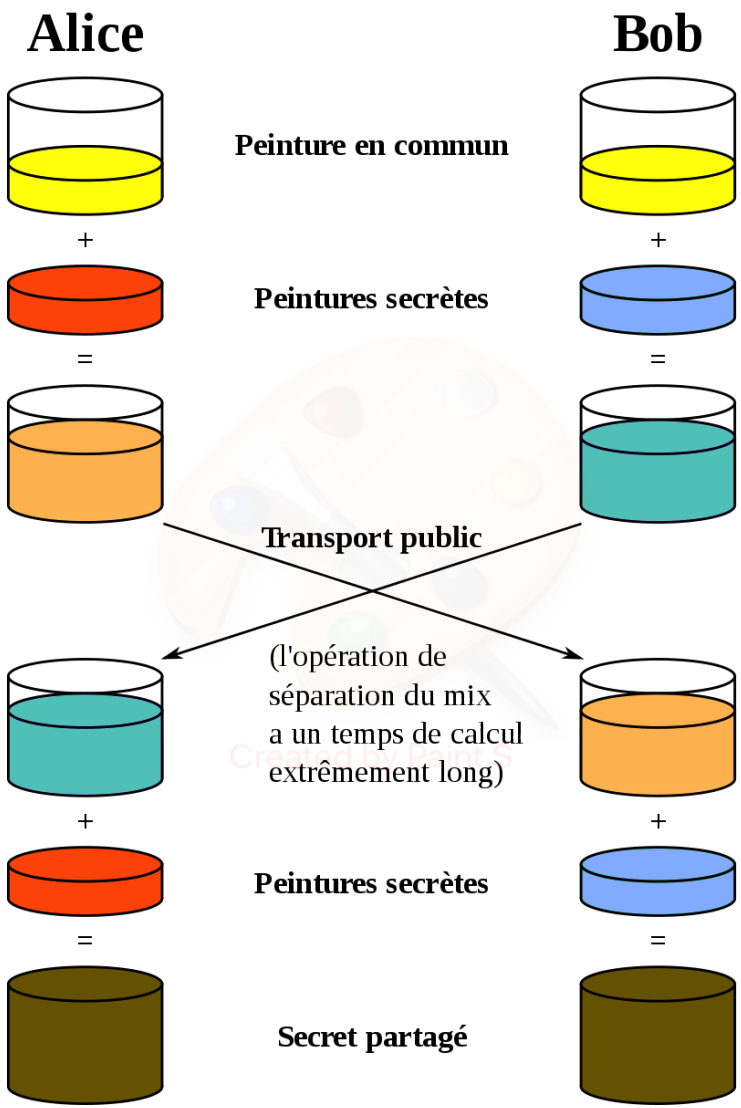
$$\text{Chiffré}[i] = \text{Texte}[i] + \text{Clés}[i] \quad [26]$$

Le chiffre de Vigenère

Jeu en duo :

1. Ecrire un message, choisir une clé.
2. Coder le message à l'aide de la clé en utilisant le chiffre de Vigenère.
3. Passer le message codé à son voisin ainsi que la clé.
4. Décoder le message de son voisin.

Échange de clés Diffie-Hellman



Échange de clés Diffie-Hellman

Alice et Bob doivent choisir deux nombres communs qu'ils se communiquent en clair par le canal public :

- Un nombre premier p
- Un nombre entier g

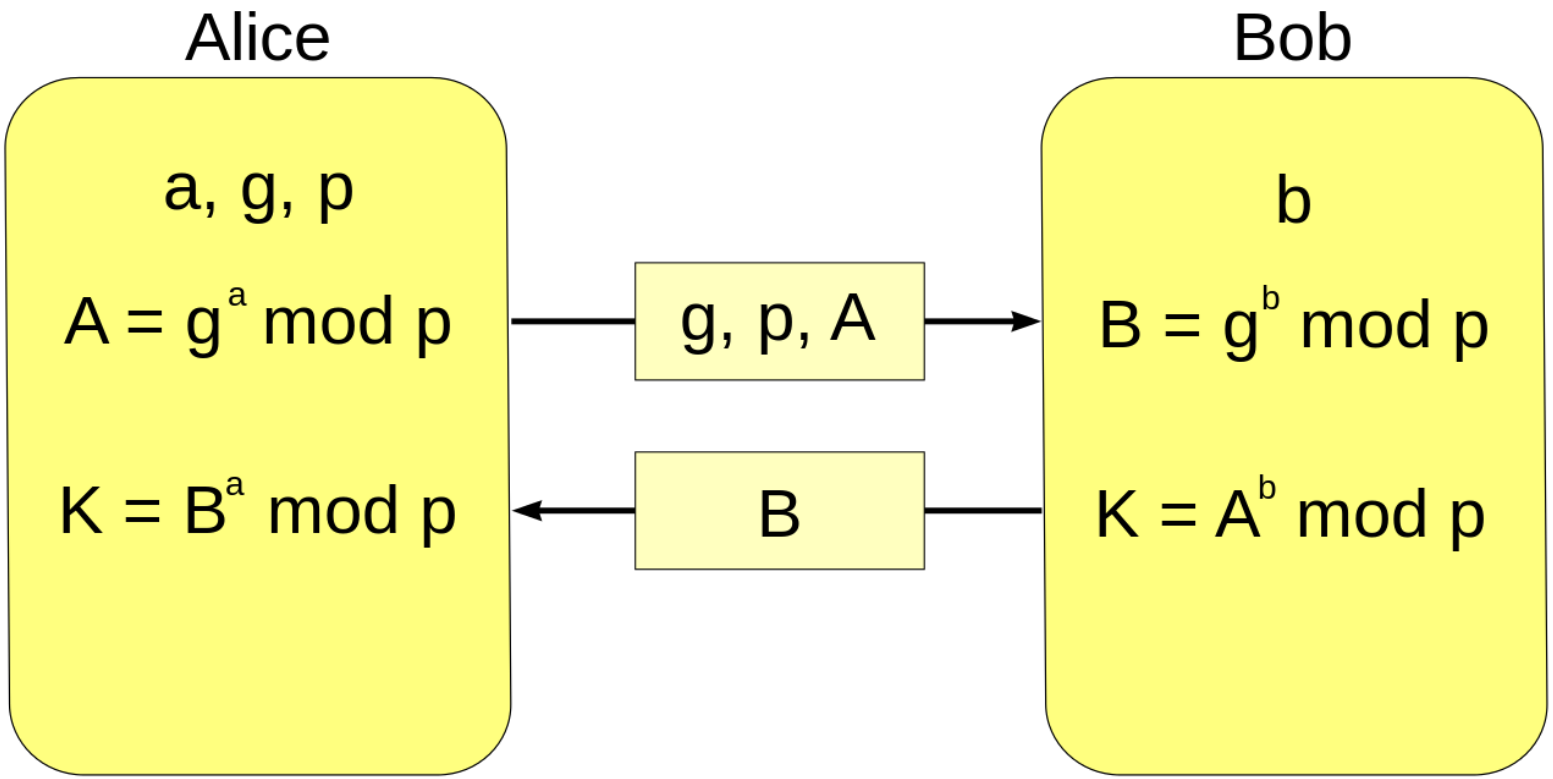
Puis :

- Alice se choisit un nombre privé a.
- Bob se choisit un nombre privé b.
- Alice envoie à Bob le nombre $A \equiv g^a \quad [p]$ où $0 \leqslant A < p$
- Bob envoie à Alice le nombre $B \equiv g^b \quad [p]$ où $0 \leqslant B < p$
- Bob calcule la clé K par : $K \equiv A^b \quad [p]$ où $0 \leqslant K < p$
- Alice calcule la clé K par : $K \equiv B^a \quad [p]$ où $0 \leqslant K < p$

A la fin, Alice et bob ont le même nombre $K \equiv g^{ab} \quad [p]$ où $0 \leqslant K < p$

Échange de clés Diffie-Hellman

Plus schématiquement :



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Exercice 8

Alice et bob choisissent :

$$p = 2741, \quad g = 14, \quad a = 3 \quad \text{et} \quad b = 12.$$

- Déterminer A
- Déterminer B
  N.B. : on pourra remarquer que $14^{12} = 14^6 \times 14^6$
- Déterminer K