Initiation à la cryptographie

Laurent Debize

TIIS1

Outils mathématiques pour 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

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 ou égal 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

Exercice 1

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

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 $ab \equiv cd\,(mod\ n)$

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

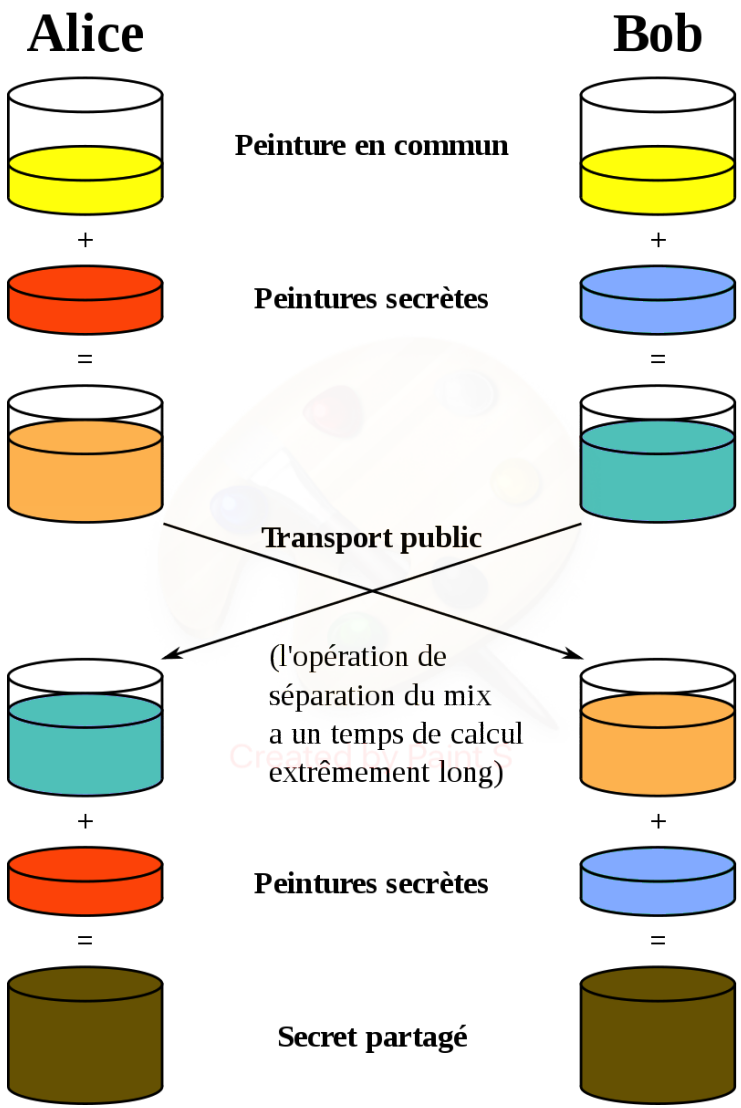
Il suffit de faire l'opération inverse : $x \equiv y - 3$ [26]

Le chiffre de César

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

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

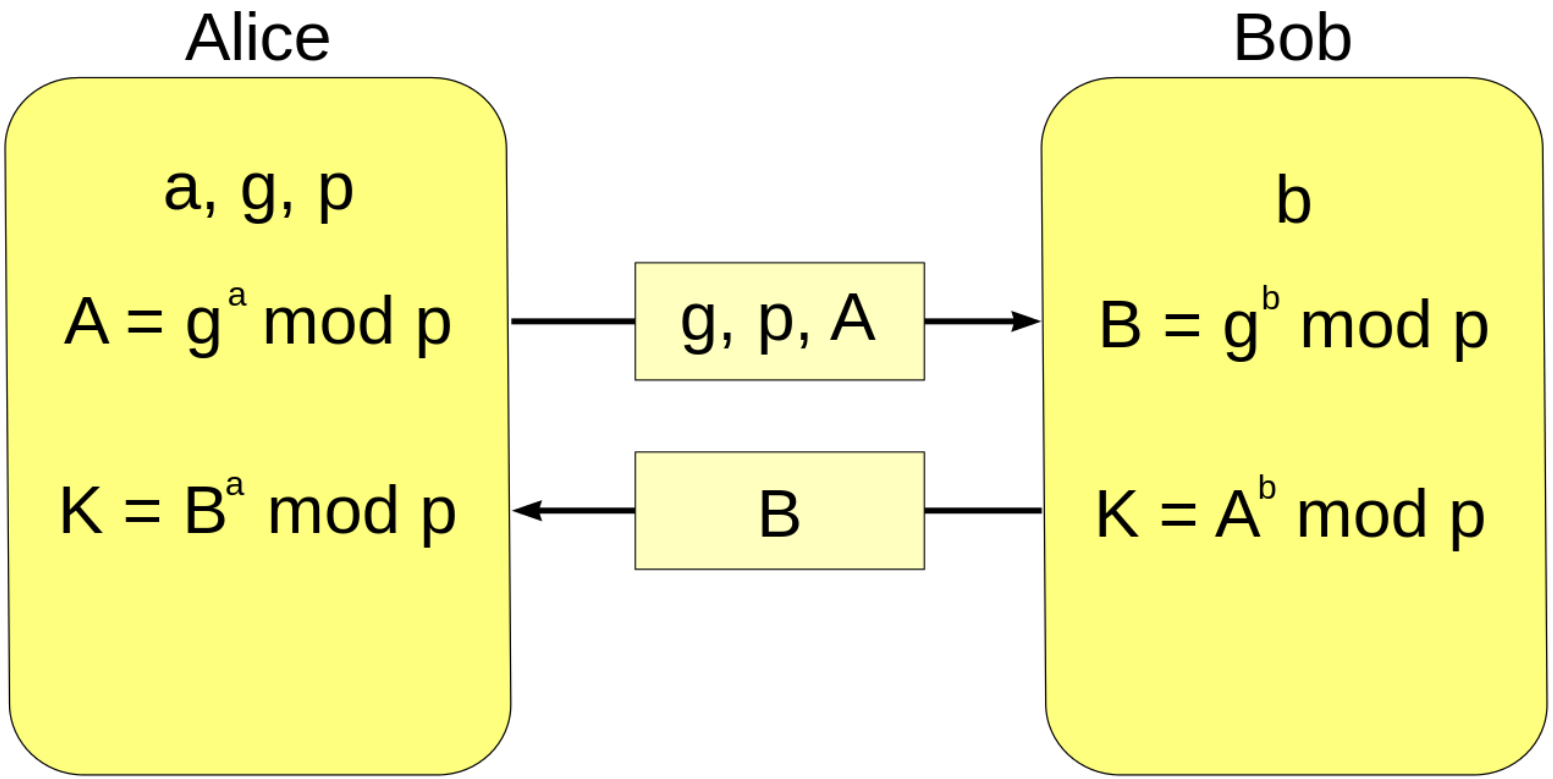
Puis :

- 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 2

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

Le chiffrement RSA

Présentation

C'est un **chiffrement asymétrique**, autrement dit, la clé de chiffrement est différente de la clé de déchiffrement.
La clé de chiffrement est **publique**, autrement dit tout le monde la connaît.
La clé de déchiffrement est **secrète**, connue uniquement du destinataire.

RSA sont les initiales des inventeurs de cette méthode, Ronald Rivest, Adi Shamir et Leonard Adleman. Ils ont publié cette méthode en 1977. Elle est encore utilisée aujourd'hui, notamment dans le commerce électronique.

Le chiffrement RSA

Théorème du RSA

Soient p et q deux nombres premiers distincts et supérieurs ou égaux à 3. On pose $n = pq$.
Si le nombre e est un entier dont le PGCD avec $m = (p-1)(q-1)$ vaut 1, alors il existe un entier d strictement positif tel que $ed \equiv 1\ [(p-1)(q-1)]$ et, pour cet entier d et un entier naturel A quelconque, on a : $A^{ed} \equiv A\ [n]$

Le chiffrement RSA

Principe

Alice, l'émettrice, souhaite envoyer un message chiffré à Bob, le destinataire.

- Création de la clé privée
  Bob se donne un quadruplet de nombres $(p; q; e; d)$ tel que : p et q sont deux nombres premiers ; e est un entier dont le PGCD avec $(p-1)(q-1)$ vaut 1 et d est un entier strictement positif tel que $ed \equiv 1\ [(p-1)(q-1)]$. L'entier d constitue la clé privée tenue secrète par Bob.
- Création de la clé publique
  On pose $n = pq$. Bob rend public le couple $(n; e)$ qui constitue la clé publique.

Le chiffrement RSA

Principe

- Chiffrement
  Alice veut transmettre une information sous la forme d'un nombre A à Bob avec $A < n$. Pour cela, elle calcule $B \equiv A^e \ [n]$ et envoie le nombre B à Bob.
- Déchiffrement
  Pour décoder B, Bob calcule $B^d \equiv A^{ed} \equiv A \ [n]$, ce qui lui redonne A d'après le théorème du RSA.

Exercice 3

Bob a choisi :

$$p = 5, \quad q = 23$$

- Montrer que p et q sont premiers. Calculer ensuite $n = pq$
- Calculer $m = (p-1)(q-1)$.
  Bob choisit ensuite $e = 9$.
- Il faut enfin trouver l'entier d tel que $ed \equiv 1\ [m]$. Bob a trouvé $d = 49$. Montrer que $49 \times 9 \equiv 1\ [m]$.
- Bob envoie sa clé publique (n,e) à Alice et celle-ci l'utilise pour chiffrer le nombre $A = 12$. Calculer $B \equiv A^e\ [n]$.
- Bob reçoit B. Pour le déchiffrer, calculer $B^d\ [n]$.