Arithmétique et Cryptographie (M32)

KOCAK Mikail

8 novembre 2018

Table des matières

1 Introduction sur la crypto

1.1 De l'antiquité au XIX^{e} siècle

— Dans un objectif de confidentialité ;
— Le chiffrement repose sur des permutations et des substitutions (mono ou poly) alphabétiques ;
— C'est un artisanat, et non pas un art scientifique et c'est un secret.

1.2 L'ère de la guerre industrielle

— Les communications sont importantes ;
— La cryptographie progresse ;
— Le premier texte énonçant des principes systématiques, il est connu sous le nom du *Principe de Kerckhoffs*, qui en résumé, dit :
`Le secret doit résider dans la clef et non dans le procédé de chiffrement.` [1]
C'est donc plus facile à changer. Par exemple, communiquer à 100000 hommes une clef plutôt qu'une nouvelle méthode complexe.
— **Confusion, Diffusion,** changer au maximum le message dès lorsqu'un bit change.

1.3 Les années 70 : double révolution

— Explosion des besoins en cryptographie à clé publique ;
— Premier standard de chiffrement par blocs plus ou moins universel : DES [1] (RSA), qui simplifie les communications, tout le monde se met d'accord.

1.4 Cryptographie à clef publique

— Facile à calculer ;
— Difficile à dé-calculer, **sauf si on sait une chose en plus.**

1.5 Standard de chiffrement par blocs

— 1977 DES est né ;
— 1990, DES est déclaré trop vulnérable au brute force, car la clef est trop courte (56 bits) ;
— 2000, un concours international est lancé pour choisir un nouvel algorithme. L'algorithme de Rijndael (aujourd'hui nommé AES) est gagnant.
— Les clés AES sont de 128, 192 ou 256 bits. Ce qui rend les attaques brute force quasiment physiquement impossibles.

1.6 Aujourd'hui

— On veut de la confidentialité ;
— On veut assurer l'intégrité des échanges (ne pas pouvoir modifier le message) ;
— L'authentification (y compris signature), on doit assurer que le destinataire est le vrai.

Le certificat de la clef publique permet d'assurer que seule cette personne saura déchiffrer le message. Le certificat est vérifié via la signature.

Références

[1] Auguste Kerckhoffs

1. Data Encryption Standard

2 Arithmétique Élémentaire

2.1 Divisibilité

2.1.1 Le cadre

— $\mathbb{N}$, des entiers naturels, est un ensemble **bien ordonné** ;
— $\mathbb{Z}$, des entiers relatifs, forme un **anneau commutatif**. Ce qui impliques :
  — Les lois associatives ;
  — Les lois commutatives.

Exemple de structure d'anneau
$a \times (b + c) = a \times b + a \times c$, c'est une structure d'anneau, car un $+$ est lié à un $\times$.

2.1.2 Définition : Relation de divisibilité

Soit a et b, deux entiers. On dit que a **divise** b, ou que a est un diviseur de b, ou encore que b est un multiple de a. Et on écrit $a|b$, s'il existe un entier k tel que $b = ka$.

Remarques
— Zéro n'est diviseur d'aucun entier, et multiple de tous ;
— Tous les entiers sont diviseurs de zéro ;
— Un entier a est toujours divisible par 1 et par a (ainsi que par -1 et $-a$).

2.1.3 Les nombres premiers

Définition

1. Soit p, un entier positif, on dit que p est premier **si ses seuls diviseurs positifs sont** 1 **et lui-même** ;
2. Soit a et b, deux entiers, on dit que a et b sont premiers entre eux **quand leur seul diviseur commun positif est** 1.

2.1.4 Plus grand commun diviseur (PGCD)

Soit a et b, deux entiers. L'ensemble des diviseurs positifs communs à a et b n'est vide (il contient au moins 1), et fini (tout diviseur de a est inférieur à $|a|$).
Il admet donc un plus grand élément : le plus grand diviseur commun à a et b, noté $pgcd(a, b)$.

2.2 Algorithme d'Euclide

2.2.1 Division eucliedienne

Deux entiers positifs a et b, avec $b > 0$. Il existe un unique couple d'entier positifs (q, r), tels que :

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Les entiers q et r sont appelés respectivement **quotient** et **reste** de la division euclidienne de a par b.

Démonstration
Il suffit de remarquer que $\{a - bx | x \in \mathbb{N}, a - bx \geq 0\}$ est un ensemble non vide (il y a au moins a) qui admet donc un plus petit élément, d'où r, puis q...

2.2.2 PGCD

Le calcul de $pgcd(a, b)$ peut-être obtenu par une suite de division euclidiennes : c'est **l'algorithme d'Euclide**.
Comme il est évident que $pgcd(a, 0) = a$, on peut supposer $0 < b \leq a$:

$$
\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\dots \quad \dots \quad \dots \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}
$$

1. La suite des restes est strictement décroissante à valeur positive donc finit par prendre la valeur 0 : arrêt de l'algorithme.
2. En parcourant les lignes de calcul de haut en bas, on voit que tout diviseur de a et b est diviseur de la suite des restes.
3. En les parcourant de bas en haut, on voit que r_n est diviseur commun de a et de b ; on en déduit $r_n = pgcd(a, b)$.

2.2.3 L'identité de Bézout

On peut aussi utiliser chacune des divisions euclidiennes de l'algorithme d'Euclide, de haut en bas, pour exprimer le reste r_k comme combinaison linéaire de a et de b, ce qui donne, pour $k = n$:

Identité de Bézout. *Pour tous entiers positifs a, b, il existe des entiers (relatifs) u et v (parfois appelés « coefficients de Bézout »), tels que :*

$$au + bv = pgcd(a, b)$$

Deux conséquences de l'identité de Bézout :

1. **Corollaire :** a et b sont **premiers entre eux** (i.e. $pgcd(a, b) = 1$) si et seulement s'il existe des entiers u et v tels que $au + bv = 1$.
2. **Lemme de Gauß :** Si a divise le produit bc, donc, $a|bc$ et $pgcd(a, b) = 1$ (a et b sont donc premiers entre eux), alors $a|c$.

2.3 Théorème fondamental de l'arithmétique

2.3.1 Définition

Un entier positif est dit **premier** s'il possède exactement deux diviseurs positifs.
Les résultats suivants sont démontrés dans les *Éléments* d'Euclide, IV$^{\text{e}}$ s.

2.3.2 Proposition

1. Soit a un entier positif :
   — ou bien a est premier,
   — ou bien a admet un diviseur premier inférieur ou égal à $\sqrt{a}$.
2. Il existe une infinité de nombres premiers.

2.3.3 Démonstration

— En effet, si a n'est pas premier, il admet des diviseurs, et le plus petit d'entre eux sera premier...
— Par l'absurde, en considérant le produit de tous les premiers augmenté de 1...

2.3.4 Théorème (Th. Fondamental de l'arithmétique)

Soit $\mathcal{P}$ l'ensemble (infini) des nombres premiers, tout entier positif admet une décomposition unique, à l'ordre près des facteurs, comme produit de nombre premiers :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)},$$

où les entiers $v_p(n)$ sont nuls sauf pour un nombre fini de premiers p.

Démonstration

L'existence est une récurrence facile sur les entiers, l'unicité est la partie la plus « forte » de l'énoncé : c'est aussi une récurrence sur les entiers, où le cas de « base » est celui des nombres premiers, et où l'étape de récurrence s'appuie sur le lemme de Gauß.

Remarque

Il n'y a pas d'algorithme efficace connu permettant de générer les nombres premiers, ou de factoriser un entier.

3 Arithmétique Modulaire

3.1 L'anneau $\mathbb{Z}/n\mathbb{Z}$ – Les entiers modulaires n

3.1.1 Définition

Soit $n \in \mathbb{N}^*$, on définit la relation suivante sur $\mathbb{Z}$:

$$x \equiv y \mod n \iff n|(x-a)$$

L'ensemble des classes d'équivalences est noté $\mathbb{Z}/n\mathbb{Z}$. On note, $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$, ou encore $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, la classe de l'entier $a \in \mathbb{Z}$.

3.1.2 Proposition

Pour tous entiers a, et b, on a une relation d'équivalence de :

1. $a \equiv b \mod n$
2. a et b ont le même reste dans la division euclidienne par n.

3.1.3 Caractéristiques

Réflexivité : $n|0 = a - a$, donc $a \equiv a[n]$;

Surjection :

$$\begin{aligned} a \equiv b[n] &\iff n/(b-a) \\ &\iff n/(a-b) \\ &\iff b \equiv a[n] \end{aligned}$$

Par conséquent, un système "naturel" de représentants des classes est l'ensemble des entiers compris entre 0 et $n-1$: chaque entier est représenté par son reste dans la division euclidienne par n.

Remarque : Il peut être intéressant (surtout pour les calculs "à la main"), de travailler avec un autre système de représentants :

$$\begin{aligned} \mathbb{Z}/5\mathbb{Z} &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} \\ &= \{\bar{-2}, \bar{-1}, \bar{0}, \bar{1}, \bar{2}\} \end{aligned}$$