Cours de Cryptographie BUT2

Leopold Trémant, Pierre Catoire

23 décembre 2024

1 Introduction à la cryptographie

1.1 Qu'est-ce que la cryptographie ?

Nous considérons la situation donnée dans la figure 1 où un *émetteur/source* souhaite envoyé un message à une *destinataire* via un *canal* généralement non sécurisé. Ainsi, un *agent* peut potentiellement intercepté l'information en transit via le canal. Ceci lui permet alors de la *consulter* ou de la *modifier*. En cryptographie, la source s'appelle *Alice*, le destinataire *Bob* et l'agent interceptant le message s'appelle *Eve*.

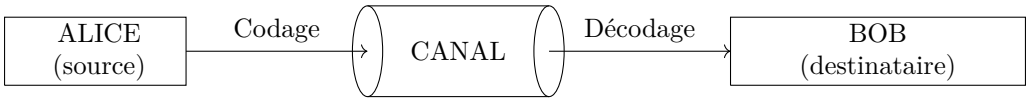


Figure 1 – Notre situation

Pour remédier au problème de l'*interception* par un tiers dans le canal non sécurisé, il suffit d'envoyer un charabia incompréhensible qui ne peut être compris que du destinataire. Cette procédure sera appelé *chiffrement*. Plus précisément, Alice souhaite envoyer un message à Bob via le canal espionné par Eve. Au préalable, Bob et Alice choisissent un moyen de *chiffrés* leurs messages pour leur communication. Ils choisissent une procédure de chiffrement C et une autre de déchiffrement D. Alice écrit son message M et le chiffre via la procédure C choisie avant de l'envoyer dans le canal. Eve ne peut donc lire que le message chiffré $C(M)$ dans le canal. Lorsque Bob, reçoit le message chiffré, il n'a plus qu'à calculer $D \circ C(M) = M$ pour retrouver le message original. On peut voir ceci dans la figure 2.

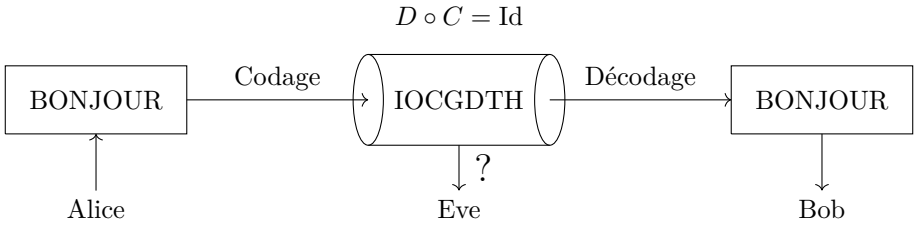


Figure 2 – L'envoi du message d'Alice

Définition 1.1. Dans ce contexte M est appelé le *message en clair* et $C(M)$ est le *message chiffré*. Le *décodage* est la procédure permettant Une *attaque* est une tentative de lecture du texte chiffré. En général, les procédés C et D dépendent également d'un paramètre que nous appellerons la *clé* de chiffrement et/ou de *déchiffrement*.

La discipline consacrée à l'étude des codes secrets et appelée *cryptologie*. Ce domaine est également découpé en deux autres sous-domaines :

— la *cryptographie* qui est l'étude et la conception de processus de chiffrement ;
— la *cryptanalyse* qui est l'étude des textes chiffrés afin de créer des attaques sur des messages chiffrés.

Remarque 1.1. Les procédures de chiffrement prenant un peu de temps, l'utilisation de certains canaux ne permet pas le chiffrement des messages comme les lignes téléphoniques.

1.2 Applications de la cryptographie

Les procédures cryptographiques permettent d'avoir de la *confidentialité*, des *authentifications*, *signatures électroniques*...

Sans surprise, pouvoir envoyer des messages sans être compris par d'autres est d'une importance capitale. Depuis l'antiquité, les hommes souhaitent envoyés des messages secrets pour des raisons commerciales, militaires...

2 Moyen de chiffrement

2.1 Comment être en sécurité ?

Toute procédure de chiffrement peut-être attaquée de manière brutale. Cependant, la sécurité de nos procédures réside dans le fait que l'algorithme capable d'attaquer un texte chiffré est extrêmement lent à fournir une réponse bien qu'un ordinateur effectue 10^9 opérations par secondes ! Autrement, la complexité de l'algorithme attaquant est trop élevée. Ainsi, l'information du message sera périmée ou Eve sera morte de vieillesse avant que l'attaque ait abouti.

2.2 Deux types de chiffrement distincts

Parmi tous les procédés cryptographiques, aussi appelées *chiffrements*, deux grandes familles s'en dégagent :

— les chiffrements *symétriques/à clef secrète* où une même clef est connue *uniquement* d'Alice et Bob qui s'en servent pour chiffrer et déchiffrer les messages. L'avantage de cette procédure est d'avoir un chiffrement et déchiffrement rapide. En revanche, sa sécurité repose sur le secret entre Alice et Bob.
— les chiffrements *asymétriques/à clef publique* où il y a une clef de chiffrement K_e connue de tous et une clé de déchiffrement $K_d \neq K_e$ connue uniquement de Bob. Ainsi, Alice peut communiquer avec Bob mais Bob est le seul à savoir déchiffrer l'information. Les avantages de cette procédure est qu'il est plus aisée de convenir d'une clef de cryptage sans échange préalable entre Alice et Bob. Cependant, le temps de chiffrement et déchiffrement sont plus longs.

Pour des raisons pratiques, il est plus aisé d'associer à chaque lettre un entier. La manière la plus simple est d'associer à une lettre sa position dans l'alphabet, voir le tableau 3. Au lieu de recevoir un message de lettres nous recevrons alors un message de nombre que nous convertirons à nouveau en lettres.

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
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

FIGURE 3 – Correspondance lettres/entiers

Remarque 2.1. On peut utiliser le code ASCII par exemple.

Les exemples donnés ci-dessous seront approfondis plus tard dans la suite du cours :

Exemples 2.1 (Chiffrements symétriques)**.**

1. le chiffrement de CÉSAR consiste à décaler les lettres de l'alphabet d'un paramètre K un entier entre 1 et 26. Prenons $K = 6$ et chiffrons le message « Bonjour ». Ainsi :

B	O	N	J	O	U	R	
↓	↓	↓	↓	↓	↓	↓	
1	14	13	9	14	20	17	
↓	↓	↓	↓	↓	↓	↓	+6
7	20	19	15	20	0	23	
↓	↓	↓	↓	↓	↓	↓	
H	U	T	P	U	A	X	

   Pour déchiffrer, il suffit de décaler toutes les lettres de l'alphabet de 20 ou, de manière équivalente, de -6.
2. le chiffrement par *permutation* consistant à permuter les lettres de l'alphabet en chiffrant puis d'appliquant la permutation inverse pour déchiffrer.
3. le chiffrement de VIGENÈRE ;
4. le chiffrement de VERNAM ;
5. le chiffrement de HILL ;
6. le chiffrement *Enigma* utilisé par la marine allemande durant la seconde guerre mondiale.
7. le chiffrement *Digital Encryption Standard* appelé DES.

Exemples 2.2 (Chiffrements asymétriques)**.**

1. le chiffrement EL GAMAL ;
2. le chiffrement RIVEST-SHANIR-ADLEMAN appelé RSA, utilisé pour les cartes bleues ;
3. le chiffrement EdDSA.

Exemples 2.3 (Chiffrements hybrides)**.**

1. la procédure de DIFFIE-HELLMANN qui permet d'échanger une clé de chiffrement de manière sécurisée ;
2. le chiffrement *PGP*, via *GNU Privacy Guard*.

Exercice 2.1 (Chiffrement par permutation)**.** Chiffrer le message « BONJOUR » par permutation à partir de la permutation suivante.

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
M	Y	G	U	W	K	F	O	A	N	R	X	Q	S	I	E	L	T	J	C	B	H	D	Z	V	P

3 Éléments d'arithmétique

Comme on l'a vu ci-dessus, il est pratique d'identifier les lettres à des entiers. C'est pourquoi dans la suite, on ne considère que des entiers, dont la manipulation requiert quelques notions d'arithmétique.

3.1 Introduction aux espaces de congruences

Notation 3.1. On note $\mathbb{N}$ l'ensemble des entiers naturels (positifs ou nuls) et $\mathbb{Z}$ l'ensemble des entiers relatifs.

Définition 3.1 (Divisibilité)**.** Soit n, m deux éléments de $\mathbb{Z}$. On dit que n *divise* m s'il existe $k \in \mathbb{Z}$ tel que :

$$n = km.$$

On note ceci $n|m$.

Exemple 3.1. Nous avons $3|6$ car $6 = 2 \times 3$ et $6|24$ car $24 = 4 \times 6$. En revanche, $3 \not| 10$.

Lemme 3.2. *Soit n, m deux entiers dans $\mathbb{N}$. On a $n|m$ et $m|n$ si et seulement si $n = m$.*

Démonstration. Soit n, m deux entiers de $\mathbb{N}$ tels que $n|m$ et $m|n$. Par conséquent, il existe k, l deux éléments de $\mathbb{Z}$ tels que :

$$n = l \times m \text{ et } m = k \times n.$$

Par conséquent :

$$n = l \times (k \times n) = (l \times k) \times n.$$

Donc, $k \times l = 1$. Ainsi, $k = 1 = l$ ou $k = l = -1$. Or, comme m et n sont tous les deux positifs k et l sont également positifs. Donc, $k = 1 = l$, ce qui entraîne que $n = m$. □

Proposition 3.3. *Soit d, n, m trois éléments de $\mathbb{Z}$ tels que $d|n$ et $n|m$. Alors, $d|m$.*

Démonstration. Soit d, n, m trois éléments de $\mathbb{Z}$ tels que $d|n$ et $n|m$. Ainsi, il existe k et k' deux éléments de $\mathbb{Z}$ tels que :

$$n = d \times k \text{ et } m = n \times k'.$$

Ainsi :

$$m = (d \times k) \times k' = d \times (k \times k').$$

Donc, en posant $K = k \times k'$, on a $m = d \times K$. Donc $d|m$. □

Exemple 3.2. Nous avons $3|6$ et $6|24$ donc $3|24$. Autrement dit la relation de divisibilité est *transitive.*

Proposition 3.4. *Soit d, n, m trois éléments de $\mathbb{Z}$ tels que $d|n$ et $d|m$. Alors, pour tout $(k, l) \in \mathbb{Z}^2$:*

$$d|k \times n + l \times m.$$

Démonstration. Soit d, n, m trois éléments de $\mathbb{Z}$ tels que $d|n$ et $d|m$. Ainsi, il existe s, q deux entiers de $\mathbb{Z}$ tels que :

$$n = s \times d \text{ et } m = q \times d.$$

Soit k, l deux éléments quelconques de $\mathbb{Z}$. Ainsi :

$$\begin{aligned} k \times n + l \times m &= k \times (s \times d) + l \times (q \times d) \\ &= (k \times s) \times d + (l \times q) \times d \\ &= (k \times s + l \times q) \times d. \end{aligned}$$

Donc, $d | kn + lm$. □

Définition 3.5 (Classe de congruence)**.** Soit $n \in \mathbb{Z}^*$. On dit que deux entiers relatifs a et b **sont congrus modulo** n si $n | a - b$. On note alors $a \equiv b \mod n$.

Exemple 3.3. On a :

$$29 - 5 = 24 = 3 \times 8 \implies 29 \equiv 5 \mod 8.$$

Exercice 3.1. Donner la classe d'équivalence de -3 modulo 5.

Proposition 3.6. *Soit $d \in \mathbb{N}, d \geq 1$. Soit $n \in \mathbb{Z}$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tels que :*

$$\begin{cases} n = qd + r, \\ 0 \leq r < d. \end{cases}$$

Définition 3.7. L'expression $a = qb + r$ avec $0 \leq d < r$ s'appelle *la division euclidienne* de a par b. En Python, cette division s'effectue avec `q = a // b` et `r = a % b`, ou bien `q, r = divmod(a, b)`. On peut également choisir $b < 0$, ce qui donne un reste r négatif, $b < r \leq 0$.

Exemple 3.4. On réalise la division euclidienne de 29 par 8 :

$$29 = 3 \times 8 + 5.$$

Définition 3.8. Soit E un ensemble et une relation $\mathscr{R}$ sur E (c'est-à-dire un sous-ensemble de E^2). On dit que $\mathscr{R}$ est une relation d'équivalence si $\mathscr{R}$ vérifient les propriétés suivantes :

— $\mathscr{R}$ est *réflexive*. C'est-à-dire pour tout $x \in E$ on a $x \mathscr{R} x$.

— $\mathscr{R}$ est *symétrique*. C'est-à-dire que pour tous $x, y \in E$ tels que $x \mathscr{R} y$ on a $y \mathscr{R} x$.

$$\forall (x, y) \in E^2,\ x \mathscr{R} y \implies y \mathscr{R} x.$$

— $\mathscr{R}$ est *transitive*. C'est-à-dire que pour tous $x, y, z \in E$ tels que $x \mathscr{R} y$ et $y \mathscr{R} z$ on a $x \mathscr{R} z$.

$$\forall (x, y, z) \in E^3,\ x \mathscr{R} y \text{ et } y \mathscr{R} z \implies x \mathscr{R} z.$$

Proposition 3.9. *La relation de congruence sur $\mathbb{Z}$ est une relation d'équivalence.*

Exercice 3.2. Prouver que la relation de congruence modulo n est une relation d'équivalence.

Définition 3.10 (Classe d'équivalence)**.** Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E, la classe d'équivalence de x, notée $\overline{x}$, est l'ensemble des $y \in E$ en relation avec x :

$$\overline{x} := \{ y \in E \text{ tels que } x \mathscr{R} y \}.$$

Dans cette situation, x est appelé un représentant de la classe $\overline{x}$.

Remarque 3.1. Soit $x, y \in E$. Si $x \mathscr{R} y$, alors $\overline{x} = \overline{y}$.

Exemple 3.5. Considérons la relation de congruence modulo 5. La classe d'équivalence de 3 est :

$$\begin{aligned}\overline{3} &= \{n \in \mathbb{Z} \,|\, x \equiv 3 \mod 5\} \\ &= \{\dots, -17, -12, -7, -2, 3, 8, 13, 18, 23, 28, \dots\}\,.\end{aligned}$$

Définition 3.11 (Ensemble quotient)**.** Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. On appelle **ensemble quotient** de E par $\mathscr{R}$, noté $E/\mathscr{R}$, comme l'ensemble des classes d'équivalence des éléments de E.

Exemple 3.6. Considérons la relation de congruence modulo 4 dans $\mathbb{Z}$. Ainsi :

$$\mathbb{Z}/_{4\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}\,.$$

Dans l'espace quotient $\mathbb{Z}/_{n\mathbb{Z}}$, les points d'une même classe sont identifier comme étant un seul et même point dans l'espace quotient. Cela ressemble à l'enroulement de la droite réelle sur un cercle, voir l'exemple de la figure 4 dans $\mathbb{Z}/_{4\mathbb{Z}}$.

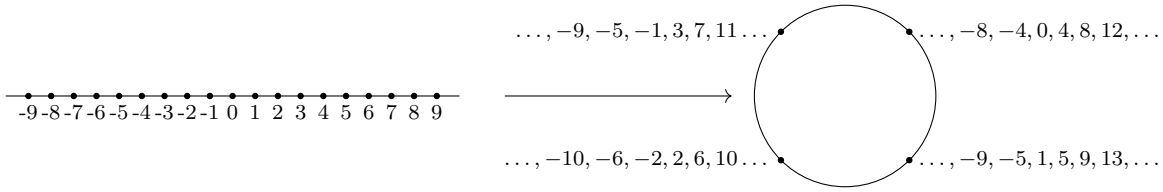


FIGURE 4 – L'ensemble quotient $\mathbb{Z}/_{4\mathbb{Z}}$

Proposition 3.12 (Structure des ensembles quotient)**.** *Pour tout $n \in \mathbb{Z}$, l'ensemble quotient $\mathbb{Z}/_{n\mathbb{Z}}$ est fini et de cardinal n. En outre, il est muni d'une structure d'anneau, i.e. on peut effectuer des additions, des soustractions et des multiplications. On a $\overline{a} + \overline{b} = \overline{a+b}$, $-\overline{a} = \overline{-a}$ et $\overline{a} \times \overline{b} = \overline{a \times b}$.*

Exercice 3.3. Prouver que pour tout représentants $x \in \overline{a}$ et $y \in \overline{b}$, on a $\overline{x+y} = \overline{a+b}$ et $\overline{x \times y} = \overline{a \times b}$.

En général, pour représenter $\overline{a}$, on choisit le reste de la division euclidienne de a par n. En effet, r est dans la classe d'équivalence $\overline{a}$ car $a - r = qn$ est divisble par n, et donc $\overline{a} = \overline{r}$.

Exercice 3.4. Montrer que :

1. la somme de deux entiers impairs consécutifs est divisible par 4.
2. pour tout $a \in \mathbb{Z}$, le produit $a(a+1)$ est divisible par 2.
3. le produit de trois nombres pairs consécutifs est divisible par 48.
4. pour tout $a \in \mathbb{Z}$, le produit $a(a+1)(a+2)(a+3)(a+4)$ est divisible par 120.
5. pour tout $a \in \mathbb{Z}$, $n(n+1)(2n+1)$ est divisible par 6. En déduire que $n(n+1)(7n+1)$ est aussi divisible par 7.
6. si a et b sont impairs, alors $a^2 + b^2$ est divisible par 2 mais pas par 4.

Exercice 3.5 (Résolution de systèmes)**.**

1. Démontrer que, pour tout $x \in \mathbb{Z}$, on a la congruence $x^3 = x \mod 3$.
2. Trouver $x \in \mathbb{Z}$ tel que $3^{2n} - 2^n = x \mod 7$ en fonction de $n \in \mathbb{N}$.
3. À quelle condition sur $a \in \mathbb{Z}/7\mathbb{Z}$ l'équation $x^2 = a \mod 7$ admet-elle des solutions ? Même question pour $x^3 = a \mod 7$.

Exercice 3.6 (Divisibilité par 3)**.**

1. On dénote $(a_k)_k$ les chiffres de n en écriture décimale, i.e. $n = a_0 + 10a_1 + ... + 10^r a_r$ avec $a_k < 10$ pour tout k. Montrer que n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.
2. De même pour la divisibilité par 9 : montrer que n est divisible si et seulement si la somme de ses chiffres est divisible par 9.
3. Est-ce qu'il existe d'autres nombres entre 1 et 9 qui ont cette propriété ?

Exercice 3.7 (Simplification de congruences)**.** Montrer que

1. si $ac = bc \quad [nc]$ alors $a = b \quad [n]$.
2. si m divise n et $a = b \quad [n]$, alors $a = b \quad [m]$.
3. si $ac = bc \quad [m]$, on n'a pas forcément $a = b \quad [m]$.
4. si $a = b \quad [m]$ et $a = b \quad [n]$, on n'a pas forcément $a = b \quad [mn]$.

La propriété 3 (resp. 4) devient vraie si c et m (resp. m et n) sont premiers entre eux, une notion discutée en TD2.

Exercice 3.8. Quels sont les deux derniers chiffres de $7^{9^{9^9}}$?

3.2 Autour de la division euclidienne dans $\mathbb{Z}$

3.2.1 Entiers premiers et premiers entre eux

Définition 3.13. Soit n, m deux éléments de $\mathbb{Z}$. On définit $\text{pgcd}(n, m)$ comme suit :

1. si $n, m \neq 0, \text{pgcd}(n, m)$ est le plus grand entier $d \in \mathbb{N} \setminus \{0\}$ tel que $d|n$ et $d|m$.
2. si $b = 0, \text{pgcd}(a, b) := |a|$.

Autrement dit, $\text{pgcd}(n, m)$ est le *plus grand diviseur commun* de n et m. On dit que n et m sont premiers entre eux si $\text{pgcd}(n, m) = 1$.

Exemple 3.7. Nous avons $\text{pgcd}(3, 6) = 3$ et $\text{pgcd}(9, 15) = 3$. Tandis que $\text{pgcd}(3, 10) = 1$, ils sont donc premiers entre eux.

Définition 3.14. Soit $p \in \mathbb{Z}$. Si p admet uniquement pour diviseur 1 et p, on dit que p est *premier*. Par convention, 1 n'est pas un nombre premier.

On note l'ensemble des nombres premiers $\mathscr{P}$.

Exemple 3.8. Les entiers 2, 3, 5, 7, 11, 13 et 17 sont premiers.

Remarque 3.2. Faire une digression sur le crible d'Ératosthène.

Théorème 3.15. *Soit $n \in \mathbb{Z}$. Alors, il existe des uniques familles $(p_1, \ldots, p_k)$ d'éléments de $\mathcal{P}$ deux à deux distincts, $(\alpha_1, \ldots, \alpha_k)$ d'éléments de $\mathbb{N} \setminus \{0\}$ et $u \in \{-1, 1\}$ tel que :*

$$n = u \times {p_1}^{\alpha_1} \ldots {p_k}^{\alpha_k}.$$

Cette expression s'appelle la décomposition en produits de facteurs premiers *de n.*

Exemple 3.9. La décomposition en produits de facteurs premiers de 230 est :

$$\begin{aligned} 230 &= 2 \times 115 \\ &= 2 \times 5 \times 23. \end{aligned}$$

Exercice 3.9. Donner la décomposition en produits de facteurs premiers de 196, -255 et 2 903 040.

Proposition 3.16 (Lemme de Gauss)**.** *Soit a, b, c trois entiers tels que a et b sont premiers entre eux et $a|bc$. Alors, $a|c$.*

3.2.2 Algorithme d'Euclide

Calculer le pgcd de deux entiers peut s'avérer compliqué. Pour nous simplifier la tâche, nous avons :

Proposition 3.17. *Soit n, m deux entiers de $\mathbb{Z}$ et considérons $n = q \times m + r$ la division euclidienne de n par m. Alors :*

$$\text{pgcd}(n, m) = \text{pgcd}(m, r).$$

Démonstration. Soit n, m deux entiers de $\mathbb{Z}$. Considérons :

$$n = q \times m + r.$$

Posons $d = \text{pgcd}(n, m)$ et $d' = \text{pgcd}(m, r)$. Alors, $d|n$ et $d|m$. Par la proposition 3.4, nous en déduisons que :

$$d|n - q \times m.$$

Or, $n - qm = r$. Donc, $d|m$ et $d|r$. D'où $d \leq \text{pgcd}(m, r) = d'$.

Réciproquement, montrons que $d' = \text{pgcd}(m, r) \leq d = \text{pgcd}(n, m)$. Comme $d'|r$ et $d'|m$, on a :

$$d'|qm + r.$$

Donc, $d'|n$ et $d'|m$, donc $d' \leq d$. Ce qui implique $d = d'$. □

L'algorithme d'Euclide, repose sur la proposition précédente. Il consiste à effectuer des division euclidienne successive jusqu'à trouver $\text{pgcd}(n, m)$.

Algorithme 1 : Algorithme d'EUCLIDE

Entrées : un couple d'entier (n, m)
Sorties : le pgcd de n et m
Initialisation ;
$q \leftarrow n$;
$r \leftarrow m$;
tant que $r \neq 0$ **faire**
  Faire la division euclidienne de q par r, ceci donne $q = k \times r + r'$;
  $q \leftarrow r$;
  $r \leftarrow r'$;
fin
Retourner q.

Remarque 3.3.
— L'algorithme s'arrête car la suite des restes est une une suite décroissante dans $\mathbb{N}$.
— L'algorithme retourne bien $\text{pgcd}(n, m)$ grâce à la proposition 3.17 puisque :

$$\text{pgcd}(n, m) = \text{pgcd}(q, r_0) = \text{pgcd}(r_0, r_1) = \cdots = \text{pgcd}(r_{k-1}, r_k) = \text{pgcd}(r_k, 0).$$

Exemple 3.10. Appliquons l'algorithme d'Euclide à 119 et 35 :

$$\begin{aligned} 119 &= 3 \times 35 + 14, \\ 35 &= 2 \times 14 + 7, \\ 14 &= 2 \times 7 + 0. \end{aligned}$$

L'algorithme renvoie alors l'entier $q = 7$.

Exercice 3.10. Déterminer :

1. $\text{pgcd}(13, 4)$;
2. $\text{pgcd}(33, 42)$;
3. $\text{pgcd}(355, 90)$;
4. $\text{pgcd}(92, 232)$;

3.3 Notions de groupes et sous-groupes

3.3.1 Définitions abstraites

Définition 3.18. Un groupe est un ensemble G muni d'une loi de composition interne $* : G \times G \to G$ vérifiant les propriétés suivantes :
— $*$ est *associative*, c'est-à-dire pour tous $x, y, z \in G$:

$$x * (y * z) = (x * y) * z.$$

— $*$ admet un *élément neutre*, c'est-à-dire il existe $e \in G$ tel que pour tout $x \in G$:

$$e * x = x * x * e.$$

— $*$ est admet des *inverses*, c'est-à-dire pour tout $x \in G$, il existe $y \in G$ tel que :

$$x * y = e = y * x.$$

Dans ce cas, on dit que $(G, *, e)$ est un *groupe*.

De plus, si $*$ est *commutative* c'est-à-dire pour tout $x, y \in G, x * y = y * x$, on dit que $(G, *, e)$ est un groupe *abélien*.

Notation 3.2. Dans un groupe $(G, *, e)$, pour tout $x \in G$, on note traditionnellement x^{-1} ou $-x$ son inverse suivant le contexte.

Exemple 3.11. Nous manipulons des groupes assez souvent :

1. $\mathbb{Z}$ muni de l'addition $+$ est un groupe abélien ;
2. l'ensemble des matrices muni de la multiplication matricielle ;
3. $\mathbb{R}$ muni de l'addition $+$.

Notation 3.3. Lorsqu'on dit « soit G un groupe », il faut comprendre G muni de la loi $*$ et d'élément neutre e est un groupe.

Définition 3.19. Soit G un groupe. On dit que H est un sous-groupe de $(G, *)$ si :
— $H \subseteq G$;
— $e \in H$;
— H est stable par $*$, c'est-à-dire pour tout $x, y \in H, x * y \in H$;
— H est stable par inverse, c'est-à-dire pour tout $x \in H, x^{-1} \in H$.

Exemple 3.12. Par exemple $(\mathbb{Z}, +, 0)$ est un sous-groupe de $(\mathbb{R}, +, 0)$.

3.3.2 Applications à $\mathbb{Z}$

Avec ce langage, $(\mathbb{Z}, +, 0)$ est un groupe. Quels sont les sous-groupes de $(\mathbb{Z}, +, 0)$?

Proposition 3.20. *Les sous-groupes de $\mathbb{Z}$ sont de la forme :*

$$d\mathbb{Z} = \{n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, n = k \times d\},$$

où d est un entier quelconque.

Démonstration. Vérifions tout d'abord que $d\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$:

1. $d\mathbb{Z} \subseteq \mathbb{Z}$;
2. $0 \in d\mathbb{Z}$;
3. soit $x, y \in d\mathbb{Z}$, ainsi il existe $(k, l) \in \mathbb{Z}^2$ tel que $x = kd$ et $y = ld$. Donc :

   $$x + y = (k + l)d \in d\mathbb{Z}.$$

   Donc, $d\mathbb{Z}$ est stable par somme.
4. soit $x \in d\mathbb{Z}$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $x = kd$, son inverse pour la loi $+$ est $y = -kd \in d\mathbb{Z}$.

Donc, $d\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$. Enfin, vérifions que tout sous-groupe de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour un certain d. Soit H un sous-groupe de $\mathbb{Z}$. Si $H = (0)$, c'est correct. Sinon, on pose :

$$d = \min(H \cap \mathbb{N} \setminus \{0\}).$$

Montrons donc que $H = d\mathbb{Z}$ par double inclusion.

Comme H est un sous-groupe de $\mathbb{Z}$ toutes les sommes de d et de son opposé $-d$ sont dans H. Donc, $d\mathbb{Z} \subseteq H$.

Enfin, soit $x \in H$. Faisons la division euclidienne de x par d. Ainsi, il existe $k \in \mathbb{Z}$ et $0 \leq r < d$ tel que :

$$x = k \times d + r.$$

Or, $x \in H$, $k \times d \in H$ puis H est stable par somme, donc :

$$r = x - k \times d \in H.$$

Or, $r < d$ et d est le minimum de $H \cap \mathbb{N}^*$. Par conséquent, $r = 0$, ce qui entraîne que $x \in d\mathbb{Z}$ et $H \subseteq d\mathbb{Z}$. □

3.4 Algorithme d'Euclide étendu et combinaison de Bézout

L'*algorithme d'Euclide étendu* est une version plus complète de l'algorithme 1 permettant d'obtenir une expression du pgcd de deux nombres comme une combinaison linéaire de ces deux derniers. Pour ce faire, il suffit de « remonter » l'algorithme d'Euclide, voir l'exemple 3.13.

Exemple 3.13. On reprends les divisions faites dans l'exemple 3.10 :

$$\begin{aligned} 119 &= 3 \times 35 + 14, \\ 35 &= 2 \times 14 + 7, \\ 14 &= 2 \times 7 + 0. \end{aligned}$$

Nous savons alors $\text{pgcd}(119, 35) = 7$. Maintenant, en remontant ces équations, nous trouvons une combinaisons linéaires de 119 et 35 donnant 7 :

$$\begin{aligned} 7 &= 35 - 2 \times 14 \\ &= 35 - 2 \times (119 - 3 \times 35) \\ &= 5 \times 35 - 2 \times 119. \end{aligned}$$

De cette procédure, on en déduit :

Théorème 3.21 (de Bézout)**.** *Soit a, b deux entiers de $\mathbb{Z}$. Alors, il existe $(u, v) \in \mathbb{Z}^2$ tel que :*

$$a \times u + b \times v = \text{pgcd}(a, b).$$

L'expression $a \times u + b \times v = \text{pgcd}(a, b)$ s'appelle combinaison de Bézout.

En tant que corollaire immédiat, nous avons :

Corollaire 3.22. *Soit a, b deux entiers. Les assertions suivantes sont équivalentes :*

- *a et b sont premiers entre eux ;*
- *il existe $(u, v) \in \mathbb{Z}^2$ tel que :*
$$au + bv = 1.$$
- $\text{pgcd}(a, b) = 1$ *;*

Exercice 3.11. Appliquer l'algorithme d'Euclide étendu et trouver les combinaisons de Bézout pour les paires d'entiers suivantes :

1. $(46, 21)$;
2. $(214, 76)$;
3. $(417, 55)$;

3.5 Anneaux de congruences

3.5.1 L'addition et la multiplication

Soit $n \in \mathbb{Z}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ hérite des deux lois $+$ et x de $\mathbb{Z}$. En effet :

Proposition 3.23. *Les applications suivantes sont bien définies et sont des lois de composition interne dans $\mathbb{Z}/n\mathbb{Z}$:*

$$+ : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z}, \\ (\bar{x}, \bar{y}) & \mapsto & \overline{x+y}, \end{array} \right. \qquad \times : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z}, \\ (\bar{x}, \bar{y}) & \mapsto & \overline{x \times y}. \end{array} \right.$$

En particulier, $+$ est une loi de groupe commutative sur $\mathbb{Z}/n\mathbb{Z}$.

Nous illustrons cette proposition par l'exemple ci-dessous :

Exemple 3.14. On considère $\mathbb{Z}/_{6\mathbb{Z}}$, on a $\overline{4} = \overline{10}$. Ainsi :

$$\begin{aligned} \overline{4} + \overline{5} &= \overline{9} = \overline{3}, \\ \overline{10} + \overline{5} &= \overline{15} = \overline{3}. \end{aligned}$$

De même :

$$\begin{aligned} \overline{4} \times \overline{5} &= \overline{20} = \overline{2}, \\ \overline{10} \times \overline{5} &= \overline{50} = \overline{2}. \end{aligned}$$

Ainsi :

Proposition 3.24. *Pour tout $n \in \mathbb{N}$:*
- $\left(\mathbb{Z}/_{n\mathbb{Z}}, +, \overline{0}\right)$ *est une groupe abélien ;*
- $\times$ *est une loi associative, d'élément neutre* $\overline{1}$ *;*
- *pour tout $x, y, z \in \mathbb{Z}/_{n\mathbb{Z}}$:*

$$x \times (y + z) = x \times y + x \times z \text{ et } (x + y) \times z = x \times z + y \times z.$$

On dit que $\left(\mathbb{Z}/_{n\mathbb{Z}}, +, \times, \overline{0}, \overline{1}\right)$ *est une structure d'*anneau.

En revanche, notez que dans $\mathbb{Z}/_{6\mathbb{Z}}$, nous avons :

$$\overline{2} \times \overline{3} = \overline{6} = \overline{0}.$$

Nous voyons qu'en général $\left(\mathbb{Z}/_{n\mathbb{Z}} \setminus \{\overline{0}\}, \times, \overline{1}\right)$ n'est pas un groupe.

3.6 Calcul d'inverses dans les anneaux de congruences

Proposition 3.25. *Soit $n \in \mathbb{N}$ et soit $\overline{x} \in \mathbb{Z}/_{n\mathbb{Z}}$. Alors :*

$$\overline{x} \text{ admet un inverse pour la multiplication dans } \mathbb{Z}/_{n\mathbb{Z}} \iff \operatorname{pgcd}(x, n) = 1,$$

où x est un représentant de $\overline{x}$.

Démonstration. Soit $n \in \mathbb{N} \setminus \{0\}$ et considérons $\overline{x} \in \mathbb{Z}/_{n\mathbb{Z}}$ tel que x est un représentant de $\overline{x}$ vérifiant $\operatorname{pgcd}(x, n) = 1$. Par le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}$ tel que :

$$xu + nv = \operatorname{pgcd}(n, p) = 1.$$

Ainsi :

$$\begin{aligned} \overline{1} &= \overline{xu + nv} \\ &= \overline{xu} + \overline{nv} \\ &= \overline{xu} + \overline{0}. \end{aligned}$$

Donc, $\overline{u}$ est l'inverse de $\overline{x}$ dans $\mathbb{Z}/_{n\mathbb{Z}}$.

Réciproquement, supposons que $\overline{x}$ admet un inverse dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, il existe $\overline{u} \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ tel que :

$$\overline{x \times u} = \overline{x} \times \overline{u} = \overline{1}.$$

En revenant à la définition des classes, cela signifie :

$$\{m \in \mathbb{Z} \,|\, \exists k \in \mathbb{Z}, m = xu + kn\} = \{r \in \mathbb{Z} \,|\, \exists q \in \mathbb{Z}, r = 1 + qn\}.$$

En particulier, $1 \in \overline{x \times u}$. Donc, il existe $k \in \mathbb{Z}$ tel que :

$$1 = xu + kn.$$

Par le corollaire 3.22, on en déduit $\text{pgcd}(x, n) = 1$. □

Exemple 3.15. Calculons dans $\mathbb{Z}/6\mathbb{Z}$ l'inverse de $\overline{5}$. Pour cela, on calcule une combinaison de Bézout :

$$1 = 6 + (-1) \times 5.$$

L'inverse de $\overline{7}$ est $\overline{-1} = \overline{5}$.

Soit $n \in \mathbb{N} \setminus \{0\}$. En pratique, comment fait-on pour calculer l'inverse d'un élément dans $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$?

Soit $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$. On calcule une combinaison de Bézout entre un représentant x de la classe $\overline{x}$ et p :

$$ax + bp = 1.$$

L'inverse de $\overline{x}$ dans $\mathbb{Z}/p\mathbb{Z}$ est donné par $\overline{b}$.

Exercice 3.12. Dire si les éléments suivants sont inversibles dans l'anneau de congruence. Si oui, calculer leurs inverses :

— $\overline{13}$ dans $\mathbb{Z}/5\mathbb{Z}$;
— $\overline{3}$ dans $\mathbb{Z}/6\mathbb{Z}$;
— $\overline{-2}$ dans $\mathbb{Z}/4\mathbb{Z}$;
— $\overline{3}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Exemple 3.16. Calculons dans $\mathbb{Z}/11\mathbb{Z}$ l'inverse de $\overline{7}$. Pour cela, on calcule une combinaison de Bézout :

$$\begin{aligned} 11 &= 1 \times 7 + 4 \\ 7 &= 1 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \\ 3 &= 3 \times 1 + 0. \end{aligned}$$

Donc :

$$1 = 2 \times 11 - 3 \times 7.$$

L'inverse de $\overline{7}$ est $\overline{-3} = \overline{8}$.

3.6.1 Cas particulier du corps

Pour nos besoins en cryptographie, nous souhaitons que $\left(\mathbb{Z}/_{n\mathbb{Z}} \setminus \{\overline{0}\}, \times, \overline{1}\right)$ soit un groupe.

Théorème 3.26. *Soit $p \in \mathbb{Z}$. Alors :*

$$p \text{ est premier} \iff \left(\mathbb{Z}/_{p\mathbb{Z}} \setminus \{\overline{0}\}, \times, \overline{1}\right) \text{ est un groupe.}$$

Démonstration. Ceci découle de la proposition 3.25. □

Lorsque $p \in \mathscr{P}$, nous avons :
— $\left(\mathbb{Z}/_{p\mathbb{Z}}, +, \overline{0}\right)$ est un groupe abélien ;
— $\left(\mathbb{Z}/_{p\mathbb{Z}}, \times, \overline{1}\right)$ est un groupe abélien ;
— pour tout $x, y, z \in \mathbb{Z}/_{n\mathbb{Z}}$:

$$x \times (y + z) = x \times y + x \times z.$$

Dans ce cas, on dit que $\mathbb{Z}/_{p\mathbb{Z}}$ est un *corps*.

4 Un outil important : le logarithme discret

Dans cette section, nous introduisons le logarithme discret pour introduire le chiffrement de El Gamal plus tard.

4.1 Groupe cyclique

Définition 4.1. Soit G un groupe et $g \in G$. On dit que g est *un générateur/une racine primitive* de G si pour tout élément $x \in G$, il existe $i \in \mathbb{Z}$ tel que $x = g^i$.

Si un groupe G de cardinal *fini* admet un générateur, on dit que G est *cyclique*.

Exemple 4.1. Le groupe $\left(\mathbb{Z}/_{5\mathbb{Z}} \setminus \{0\}, \times, \overline{1}\right)$ est cyclique. En effet, calculons les listes des puissances successives des éléments de ce groupe dans la figure 5 :

FIGURE 5 – Puissance des éléments de $\mathbb{Z}/_{5\mathbb{Z}} \setminus \{0\}$

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	...
$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	...
$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	...
$\overline{3}$	$\overline{4}$	$\overline{2}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{2}$	$\overline{1}$	...
$\overline{4}$	$\overline{1}$	$\overline{4}$	$\overline{1}$	$\overline{4}$	$\overline{1}$	$\overline{4}$	$\overline{1}$	...

Exercice 4.1. Parmi les groupes suivantes lesquels sont cycliques :

1. $\left(\mathbb{Z}/_{7\mathbb{Z}} \setminus \{0\}, \times\right)$,
2. $\left(\mathbb{Z}/_{5\mathbb{Z}}, +\right)$,
3. $\left(\mathbb{Z}/_{16\mathbb{Z}}, \times\right)$,
4. $\left(\mathbb{Z}/_{16\mathbb{Z}}, +\right)$.

4.2 Ordre d'un élément

Définition 4.2. Soit $(G, *, 1)$ un groupe fini et $g \in G$. On note $\text{ord}(g)$ le plus petit entier $n \in \mathbb{N}$ tel que :

$$a^n = 1.$$

Théorème 4.3 (de Lagrange)**.** *Soit G un groupe fini et $g \in G$. Alors,* $\text{ord}(g)$ *divise* $|G|$.

Exemple 4.2. Dans $\left(\mathbb{Z}/_{5\mathbb{Z}} \setminus \{0\}, \times\right)$, l'ordre de $\overline{3}$ est 4 et l'ordre de $\overline{4}$ est 2.

Remarque 4.1. Peut-on parler de l'ordre d'un élément dans $\left(\mathbb{Z}/_{4\mathbb{Z}}, \times\right)$?

Exercice 4.2. Quel est l'ordre de $\overline{5}$ dans $\left(\mathbb{Z}/_{13\mathbb{Z}}, +, \overline{0}\right)$ et dans $\left(\mathbb{Z}/_{13\mathbb{Z}}, +, \overline{1}\right)$?

Proposition 4.4. *Soit G un groupe fini et $g \in G$. Alors :*

$$g \text{ est un générateur de} G \iff \text{ord}(g) \text{ est maximal.}$$

4.3 Indicatrice d'Euler, petit théorème de Fermat et théorème chinois

Notation 4.1. Soit $n \in \mathbb{N}$ avec $n \geq 2$. On note :

$$\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^* := \left\{\overline{x} \in \mathbb{Z}/_{n\mathbb{Z}} \,|\, \text{pgcd}(x, n) = 1\right\}.$$

En particulier, $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*$ est le plus grand sous-ensemble de $\mathbb{Z}/_{n\mathbb{Z}}$ formant un groupe lorsqu'il est muni de la multiplication $\times$.

Définition 4.5. Soit $n \in \mathbb{N}$, on pose :

$$\varphi(n) = |\{m \in \mathbb{Z} \,|\, 1 \leq m < n - 1, \text{pgcd}(n, m) = 1\}|.$$

En particulier, $\varphi(n)$ est le cardinal de $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*$. Pour tout entier $n \in \mathbb{N}$, on appelle $\varphi(n)$ la *caractéristique d'Euler* de n.

Exemple 4.3.
1. Si p est premier, $\varphi(p) = p - 1$,
2. $\varphi(8) = 4$. En effet, les seuls entiers premiers à 8 sont $1, 3, 5, 7$.

Exercice 4.3. Vérifier les énoncés suivants concernant la caractéristique d'Euler :
1. Vérifier l'équation $\varphi(15) = \varphi(3)\varphi(5)$ et calculer $\varphi(9)$.
2. Calculer $\varphi(n)$ lorsque $n = p^k$ avec $k \in \mathbb{N}^*$.

Proposition 4.6. *Soit m et n deux entiers premiers entre eux. Alors :*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Une propriété importante de la caractéristique d'Euler est :

Théorème 4.7 (Euler)**.** *Soit $n \in \mathbb{N}^*$. Soit $a \in \mathbb{Z}$ tel que* $\text{pgcd}(a, n) = 1$*, alors :*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

En particulier, pour tout $\overline{a} \in \mathbb{Z}/_{n\mathbb{Z}}$, on a dans $\mathbb{Z}/_{n\mathbb{Z}}$:

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

En particulier, on en déduit :

Corollaire 4.8 (Petit théorème de FERMAT)**.** *Soit $p \in \mathcal{P}$, alors pour tout $a \in \mathbb{Z}$, on a :*

$$a^p \equiv a \mod p.$$

En particulier, pour tout $a \in \mathbb{Z}/p\mathbb{Z}$:

$$\overline{a}^p = \overline{a}.$$

Démonstration. Soit $n \in \mathbb{N}$ et $a \in \mathbb{Z}$. Il suffit de remarquer que $\varphi(p) = p - 1$. Donc, par le théorème 4.7, on en déduit :

$$a^{p-1} \equiv 1 \mod p.$$

Donc, en multipliant par a une nouvelle fois, nous obtenons :

$$a^p \equiv a \mod p. \qquad \square$$

Exemple 4.4. Grâce à ces théorèmes, nous savons :

$$3^4 \equiv 3 \mod 8 \text{ et } 156^{600} \equiv 1 \mod 601.$$

Exercice 4.4. Vérifier que $12^8 \equiv 12 \mod 15$.

Théorème 4.9 (des restes chinois faible)**.** *Soit p et q deux entiers premiers entre eux et posons $n = pq$. Alors, pour tous entiers a_1, a_2, il existe un unique entier m modulo n tel que :*

$$\begin{cases} m & \equiv a_1 \mod p, \\ m & \equiv a_2 \mod q. \end{cases}$$

4.4 Exponentiation modulaire et logarithme discret

4.4.1 Exponentiation modulaire

Définition 4.10. Soit $n \in \mathbb{N}^*$. Une *exponentiation modulaire* de paramètre $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ est une application :

$$E_{\overline{a}} : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & (\mathbb{Z}/n\mathbb{Z})^* \\ b & \mapsto & \overline{a}^b \end{array} \right.$$

Exercice 4.5. Vérifier que l'expression de E_a ne dépends pas du représentant choisi de la classe de $\overline{a}$.

Dans le cadre des nombres réels, il y a un algorithme bien connu appelé « exponentiation rapide » qui permet de calculer a^b en $O(\log_2(n))$ multiplications. On peut utiliser cette même astuce pour réduire le temps de calcul dans le cadre de exponentiation modulaire donnée dans l'algorithme 2.

Exemple 4.5. Appliquons cette méthode au calcul de a^{13}. L'algorithme 2 calcule alors :

$$a^{13} = a^{12} \times a = (a^6)^2 \times a = \left(\left(a^3\right)^2\right)^2 \times a = \left(\left(a^2 \times a\right)^2\right)^2 \times a.$$

Ainsi, le calcul se fait au prix de 5 multiplications au lieu de 13 en utilisant une méthode naïve.

Nous remarquons que calculer la puissance modulaire d'une classe est une opération peut coûteuse car sa complexité est de l'ordre de $\log_2(n)$.

Algorithme 2 : Exponentiation modulaire

Entrées : L'entier non-nul représentant l'anneau de congruence, la base de l'exponentiation, la puissance à calculer.
Sorties : la classe de congruence de $\overline{a}^b$
if *b=0* **then**
  Retourner 1
else
  Calculer récursivement $a^{\lfloor \frac{b}{2} \rfloor}$ modulo n ;
  On affecte ce résultat dans la variable temp ;
  if *b est impair* **then**
    temp← temp*a mod n ;
  end
end
Retourner temp.

Exercice 4.6. Appliquer l'algorithme exponentiation modulaire aux exemples suivants dans $\mathbb{Z}/n\mathbb{Z}$:
- $n = 23$, que vaut $\overline{6}^4$?
- $n = 28$, que vaut $\overline{3}^8$?
- $n = 13$, que vaut $\overline{3}^{256}$?
- $n = 5$, que vaut $\overline{3}^3 0$?

4.4.2 Logarithme discret

Lorsque $\overline{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}^*$, la fonction $E_{\overline{a}}$ est surjective. Dans ce cas précis :

Définition 4.11. Soit $n \in \mathbb{N}^*$ et considérons $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$. On peut définir une réciproque partielle à la fonction E_a qui est appelée *logarithme discret* en base $\overline{a}$ définie par :

$$L_{\overline{a}} : \left\{ \begin{array}{rcl} \mathbb{Z}/n\mathbb{Z}^* & \to & \mathbb{Z}, \\ \overline{b} & \mapsto & \log_{\overline{a}}(\overline{b}), \end{array} \right.$$

où la quantité $c \coloneqq \log_{\overline{a}}(\overline{b})$ est le plus petit entier tel que $\overline{a}^c = b$.

Exemple 4.6. Calculons $\log_{\overline{3}}(\overline{4})$ dans $\mathbb{Z}/7\mathbb{Z}$, pour cela on énumère les puissances de $\overline{3}$ dans $\mathbb{Z}/7\mathbb{Z}$ comme dans la figure 6. Ainsi, grâce à la figure 6, on trouve $\log_{\overline{3}}(\overline{4}) = 4$.

FIGURE 6 – Puissance $\overline{3}$ dans $\mathbb{Z}/7\mathbb{Z}$

x^1	x^2	x^3	x^4	x^5	x^6
$\overline{3}$	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{5}$	$\overline{1}$

Exercice 4.7. Vérifier que $\overline{2}$ et $\overline{6}$ sont deux générateurs de $\mathbb{Z}/13\mathbb{Z}$. Calculer $\log_{\overline{2}}(\overline{5})$ et $\log_{\overline{6}}(\overline{5})$

Nous énonçons le théorème qui nous permettra de mieux comprendre la difficulté du calcul du logarithme discret :

Théorème 4.12 (du logarithme discret)**.** *Soit $n \in \mathbb{N}^*$ et considérons g un générateur de $\mathbb{Z}/n\mathbb{Z}^*$. Alors, pour tous $x, y \in \mathbb{N}$:*

$$g^x = g^y \iff x \equiv y \mod \varphi(n).$$

Démonstration. Supposons que $x \equiv y \mod \varphi(n)$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $x = y + \varphi(n)$. Ainsi, par le théorème 4.7, nous obtenons :

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

Réciproquement, supposons que $g^x = g^y$. Alors :

$$\overline{1} = g^x \cdot g^{y-1} = g^x \cdot g^{-y} = g^{x-y}.$$

Or, comme g est un générateur de $\mathbb{Z}/n\mathbb{Z}^*$, nous en déduisons que $= \varphi(n) = \left|\mathbb{Z}/n\mathbb{Z}^*\right| < \text{ord}(g)$. Donc, par le théorème 4.7, nous en déduisons que :

$$\varphi(n) | (x - y).$$

Ce qui signifie $x \equiv y \mod \varphi(n)$. □

Exercice 4.8. Nous travaillons dans $\mathbb{Z}/182\mathbb{Z}$:
- Calculer le carré de $\overline{30}$,
- Vérifier que $\overline{13}^6 = \overline{13}^{78}$,
- En déduire $\overline{7}^3 = \overline{7}^{39}$.

Le théorème suivant nous dit donc que savoir si on cherche à résoudre $y = g^z = g^x$, il faut en général calculer la caractéristique d'Euler d'un entier qui n'est pas un problème facile. Sachant cela étudions la complexité de calcul du logarithme discret. Prenons un entier $n \in \mathbb{N}^*$, en règle générale, le calcul du logarithme discret ne peut se faire qu'en énumérant toutes les classes de congruences de $\mathbb{Z}/n\mathbb{Z}$ et en calculant le carré de chacune. Ce qui prends un temps $O(n)$ i.e un temps exponentiel sur la taille des données $\log_2(n)$.

La fonction exponentiation modulaire est une fonction dite *à sens unique* puisque calculer la valeur de la fonction exponentiation modulaire est très facile (en temps $O(\log_2(n))$) comparé au calcul de sa fonction réciproque qui est très difficile (en temps $O(n)$).

5 Les chiffrements symétriques

5.1 Rappels des défis à relever

Actuellement, il y a deux types d'*attaques possibles* :

1. *passives* où Eve se contente de lire les messages passant dans le canal.
2. *actives* où Eve peut modifier le message lors de son voyage vers Bob.

Ainsi, la cryptographie doit répondre à de multiples choses :
- La *confidentialité* qui consiste à empêcher l'accès aux informations transmises par toutes personnes non-destinataires du message.
- L'*authentification* des acteurs de la discussion. Il faut pouvoir détecter une usurpation d'identité lors d'attaques actives.
- L'*intégrité* des informations. Il faut pouvoir attester que le message que le message n'a pas été modifié par un tiers afin d'en altérer le contenu.

— La *non-répudiation* est une sécurité entre les acteurs de la discussion. Alice ne doit pas pouvoir envoyer un message M et certifié devant Bob qu'elle ne l'a pas fait ou à envoyer un autre autre message M'. C'est ce qui est généralement utilisé pour réaliser des *signatures numériques*.

Dans ce cours nous nous concentrerons uniquement sur la confidentialité des échanges.

5.1.1 Principes de Kerckhoffs

Pour avoir une bonne procédure de cryptographie, il est recommandé :

1. l'algorithme repose sur le secret de la clef et non sur le secret de l'algorithme (le nombre d'algorithme disponible est bine inférieur au nombre de clés),
2. le déchiffrement sans clef ne doit pas être une option raisonnable,
3. étant donné un texte en clair et un texte chiffré il est impossible de retrouver la clef.

5.2 Quelques types d'attaques

Par les principes de Kerkhoffs énoncés ci-dessus, on peut supposer que l'attaquant connaît l'algorithme de chiffrement. Il a alors plusieurs options à sa disposition.

5.2.1 Par la force brute :

Cette option est de loin la plus mauvaise. Si notre algorithme de chiffrement utilise une clé suffisamment longue, cela peut prendre un bon moment. Sur un ordinateur effectuant en moyenne un milliard de test de clef à la minute, il lui faudrait 564 ans pour trouver la bonne clef.

5.2.2 Par séquences connues :

Cette attaque consiste à supposée connue une partie du message pour deviner la clef plus aisément. Ceci est une hypothèse raisonnable étant donné que tout message normalement constitué commence par "Bonjour" et se termine par "Au revoir".

Cette attaque est une bonne option si le système de chiffrement laisse transparaître ces régularités du messages.

5.2.3 Par séquences forcées

Cela consiste à faire chiffré un message précis par l'émetteur et d'observer la réponse chiffrée.

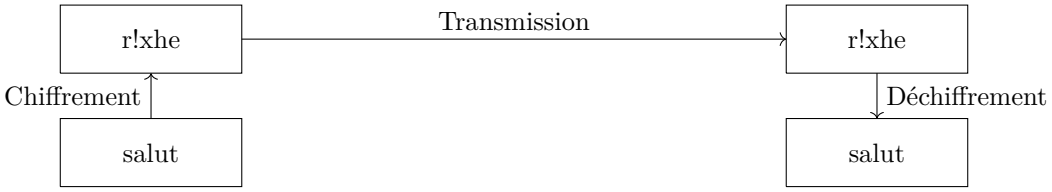
5.3 Les algorithmes de chiffrements

Définition 5.1. Un *algorithme de chiffrement symétrique/ à clef privée* est une procédure de cryptage où la clef de chiffrement et de déchiffrement sont *identiques*, autrement dit $K_e = K_d$.

Remarque 5.1. Chaque méthode de chiffrement est accompagnée de son *espace de clefs*. Il s'agit de l'ensemble des clefs envisageables afin de garantir la sécurité de la méthode cryptographique. Nous nous y intéresserons uniquement lorsque cette méthode peut être utilisée en pratique.

Rappelons le principe de la cryptographie dans la figure 7.

FIGURE 7 – Principe du chiffrement



5.4 Avantages et inconvénients

L'avantage principal de cette famille de méthode de chiffrement est le fait que la procédure de chiffrement et de déchiffrement sont calculées *rapidement* contrairement aux méthodes à clefs privées. Ainsi, ces méthodes sont plus adaptées si le transfert de l'information doit être rapide, par exemple pour les vidéos avec AES que nous ne verrons pas ici (car trop complexe).

L'inconvénient majeur de cette famille est qu'il doit y a souci de *confidentialité sur la clef de chiffrement* utilisée. Si cette clef vient à être découverte, c'est l'échange de toutes les informations qui est compromis.

5.5 Quelques procédures de chiffrements

5.5.1 Les chiffrements affines

Cette famille de chiffrement a été l'une des premières à apparaître. Cette famille de technique englobe les chiffrements de César.

Définition 5.2. Étant donné un alphabet à n caractères, on définit une méthode de *chiffrement affine* $C_{(a,b)}$ avec clé secrète $(a,b) \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}{}^{*} \times {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ avec :

$$C_{a,b} : \left\{ \begin{array}{ccc} {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} & \to & {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, \\ x & \mapsto & ax+b \mod n. \end{array} \right.$$

La fonction de déchiffrement associée est :

$$D_{(a,b)} : \left\{ \begin{array}{ccc} {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} & \to & {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, \\ \overline{y} & \mapsto & \overline{a}^{-1}\overline{(y-b)}. \end{array} \right.$$

Exercice 5.1.
1. Pourquoi $\overline{a} \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}{}^{*}$?
2. Comment retrouve t-on la méthode de chiffrement de César à partir d'une méthode de chiffrement affine ?

Remarque 5.2. Cette méthode de chiffrement chiffre une lettre d'un message toujours de la même manière. Ce qui fait que cette méthode est vulnérable à une *attaque par fréquence* d'apparition. Nous explorerons cette notion plus en détail lors de travaux pratiques.

Exercice 5.2. Chiffrer le message « BIENVENUE EN CRYPTOGRAPHIE » sur les 26 caractères alphabétiques via un chiffrement affine à clef $(3,1)$.

5.5.2 Chiffrement de Vernam

Á l'heure actuelle, il s'agit de la seule procédure de chiffrement démontrée *inconditionnellement sûre* c'est-à-dire qu'à partir du message chiffré, il est impossible de déduire la moindre information sur le message en clair.

Définition 5.3. L'opérateur *XOR*, également appelé *ou exclusif*, noté $\oplus$ est défini :

$$\oplus : \left\{ \begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z}, \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a+b}. \end{array} \right.$$

Définition 5.4 (Chiffrement de Vernam)**.** Le *chiffrement de Vernam* est une procédure de chiffrement du message M écrit sous forme de suite de 0 et de 1, de clef K dont la longueur l est exactement celle du message M, définie par :

$$C_K(M) \coloneqq (M_1 \oplus K_1, \ldots, M_l \oplus K_l) \coloneqq M \oplus K.$$

Exercice 5.3. Chiffrer le message 00100010111101 par la procédure de Vernam avec pour clef 10111010010011.

Le seul défaut de cette méthode est alors le mystère qui doit entourée la clef de chiffrement. Pour que cette procédure soit inconditionnellement sûre, il faut imposer quelques conditions sur l'espace des clefs :

— la clef doit être de la même longueur (ou plus) que le texte à chiffré ;
— la clef ne peut-être utilisée qu'une seule fois ;
— la clef doit-être générée de manière aléatoire.

Exercice 5.4. Vérifier que pour toute suite binaire S, $S \oplus S = 0$.

Soit trois messages M, M', M'' et K une clef pour le chiffrement de Vernam, quels peuvent être les problèmes si :

1. un message M et son chiffré $M \oplus K$ sont interceptés ;
2. trois messages chiffrés $M \oplus K, M' \oplus K, M'' \oplus K$ ont été interceptés.

Voici une famille de chiffrement :

Définition 5.5 (Chiffrement par blocs)**.** Une *procédure de chiffrement par blocs* est un algorithme de chiffrement qui découpe un message M en n blocs de taille r (en complétant éventuellement avec des caractères sans signification) et applique une procédure de chiffrement sur chacun de ses blocs.

5.5.3 Chiffrement de Vigenère

La procédure de chiffrement de Vigenère en est un bon exemple. Plaçons dans un cadre où nous chiffrons nos messages sur un alphabet à n éléments.

Définition 5.6 (chiffrement de Vigenère)**.** Soit M un message et K une clef des suites d'entiers entre 0 et $n-1$. Notons m la longueur du message M et l la longueur de la clef. Le chiffré du message M par la *méthode de Vigenère* est donné en décomposant le message M comme la concaténation de s blocs de longueur l :

$$M = M1 \cdot M_2 \cdot \ldots \cdot M_l.$$

Puis, sur chacun des blocs M_i on applique la fonction de chiffrement :

$$C_K : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z}^{\,l} & \to & \mathbb{Z}/n\mathbb{Z}^{\,l}, \\ (n_1, \ldots, n_l) & \mapsto & (n_1 + k_1, \ldots, n_l + k_l). \end{array} \right.$$

Exercice 5.5. Chiffré le message « BIENVENUE EN CRYPTOGRAPHIE » sur un alphabet un 26 caractères en utilisant la méthode de Vigenère avec pour clef "ATGC".

La méthode de chiffrement de Vigenère n'est plus utilisée quand la clef est trop courte puisque cette méthode a été craqué par Friedrich Kasiski en 1863. Cette méthode consiste à déterminer la taille de la clef via le test de Kasiski, puis de faire une adaptation de l'attaque par fréquence sur le message complet.

En revanche, si la clef est plus longue que le message à chiffré, cette méthode de chiffrement est sûre.

5.5.4 Chiffrement de Hill

Encore un membre de la famille des chiffrements par blocs.

Définition 5.7 (Chiffrement de Hill)**.** Cette méthode de chiffrement a pour clef une matrice K carrée de taille l inversible dans $\mathbb{Z}/n\mathbb{Z}$. Pour chiffré un message M, il faut décomposé ce message $M = M_1 \cdot \ldots \cdot M_l$ et chiffré chaque bloc par la fonction suivante :

$$C_K : \begin{cases} \left(\mathbb{Z}/n\mathbb{Z}\right)^l & \to & \left(\mathbb{Z}/n\mathbb{Z}\right)^l \\ M_i & \mapsto & K \times M_i, \end{cases}$$

où $\times$ est le produit matriciel de la matrice K avec le vecteur colonne M_i.

Cette méthode est aussi vulnérable aux attaques par fréquence de manière similaire à celles décrites pour l'algorithme de Vigenère. En revanche, elle est plus solide que cette dernière méthode.

Exercice 5.6. On considère le message « BIENVENUE » à chiffrer sur 26 caractères en utilisant la méthode de chiffrement de Hill avec pour clef :

$$\begin{pmatrix} 0 & 2 & 0 \\ 3 & 1 & 0 \\ 4 & 9 & 6 \end{pmatrix}$$

5.5.5 Chiffrement Data Encryption Standard (DES)

Il s'agit de l'ancienne version de l'algorithme de chiffrement AES (Advanced Encryption Standard) qui n'est plus utilisable de nos jours mais abordable avec nos connaissances actuelles. Nous allons ici vous expliquez comment fonctionne l'algorithme de chiffrement de *DES*.

Soit M le message à chiffrer et K la clef de l'algorithme de 54 bits. Cette algorithme décompose le message M en blocs de 64 bits comme $M = M_1 \cdot \ldots \cdot M_l$. Cet algorithme fonctionne en utilisant des « tours » de cryptage. Nous détaillons ci-dessous les différentes étapes effectuées par le DES sur *un* bloc M_i de 64 bits du message à chiffré :

— Appliquer une permutation IP aux éléments de M_i. On obtient $IP(M_i) = L_0 \cdot R_0$;
— Effectuer 16 tours de chiffrements que nous détaillons ci-dessous ;
— Ces 16 tours de chiffrement renvoie $R_{16} \cdot L_{16}$;
— On lui applique la permutation IP^{-1} ce qui donne M_i' le chiffré du bloc M_i.

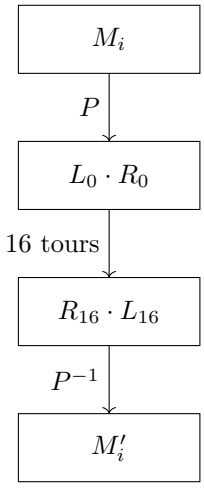
Cette procédure est détaillée dans la figure 8.

Détaillons ce qu'est un tour de DES avec l'appui du diagramme 8b. Pour tout $i \in \mathbb{N}$ avec $1 \leq i \leq 15$

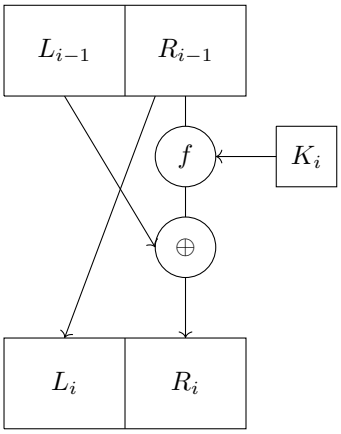
$$\begin{cases} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i), \end{cases}$$

FIGURE 8 – Chiffrement DES

(a) Principe de DES



(b) Un tour de DES



où K_i est ce qu'on appelle une *clef diversifiée*. Cette dernière est une clé de 48 bits générée à partir de la clé K de 56 bits. Nous allons décrire la méthode pour obtenir les clefs diversifiées en nous appuyant sur le diagramme 9 :

Quant à la fonction :

$$f : \begin{cases} \mathbb{Z}/n\mathbb{Z}^{32} \times \mathbb{Z}/n\mathbb{Z}^{48} & \to & \mathbb{Z}/n\mathbb{Z}^{32}, \\ A \times J & \mapsto & f(A, J), \end{cases}$$

celle-ci est définie par :

- Une fonction d'expansion de chaîne de caractères $E : \mathbb{Z}/n\mathbb{Z}^{32} \to \mathbb{Z}/n\mathbb{Z}^{48}$;
- On calcule $B = E(A) \oplus J$, puis on découpe $B = B_1 \cdot B_2 \cdot \ldots \cdot B_8$ en huit blocs de 6 bits.
- On utilise 8 fonctions de substitution $S_1, \ldots, S_8$ où :

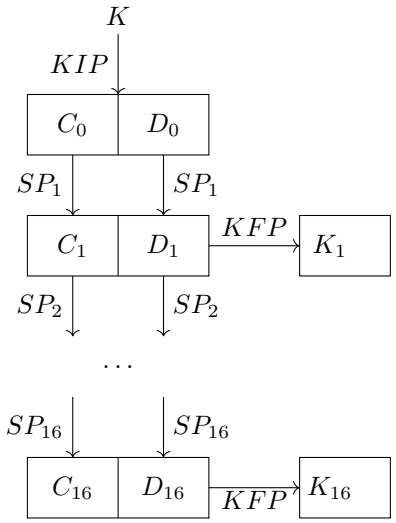
$$S_i : \mathbb{Z}/n\mathbb{Z}^{6} \to \mathbb{Z}/n\mathbb{Z}^{4}$$

- Puis, on calcule $C = C_1 \cdot \ldots \cdot C_8$ puis on retourne $P(C)$ où P est une permutation sur 32 éléments.

Remarque 5.3. Dû aux propriétés de l'opérateur XOR, il n'est pas nécessaire de savoir inverser f.

Cette méthode de cryptage, bien qu'un peu complexe, est assez facile à implémenter et plutôt rapide. En revanche, cette méthode est devenue obsolète depuis les années 2000 à cause du développement prolifique des capacités de calculs informatiques. Cette dernière à été remplacée à cette époque par le système AES.

FIGURE 9 – Diversification des clefs de DES



6 Les chiffrements asymétriques

6.1 Principe

Comme étudié précédemment, un algorithme de chiffrement permet de crypter des communications. Dans le cas d'un chiffrement *symétrique*, la clef de chiffrement K_e et la clef de déchiffrement K_d sont égales. Les méthodes de chiffrement *asymétrique* vérifie quant à elle $K_e \neq K_d$. Cette spécificité leurs confèrent plusieurs avantages et inconvénients.

La clef de chiffrement K_e est la *clef publique* qui sera mise à disposition de tous et la clef de déchiffrement est la *clef privée* qui ne doit être connue que du destinataire du message.

Une analogie pour mieux comprendre est celle de la boîte aux lettres. Tous le monde a accès à l'adresse de Bob (dont Alice) dans l'annuaire qui est l'analogue de la clef publique, mais seul Bob possède la clef de la boîte aux lettres pour accéder aux messages, c'est l'analogue de la clef privée.

6.1.1 Pourquoi cela fonctionne t-il ?

A priori, on ne voit pas pourquoi ces méthodes de chiffrements sont efficaces. En effet, comme nous connaissons les méthodes de chiffrement utilisées par le principe de Kerchoffs, on sait que $E_{K_e}^{-1} = D_{K_d}$. Donc, *en théorie* il est possible de retrouver la clef privée K_d à partir de K_e. Or, *en pratique* le calcul de la clef privée K_d à partir de la clef publique K_e dans ces méthodes de chiffrement est *extrêmement long*. La fonction E est appelée *fonction à sens unique* :

Définition 6.1 (fonction à sens unique)**.** Soit f une application $f : E \to F$ bijective. Cette application est appelée *fonction à sens unique* si f est aisément calculable, c'est-à-dire avec une complexité faible, et son inverse $f^{-1} : E \to F$ est difficilement calculable, c'est-à-dire avec une complexité élevée.

Ces fonctions à sens unique sont à la base de la cryptographie à clef publique. Pour l'instant les deux fonctions dites à sens unique que nous connaissons sont :

— l'exponentiation modulaire ;
— la fonction qui associe à des puissances de nombres premiers leurs produits.

Par conséquent, le concept de *complexité algorithmique* est crucial pour étudier la difficulté de calcul de la clef privé à partir de la clef publique.

6.1.2 Avantages et inconvénients

L'avantage principal des méthodes de chiffrements asymétriques est qu'il n'est pas nécessaire de garder un quelconque secret concernant les clefs puisque la première est publique et la seconde n'a pas besoin d'être partagée. Ce qui fait qu'il est plus aisée de communiquer à distance avec cette méthode.

En revanche, ces méthodes sont plus coûteuses en terme de temps de calcul afin de générer des clefs convenables, de chiffrer et déchiffrer le message. Par ailleurs, il faut également être attentif aux évolutions des attaques sur ces méthodes de chiffrement afin de prendre des clefs suffisamment complexes.

6.2 Échange de clefs de Diffie-Hellman

Cette procédure permet d'échanger des clefs de chiffrements de manière sûre, sans avoir à procéder à une rencontre physique pour échanger les clefs, afin d'utiliser une procédure de chiffrement symétrique.

6.2.1 Procédure d'échange de clefs

Alice et Bob se mettent d'accord (à la vue de tous) d'un entier p premier et d'un générateur g de $\left(\mathbb{Z}/p\mathbb{Z}^*, \times, \overline{1}\right)$.

Étape 1 : Alice et Bob choisissent respectivement des éléments a, b de $\mathbb{Z}/p\mathbb{Z}^*$. Alice calcule :

$$A = g^a \mod p.$$

Quant à lui, Bob calcule :

$$B = g^b \mod p.$$

Étape 2 : Alice envoie A à Bob et Bob envoie B à Alice à la vue de l'agent Ève.

Étape 3 : Alice calcule B^a et Bob A^b. Or :

$$B^a = (g^b)^a = (g^a)^b = A^b.$$

Ainsi, Bob et Alice prennent pour clef secrète $K = B^a$.

Exemple 6.1. Dans cet exemple, on choisit $p = 11$ et $g = \overline{7}$. Alice choisit l'entier $a = 3$ et Bob choisit $b = 9$. Ainsi, Alice et Bob calcule séparément :

$$A = \overline{7}^3 = \overline{2} \text{ et } B = \overline{7}^8 = \overline{9}.$$

Puis, Bob reçoit A et Alice reçoit B et chacun calcule :

$$B^3 = \overline{9}^3 = \overline{3} \text{ et } A^8 = \overline{3}$$

Exercice 6.1. On choisit $p = 17$ et $g = \overline{7}$. Qu'elle est la clef échangée en prenant $a = 4$ et $b = 11$?

6.2.2 Pourquoi ça fonctionne ?

Lorsque Ève voit les deux clefs A et B traverser le canal, cette dernière ne peut pas prédire quelle va être a clef utilisée par Bob ou Alice. En effet, si elle souhaite calculer K, elle doit découvrir quel indice Bob ou Alice a utilisée. Donc, cette dernière devra résoudre un problème de logarithme discret qui est trop long à résoudre sous réserve que l'entier p est suffisamment grand.

6.3 Le chiffrement de Rivest-Shamir-Adleman (RSA)

Le chiffrement RSA est basé sur le résultat suivant :

Théorème 6.2 (RSA)**.** *Soit $n = pq$ un produit de deux nombres premiers. Soit $a \in \mathbb{Z}/n\mathbb{Z}$. Alors, pour tout $k \in \mathbb{Z}$:*

$$a^{k\varphi(n)+1} \equiv a \mod n.$$

Démonstration. Il faut faire deux cas :

1er cas si a est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Dans ce cas, par le théorème 4.7, $a^{\varphi(n)} \equiv 1 \mod n$. Donc :

$$1 = \left(a^{\varphi(n)}\right)^k \times a = a^{k\varphi(n)+1}.$$

2e cas si a n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Si a est nul, le résultat est vrai. Enfin, si a n'est pas nul et n'est pas inversible modulo n, alors soit $a \equiv 0 \mod p$ et $a \equiv 0 \mod q$.

Cas 1 $a \equiv 0 \mod p$. Alors, $a \not\equiv 0 \mod q$. Ainsi, par le petit théorème de Fermat 4.8, nous avons :

$$a^{q-1} \equiv 1 \mod q.$$

Par conséquent, pour tout entier k :

$$a^{k(p-1)(q-1)+1} = \left(a^{q-1}\right)^{k(p-1)} \times a = a.$$

Cas 2 $a \equiv 0 \mod q$. On effectue le même raisonnement que précédemment.

Par conséquent, nous avons démontré le théorème. □

De ce théorème, nous pouvons en déduire la méthode de chiffrement de RSA.

6.3.1 Procédure de chiffrement RSA

On considère M un message à chiffrer. Pour utiliser la méthode RSA, nous avons besoin de deux "grands" nombres premiers p et q. Puis, c'est tout ! On applique alors la procédure suivante :

1. Calculer l'entier $n = pq$ (il est vraiment très grand !) ;
2. Calculer $\varphi(n) = (p-1)(q-1)$;
3. Choisir e un entier pas trop "petit" premier avec $\varphi(n)$;
4. Calculer son inverse dans le groupe $\left(\mathbb{Z}/n\mathbb{Z}^*, \times, \overline{1}\right)$;
5. Publier (n, e) comme *clé publique* ;
6. Conserver jalousement (n, d) la *clé privée*.

Cryptage : Une fois les clefs privée et publique calculer, si Bob souhaite envoyé un message à Alice via un canal non sécurisé, il chiffre son message M (qui sera considéré comme un entier plus petit que n) en calculant :

$$C = M^e \mod n.$$

Décryptage : Alice reçoit le message chiffré C est alors envoyé à Alice qui le décrypte en calculant $C^d \mod n$.

Lemme 6.3. *Avec les notations ci-dessous :*

$$C^d = M.$$

Démonstration. En effet :

$$C^d = (M^e)^d \mod n = M^{ed} \mod n.$$

Or, d est l'inverse de e modulo $\varphi(n)$. Par conséquent, il existe $k \in \mathbb{Z}$ tel que :

$$ed = k\varphi(n) + 1.$$

D'où, par le théorème 6.2, nous avons :

$$C^d = \left(M^{\varphi(n)}\right)^k \times M \mod n = M \mod n. \qquad \square$$

Exemple 6.2. Considérons les entiers $p = 13$ et $q = 17$. Ainsi, $n = 221$ et $\varphi(n) = (13-1) \times (17-1) = 192$.

Choisissons un petit entier e premier à 192, par exemple 5. Calculons son inverse dans $\left(\mathbb{Z}/221\mathbb{Z}^*, \times, \overline{1}\right)$:

$$\overline{5} \times \overline{-44} = \overline{1} \text{ dans } \mathbb{Z}/221\mathbb{Z}.$$

Nous pouvons alors publier la clef publique $(221, 5)$ et nous gardons la clef privée $(221, -44)$.

Considérons $M = 132$ le message à chiffrer. Son chiffré est :

$$C = M^5 \mod 221 = 149 \mod 221.$$

Puis, le destinataire, grâce à la connaissance de sa clef privée $(221, 5)$ déchiffre le message en calculant :

$$D = C^5 \mod 221 = \overline{132} = M$$

Exercice 6.2. On considère $p = 49$ et $q = 47$.

- Déterminer la clef publique en choisissant $e = 19$ et la clef privée de RSA associées à ces deux entiers.
- Chiffrer la lettre C dont le code ASCII est 67 avec la clef publique. Puis, vérifier que la clef privée déchiffre correctement le message.

6.3.2 Les bienfaits de RSA

Avec RSA, il n'est plus nécessaire de faire reposer un quelconque secret concernant la clef puisqu'elle est publique !

En pratique, il n'est pas compliqué de générer des grands nombres premiers en utilisant l'algorithme probabiliste de Miller-Rabin.

Les calculs d'inverses son aisés à faire et les chiffrements et déchiffrements s'effectuent rapidement grâce à l'*exponentiation modulaire*.

Pour casse RSA, il est nécessaire de pouvoir calculer $\varphi(n)$ pour trouver l'inverse de la clef publique. Or, jusqu'à ce jour, on pense que calculer $\varphi(n)$ est aussi dur que trouver la décomposition en produit de facteurs premiers de n ! Ainsi, savoir casser RSA revient à résoudre le problème de la décomposition en produits de facteurs premiers d'un nombre.

6.3.3 Quelques précautions à prendre sur l'espace des clefs

Il y a néanmoins quelques précautions à prendre avec les clefs RSA. Voici une liste non-exhaustive de recommandations :

1. éviter l'utilisation d'exposant e "petit" (i.e $\leq \log(n)$)
2. éviter d'utiliser pour une même communication, le même exposant e ;
3. éviter d'utiliser pour une même communication, le même entier n ;
4. éviter que l'un des facteurs premiers de $p-1$ et $q-1$ soit trop petits. Sinon, nous nous exposons à une attaque factorielle de RSA.
5. choisir une clé enregistrée sur 2048 bits (le système RSA est cassée pour des clefs sur 829 bits).

Pour avoir plus d'informations à ce sujet, la norme PKCS#1 résume toute les conditions sur l'espace des clefs.

6.4 Chiffrement de El-Gamal

Le chiffrement de El-Gamal est une procédure ne reposant pas sur le problème de factorisation d'un nombre premier mais sur celui du *logarithme discret* détaillé plus tôt dans ce cours.

6.4.1 Génération des clefs

Pour générer les clefs d'un chiffrement El-Gamal, nous avons besoin d'un nombre premier p tel que la résolution du problème du logarithme discret est difficile. Puis, on génère les clefs en calculant les quantités suivantes :

— On choisit g un générateur de $\left(\mathbb{Z}/p\mathbb{Z}^*, \times, \overline{1}\right)$;
— On choisit s un nombre et on pose $\beta \coloneqq g^s$;
— La *clé publique* est $K_e = (p, g, \beta)$;
— La *clé privée* est s.

On considère maintenant un message M à chiffrer (on considérera que M est un entier plus petit que n) :

Chiffrement : on choisit $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ un nombre aléatoire à garder secret. On calcule un couple à partir de la clef publique :

$$E_{K_e,k}(M) = (y_1, y_2) = \left(g^k \mod p, M \times \beta^k \mod p\right).$$

Déchiffrement : ayant reçu les deux données (y_1, y_2), on calcule :

$$D_{K_d}(y_1, y_2) = y_2 \times (y_1^s)^{-1}.$$

Lemme 6.4. *Étant donné une clef privée $K_d = s$ et $K_e = (p, g, \beta)$. Dans ce cas pour tout $M, k \in \mathbb{Z}/p\mathbb{Z}^*$:*

$$D_{K_d} \circ E_{K_e,k}(M) = M.$$

Démonstration. En effet, soit M et k deux éléments de $\mathbb{Z}/p\mathbb{Z}^*$. Alors dans $\mathbb{Z}/p\mathbb{Z}^*$ nous avons :

$$E_{K_e,k}(M) = (g^k, M \times \beta^k).$$

Puis :

$$D_{K_d}(g^k, M \times \beta^k) = M \times (g^s)^k \left((g^k)^s\right)^{-1} = M.$$

□

Exemple 6.3. On considère $p = 11$ et on prends comme générateur de $\mathbb{Z}/17\mathbb{Z}^*$ l'élément $g = \overline{7}$. On choisit $s = 3$. Ainsi :

$$\beta = g^3 = 7^3 \mod 11 = 2 \mod 11.$$

La clef publique est $(11, 7, 2)$ tandis que la clef privée est $s = 3$.

Considérons le message $M = 9$ à chiffrer. On tire au hasard $k = \overline{4}$ dans $\mathbb{Z}/11\mathbb{Z}^*$. Le chiffré de ce message est le couple :

$$\begin{aligned}(g^k \mod p, M \times \beta^k \mod p) &= (\overline{7}^4, \overline{9} \times \overline{2}^4) \\ &= (\overline{3}), \overline{9} \times \overline{5}) \qquad\qquad = (\overline{3}, \overline{1}) \\ &= (y_1, y_2).\end{aligned}$$

Maintenant, le destinataire qui dispose de la clé privée $s = 3$, n'a plus qu'à calculer :

$$\begin{aligned}y_2 \times (y_1^s)^{-1} &= 1 \times \left(\overline{3}^3\right)^{-1} \\ &= \overline{5}^{-1} \qquad\qquad = \overline{9} = M.\end{aligned}$$

Exercice 6.3 (à faire avec l'assistance de l'ordinateur ou calculatrice)**.** On considère $p = 181$ et on considère comme générateur $g = \overline{2}$. On souhaite chiffrer le message $M = 153$. Appliquer la procédure du chiffrement de El Gamal en choisissant $s = 6$ et $k = 11$.

6.4.2 Les raisons pour lesquelles cette méthode fonctionne

Cette méthode de chiffrement est sécurisée même si la clef publique est à disposition. En effet, pour récupérer la valeur de M il est nécessaire de connaître l'exposant de g qui a donné β et l'exposant k qui a donné y_1.

Ainsi, il faut résoudre deux problèmes du logarithme discret qui, nous le savons, sont des problèmes de complexité élevées.

7 Le mot de la fin

Nous avons vu et compris comment des méthodes cryptographiques fonctionnent. Cependant, une grande partie des méthodes présentées ici sont *cassables*, comme le chiffrement par permutation. En revanche, nous en avons vu qui résiste encore comme RSA, le chiffrement El Gamal. Chacune de ces méthodes ont des forces et des faiblesses. Pour étudier ces méthodes plus en détail, le lecteur peut s'intéresser au domaine de la cryptographie qui s'appelle la *cryptanalyse*.

Comme vous avez pu le constater les méthodes de chiffrements à clef publique se basent soit sur le problème du logarithme discret soit sur le problème de factorisation d'un nombre. Ce qui motive les recherches académiques dans ces domaines car cela peut engendré des attaques sur certaines méthodes de chiffrement. Par conséquent, la cryptographie est un domaine vivant qui nécessite de la vigilance au sujet des recherches en cours.

Actuellement, les méthodes cryptographiques les plus évoluées sont basées sur les *courbes elliptiques* dont nous ne pouvons parler dans le cadre de ce cours de BUT Informatique car cela nécessite une certaine quantité de connaissances assez poussées en algèbre. Néanmoins, nous pouvons dire que ces méthodes sont basées sur le problème du logarithme discret dans un groupe de point d'une courbe elliptique.

Cette introduction aux méthodes cryptographiques étant terminés je vous recommande de vous documenter soit sur le net ou en bibliothèque. Si le lecteur souhaite continuer dans le domaine de la cryptographie, il y a plusieurs master en cryptographie en France pour ne citer que Bordeaux et Paris.