Travaux d'Études et de Recherches : CRYPTOGRAPHIE.

BARRE Magalie

11 juin 2005

Table des matières

1 Remerciements. 3

2 Introduction. 4

3 Structures algébriques. 5
3.1 Généralités sur les Groupes, Anneaux, Idéaux, Corps et Morphismes . 5
3.1.1 Groupes . . . 5
3.1.2 Anneaux . . . 6
3.1.3 Idéaux . . . 8
3.1.4 Anneaux euclidiens et principaux . . . 11
3.1.5 Généralités sur les corps. . . . 11
3.2 Quelques résultats fondamentaux. . . . 13

4 Théorèmes d'Arithmétique classique. 16
4.1 Etude de l'anneau $\mathbb{Z}$. . . . 16
4.1.1 Propriétés de $\mathbb{Z}$. . . . 16
4.1.2 Divisibilité dans l'anneau $\mathbb{Z}$. . . . 16
4.1.3 Théorèmes d'Arithmétique. . . . 18
4.2 Etude de l'anneau $\mathbb{Z}/n\mathbb{Z}$ . . . 19
4.3 Polynômes Cyclotomiques. . . . 22
4.3.1 Fonction de Möbius. . . . 22
4.3.2 Polynômes Cyclotomiques. . . . 23

5 Etude de l'anneau $\mathbb{F}_p[X]$ et construction de corps finis. 24
5.1 Rappels sur les corps de rupture et de décomposition d'un polynôme. 24
5.2 Clôture algébrique d'un corps. . . . 25
5.3 Corps finis . . . 26
5.3.1 Extensions de corps finis . . . 26
5.3.2 Structure de $\mathbb{F}_p$ -e.v. . . . 26
5.3.3 Polynômes irréductibles sur $\mathbb{F}_p$ avec p premier . . . 27
5.4 Preuve du Théorème de Wedderburn . . . 31

6 Tests de primalité et de composition. 33
6.1 Nombres premiers et congruences . . . 33
6.1.1 Tests de divisibilité . . . 33
6.1.2 Nombres pseudopremiers . . . 34
6.1.3 Nombres de Mersenne . . . 35

6.1.4 Nombres de Fermat . . . 36
6.2 Tests déterministes . . . 36
6.2.1 Le $(n-1)$-test. . . . 36
6.2.2 Le $(n+1)$-test. . . . 37
6.3 Tests probabilistes . . . 38
6.3.1 Test de Solovay-Strassen . . . 38
6.3.2 Test de Miller-Rabin . . . 39

7 Fondements de la Cryptographie. 43
7.1 Cryptographie à clé secrète . . . 43
7.1.1 Schémas de chiffrement à flot . . . 44
7.1.2 Schémas par blocs . . . 48
7.2 Cryptographie à clé publique . . . 50
7.2.1 Problèmes difficiles et fonctions à sens unique. . . . 50
7.2.2 Factorisation entière. . . . 51
7.2.3 L'exponentiation modulaire . . . 53
7.2.4 Le protocole de Diffie-Hellman . . . 54
7.2.5 Le système d'El Gamal . . . 55
7.2.6 Le système RSA . . . 56
7.3 Application au cryptosystème à clé publique RSA. . . . 60
7.3.1 Création des clés . . . 60
7.3.2 Algorithme de cryptage . . . 61
7.3.3 Algorithme de décryptage . . . 61
7.3.4 Sécurité du système . . . 62
7.3.5 Implémentation de RSA . . . 62

8 Conclusion 68

A Preuves des tests 69
A.1 Test de primalité de Lucas-Lehmer . . . 69
A.2 Critère de primalité de Lucas-Lehmer . . . 69
A.3 Preuve du test de Miller-Rabin . . . 70

B Fonction indicatrice d'Euler 72

C Quelques polynômes cyclotomiques 73

D Algorithme d'Euclide étendu 75

Chapitre 1

Remerciements.

- Je remercie Monsieur Abdelmajid BAYAD pour m'avoir proposé ce sujet et d'avoir accepté de m'encadrer. La gentillesse et la disponibilité dont il a fait preuve à mon égard m'ont beaucoup touchée.

- Je remercie également Monsieur François DELBOT pour sa relecture attentive et pour ses conseils.

Chapitre 2

Introduction.

Le besoin de protection de l'information est aussi ancien que la civilisation elle-même. D'abord, exclusivement utilisée par les militaires et les diplomates, elle a acquis avec l'apparition des réseaux informatiques une quantité d'applications commerciales, par exemple, l'intégrité des échanges dans une transaction financière doit être garantie. Clairement, l'utilisateur d'un tel système demandera à ce que toute information échangée soit confidentielle et la personne qui fournit un tel système voudra exclure l'utilisation frauduleuse du système.
Un autre problème peut être rencontré : l'authentification. En effet, comment pouvons-nous savoir si le message envoyé a vraiment été écrit par la personne qui prétend en être l'auteur ? Dans ce cas, nous verrons qu'il est possible de signer son message.

Le but de ce TER est d'étudier les tests de primalité et de composition et leurs applications aux cryptosystèmes.
D'une façon précise, ce TER se compose de deux parties : une théorique et une pratique. Dans la première partie qui regroupe les trois premiers chapitres, nous étudierons toutes les notions de structures de groupes, anneaux et corps ; les théorèmes fondamentaux d'arithmétique sur $\mathbb{Z}$ ainsi que la théorie des corps finis - existence et construction - et leurs preuves.
Dans la seconde partie constituée des deux derniers chapitres, nous étudierons de façon théorique et pratique :

- les tests de primalité et de composition : déterministes et probabilistes,
- la Cryptographie et son application au cryptosystème RSA.

Chapitre 3

Structures algébriques.

Dans ce chapitre, nous rappelons les notions de groupes, anneaux et corps et nous en donnons ensuite quelques théorèmes fondamentaux qui vont nous servir dans la suite de ce mémoire.

3.1 Généralités sur les Groupes, Anneaux, Idéaux, Corps et Morphismes

3.1.1 Groupes

Définition 1
Un groupe *est la donnée d'un couple (G,$*$) où :*
- *G est un ensemble non vide,*
- *$*$ est une loi de composition interne de G vérifiant :*
  1. *$*$ admet un élément neutre e,*
  2. *$*$ est associative,*
  3. *Tout élément de G admet un symétrique par la loi $*$.*

De plus, (G,$*$) est dit ***groupe abélien*** *si la loi $*$ est commutative.*

Définition 2
Un morphisme de groupes $\varphi : (G_1 , *) \longrightarrow (G_2 , T)$ est une application vérifiant :

$$\varphi(x * y) = \varphi(x) \ T \ \varphi(y) \ , \ \forall \ x, y \in G_1.$$

Conséquence 1

1. $Ker \ \varphi \lhd G_1$.
2. $Im \ \varphi < G_2$.
3. $\varphi(e_{G_1}) = e_{G_2}$.
4. $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Définition et proposition 1 (Groupe quotient)
Soit (G,$*$) un groupe et $H \lhd G$.
Il existe une structure de groupe sur $G_{/H}$ induite de celle de (G,$*$) notée ($G_{/H}$,$\overline{*}$) un groupe.

Exemple 1
$(\mathbb{Z}, +)$ est un groupe abélien et si on considère $H = n.\mathbb{Z}$ où $n \geq 1$
Alors $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}\right)$ est un groupe abélien.

3.1.2 Anneaux

Définition 3 (Anneau)

1. *Un **anneau** est la donnée d'un triplet (A,+,×) où A est un ensemble muni de deux lois de composition internes, notées + et ×, vérifiant :*
   - *(A,+) est un groupe abélien.*
   - *La loi × est associative et distributive par rapport à la loi +*
     ***c'est-à-dire** : $\forall\, x, y, z \in A,\ x \times (y + z) = x \times y + x \times z$.*
2. *Soit $A' \subset A$ où (A,+,×) est un anneau.*
   *On dit que A' est un **sous-anneau** s'il vérifie : $(A', +, \times)$ a une structure d'anneau.*
3. *L'anneau (A,+,×) est dit **commutatif** si la loi × est commutative.*
4. *L'anneau (A,+,×) est dit **unitaire** si la loi × admet un élément neutre.*
5. *L'anneau (A,+,×) est dit **intègre** s'il vérifie :*
   $\forall\, x, y \in A : x \times y = 0 \quad \Leftrightarrow \quad x = 0$ ou $y = 0$.
   *Sinon, il existe x,y ∈ A non nuls tels que x×y = 0. Dans ce cas, x et y sont appelés **diviseurs de zéro**.*

Exemple 2 *$(\mathbb{Z}/7\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif, unitaire et intègre.*

Proposition 1
Soit (A,+,×) un anneau unitaire.
L'ensemble des éléments inversibles (symétriques pour la loi ×), c'est-à-dire $A^{\times} = \{x \in A / \ \exists\, y \in A \ : \ y \times x = x \times y = 1_A\}$, a une structure de groupe.
*Il est également appelé **groupe des unités de A** s'il est muni de la multiplication et il est noté $U(A)$.*

Proposition 2

1. *Toute intersection de sous-anneau est un anneau.*
2. *Tout sous-anneau d'anneau commutatif (respectivement intègre) est commutatif (respectivement intègre).*

Remarque 1 *Une réunion de sous-anneau n'est pas forcément un sous-anneau.*

Proposition 3
Soit $(A, +, \times)$ un anneau.
Soit $S \subset A$ non vide.
*Alors le plus petit sous-anneau de A contenant S existe et est égal à l'intersection de tous les sous-anneaux de A contenant S, appelé **sous-anneau de A engendré par S**.*

En pratique : $(A, +, \times)$ est un anneau commutatif, unitaire ; B un sous-anneau de A unitaire et $s \in A$.
Alors le plus petit sous-anneau de A contenant $S = B \cup \{s\}$ est

$$\left\{ \sum_{finie} b_i s^i \ / \ b_i \in B \right\} \ = \ B[s] \, .$$

Remarque 2 *La somme de deux sous-anneaux n'est pas forcément un sous-anneau.*

Exemple 3 $\mathbb{Z}[i] + \mathbb{Z}[\frac{1}{2}]$ *n'est pas un sous-anneau car* $\frac{i}{2} \notin$ *à cet ensemble.*

Définition 4 (Morphisme d'anneaux)
Soient $(A_1, +, \times)$ *et* $(A_2, +, \times)$ *deux anneaux.*
Un ***morphisme d'anneaux*** *entre* A_1 *et* A_2 *est la donnée de* $f : A_1 \longrightarrow A_2$ *application qui vérifie :*

1. *Morphisme de groupes pour la loi + :* $f(x + y) = f(x) + f(y)$.
2. $f(x \times y) = f(x) \times f(y) \ , \ \forall \ x, y \in A_1$.

Si f est bijective alors f est dite ***isomorphisme d'anneaux****.*
On dit qu'on a un ***morphisme d'anneaux unitaires*** *si* $f(1_{A_1}) = 1_{A_2}$.

Définition 5 (Caractéristique d'un anneau)
Soit A un anneau.
Il existe un unique morphisme d'anneaux de $\mathbb{Z}$ *dans A : l'application f définie par* $f(n) = n1_A \ , \ \forall n \in \mathbb{Z}$.
$Ker \ f$ *est un idéal de* $\mathbb{Z}$ *donc il existe un unique entier naturel c (et un seul) tel que* $Ker \ f = c\mathbb{Z}$. *Comme* $f(1) = 1_A \neq 0$, *c est distinct de 1.*
Ce nombre ***c*** *est appelé la* ***caractéristique de l'anneau A*** *et on la note* ***c = carac(A)****.*

Remarques 1

1. $Im \ f = \{z.1_A \ , \ z \in \mathbb{Z}\} = \mathbb{Z}.1_A$ *est un sous-anneau de A et la décomposition canonique du morphisme f montre que* $Im \ f$ *est isomorphe à* $\mathbb{Z}/c\mathbb{Z}$.
2. *Si* $carac(A) \neq 0$ *alors* $carac(A)$ *est l'ordre additif de l'élément* 1_A.
3. *Un anneau et un quelconque de ses sous-anneaux ont la même caractéristique.*

Proposition 4
Soit A un anneau intègre.

1. *Si A contient un sous-anneau isomorphe à* $\mathbb{Z}$, *A est dit de* ***caractéristique 0****.*
2. *Si A contient un corps isomorphe à* $\mathbb{Z}/p\mathbb{Z}$, *A est dit de* ***caractéristique p****.*

3.1.3 Idéaux

Définition 6
Soit $(A, +, \times)$ un anneau et soit $I \subset A$.

1. *I est un **idéal à gauche** (respectivement à droite) de A si et seulement si :*
   - *I est un sous-groupe abélien de A pour la loi (+) c'est-à-dire $\forall x, y \in I$, $x - y \in I$.*
   - *$\forall a \in A$, $\forall x \in I$: $a.x \in I$ (respectivement $x.a \in I$).*
2. *I est un **idéal bilatère** ssi I est un idéal à gauche et à droite.*
3. *I est un **idéal strict ou propre** si $I \neq A$.*
4. *I est un **idéal premier** ssi $\forall x, y \in A$, $x.y \in I \quad \Rightarrow \quad x$ ou $y \in I$.*
   L'ensemble des idéaux premiers est le spectre de A, noté Spec(A).
5. *Si I est un idéal bilatère.*
   *On dit que I est **maximal** s'il est strict et s'il n'est contenu dans aucun autre idéal que l'anneau tout entier.*
   L'ensemble des idéaux maximaux de A est le spectre maximal de A, noté Max(A).

Proposition 5
Soit (A,+,×) un anneau unitaire. Soit I un idéal de A.
***Si** I contient l'élément unité de A ou un élément inversible de A **alors** $\boxed{I = A}$.*

Proposition 6
Dans un anneau, une intersection d'idéaux bilatères est un idéal bilatère.

Théorème 1 (Théorème de Krull)
Soit (A,+,×) un anneau commutatif, unitaire.
Alors tout idéal propre de A est contenu dans un idéal maximal.

Définition 7 (Somme et produit d'idéaux)
Soit (A,+,×) un anneau et soient I et J deux idéaux bilatères de A.
On note :

1. *$I + J = \{a + b \ / \ a \in I \ , \ b \in J\}$ est le plus petit idéal contenant I et J.*
2. $$I.J = \left\{ \sum_{somme \ finie \ selon \ i} a_i b_i \ / \ a_i \in I \ , \ b_i \in J \right\}$$
   est l'idéal engendré par les produits $a.b$ / $a \in I$ et $b \in J$.

Définition 8
Soit $(A,+,\times)$ un anneau unitaire et soit I un idéal de A.

1. *I est dit **principal** s'il est engendré par un seul élément.*
   (I est de la forme $I = s.A$ ou $A.s$ où $s \in A$)
2. *I est dit **de type fini** s'il existe $S \subset A$ finie engendrant I (c'est-à-dire : $I = S.A$ ou $A.S$).*
   On le notera (S) quand l'idéal est bilatère.

Proposition 7 (Im et Ker)
Soit $f : (A,+,\times) \longrightarrow (B,+,\times)$ un morphisme d'anneaux.
On a $Ker\ f = \{a \in A\ /\ f(a) = 0\}$ (noyau de f) et $Imf = f(A)$ (image de f).
Alors

- *$Ker\ f$ est un idéal bilatère de A.*
- *$Im\ f$ est un sous-anneau de B.*

Proposition 8
Soit $f : A \longrightarrow B$ un morphisme d'anneaux.

1. *Si I est un idéal bilatère alors $f^{-1}(I)$ est un idéal bilatère.*
2. *Si I est un idéal premier alors $f^{-1}(I)$ est un idéal premier.*

Remarque 3 *Ceci n'est pas vrai pour un idéal maximal.*

Proposition 9
Soit $(A,+,\times)$ un anneau et I un idéal bilatère.
On considère la relation d'équivalence : $xRy \Longleftrightarrow x - y \in I$.
L'ensemble des classes d'équivalence noté $A/_R$ peut être muni d'une structure d'anneau de la façon suivante :

$$\forall\ \overline{x},\overline{y} \in A/_R,\quad \overline{x} \dot{+} \overline{y} = \overline{x \dot{+} y} \quad et \quad \overline{x}\ .\ \overline{y} = \overline{x.\dot{y}}.$$

*Cet anneau est appelé **anneau quotient associé à I** qu'on notera $A/_I$.*

Théorème 2 (Théorème de transfert)
Soit A un anneau et soit I un idéal bilatère.
On a :

1. *A commutatif $\Rightarrow$ $A_{/I}$ commutatif.*
2. *A unitaire $\Rightarrow$ $A_{/I}$ unitaire.*

Théorème 3
Soit A un anneau unitaire et soit I un idéal bilatère.
On a :

1. *$A_{/I}$ intègre $\Leftrightarrow$ I premier dans A.*
2. *$A_{/I}$ corps $\Leftrightarrow$ I maximal dans A.*

Définition 9 (Factorisation)
Soient $A \xrightarrow{f} B$ et $A \xrightarrow{g} C$ deux morphismes d'anneaux.
On dira que ***f se factorise à travers g*** *s'il existe un morphisme d'anneaux : $C \xrightarrow{h} B$ tel que* $\boldsymbol{f = h \circ g}$.

Théorème 4 (Factorisation)
$A \xrightarrow{f} B$ et $A \xrightarrow{s} A/Ker\ f$ sont deux morphismes d'anneaux et f se factorise à travers s (surjection canonique) c'est-à-dire :

$$\exists \bar{f} \text{ tel que : } \begin{array}{ccc} A/Ker\, f & \longrightarrow & B \\ \bar{x} & \longmapsto & f(x) \end{array}$$

Précisément :

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle i} \\ A/_{Ker f} & \xrightarrow{\bar{f}} & f(A) \end{array}$$

où
- *i est une injection telle que $\forall y \in f(A)\ ,\ i(y) = y$*
- *s est une surjection telle que $\forall \bar{x} \in A\ ,\ s(\bar{x}) = \bar{x}$*

Alors : $\boxed{\boldsymbol{f = i \circ \bar{f} \circ s}}$ *factorisation de f.*

Théorème 5 (Propriété universelle du quotient)
Soient A et B deux anneaux.
Soit $f : A \longrightarrow B$ un morphisme d'anneaux.
Soit I un idéal bilatère de A.

$$\text{Soit } s_I : \begin{array}{ccc} A & \longrightarrow & A/_I \\ x & \longmapsto & \text{classe de } x \text{ modulo } I \end{array}$$

Alors f se factorise à travers $s_I \iff I \subset Ker\ f$.

3.1.4 Anneaux euclidiens et principaux

Définition 10 (Anneau euclidien)
*On dit qu'un anneau A est **euclidien** s'il est intègre et s'il existe une application $\delta : A\backslash\{0\} \to \mathbb{N}$, appelée stathme, telle que pour tous éléments a et b, avec $b \neq 0$, il existe des éléments q et r tels que l'on ait :*

$$a = bq + r \quad et \quad (r = 0 \ ou \ \delta(r) < \delta(b)).$$

*Une telle application est dite **division euclidienne sur A**.*

Définition 11 (Anneau principal)
*On dit qu'un anneau est **principal** s'il est intègre et si tous ses idéaux sont principaux.*

Lemme 1
Toute suite croissante d'idéaux dans un anneau principal est stationnaire.

Théorème 6
*Si A est un anneau euclidien alors il est **principal**.*

Tous les anneaux considérés dans ce mémoire sont des anneaux commutatifs et unitaires. De plus, tous les corps étudiés sont commutatifs.

3.1.5 Généralités sur les corps.

Corps.

Définition 12
*Un **corps** est la donnée d'un triplet $(K,+,\times)$ tel que :*

1. *K n'est pas réduit à $\{0\}$.*
2. *$(K,+,\times)$ est un anneau unitaire.*
3. *Tout élément de $K\backslash\{0\}$ est inversible pour la loi $\times$.*

*On dit que $(K,+,\times)$ est un corps **commutatif** si la loi $\times$ est, de plus, une loi commutative.*

Remarque 4 *Si $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ est un corps commutatif $\iff$ n est premier.*

Proposition 10
Soit $(K,+,\times)$ un corps.
On a alors : $(K,+,\times)$ est un anneau intègre et $1 \neq 0$.

Proposition 11
Tout anneau intègre, fini et non réduit à $\{0\}$ est un corps.

Proposition 12
*Soit A un anneau alors A est un **corps** ssi ses seuls idéaux sont $\{0\}$ et A.*

Proposition 13
Soit $f : K \longrightarrow A$ un morphisme d'anneaux où K est un corps et A un anneau non réduit à $\{0\}$.
On a alors :

1. *f est injectif ou nul.*
2. *Si, de plus, A est un corps et $f \neq 0$ alors f est dit **morphisme de corps**.*

Sous-corps.

Définition 13
Soit K un corps. Soit P une partie de K.
Les conditions suivantes sont équivalentes :

1. *P est non vide, est une partie stable (pour les lois $+$ et $\times$) de K et P muni des lois induites par celles de K est lui-même un corps.*
2. *P est un sous-anneau de K, $1 \in P$ et $(x \in P \Rightarrow x^{-1} \in P)$.*
3. *P est un sous-groupe de $(K, +)$ et $P^* = P \setminus \{0\}$ est un sous-groupe du groupe multiplicatif $(K^*, \times)$.*

*On dit alors que **P est un sous-corps de K**.*

Exemples 1
- *$\mathbb{Q}$ est un sous-corps de $\mathbb{R}$.*
- *$\mathbb{R}$ est un sous-corps de $\mathbb{C}$.*

Proposition 14
Soit K un corps.
Toute intersection de sous-corps de K est un sous-corps de K.

Proposition 15
Soit K un corps. Soit T une partie de K.
*L'ensemble E des sous-corps de K qui contiennent T est non vide et possède, au sens de l'inclusion, un élément minimum : ce minimum est appelé le **sous-corps de K engendré par T**.*

Caractéristique d'un corps.

Définition 14 (Caractéristique d'un corps)
Soit K un corps.
Soit $\Phi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & K \\ m & \mapsto & m.1_K \end{array}$ un morphisme d'anneaux.
*La **caractéristique de K** est le générateur positif de $Ker\ \Phi$ qu'on note : $Carac(K)$.*

Exemples 2

1. *Soit* $K = \mathbb{Q}$, $\mathbb{R}$ *ou* $\mathbb{C}$.

$$\begin{aligned} Ker\ \Phi &= \{m \in \mathbb{Z} \ :\ m.1 = 0\} \\ &= \{0\} \end{aligned}$$

Donc $\boxed{Carac(K) = 0 = Carac(\mathbb{Q}) = Carac(\mathbb{R}) = Carac(\mathbb{C}).}$

2. *Soit* $K = \mathbb{Z}/p\mathbb{Z}$ *où* p *est premier.*

$$\begin{aligned} Ker\ \Phi &= \{m \in \mathbb{Z} \ :\ m.\bar{1} = \bar{0}\} \\ &= \{m \in \mathbb{Z} \ :\ \bar{m} = \bar{0}\} \\ &= \{m \in p\mathbb{Z}\} \\ &= p\mathbb{Z} \end{aligned}$$

Donc $\boxed{Carac(K) = Carac(\mathbb{Z}/p\mathbb{Z}) = p.}$

Définition 15
Un corps K *est dit* ***premier*** *s'il est égal à* $\mathbb{Q}$ *ou à l'un des corps* $\mathbb{Z}/p\mathbb{Z}$ *avec* p *premier.*

Remarques 2

1. *Le plus petit corps isomorphe à* $\mathbb{Z}$ *de caractéristique 0 est* $\mathbb{Q}$.
2. *Le plus petit corps isomorphe à* $\mathbb{Z}$ *de caractéristique* p *est* $\mathbb{Z}/p\mathbb{Z}$ *où* p *est premier.*

Théorème 7
Soit K *un corps.*
Alors on a *:*

1. $Carac(K) = 0$ *ou à un nombre premier.*
2. *Soit* L *un corps tel que* $f \ :\ K \longrightarrow L$ *est un morphisme d'anneaux non nul* <u>*alors*</u> *:* $Carac(K) = Carac(L)$.

3.2 Quelques résultats fondamentaux.

Théorème 8 (Lagrange)
Soit (G,) un groupe fini de cardinal n.*
Soit H un sous-groupe de G d'ordre k.
<u>*Alors*</u> *k divise n.*

En particulier *: l'ordre de tout élément de G divise l'ordre de G.*

Preuve 1
Soit $\mathcal{R}_1$ la relation d'équivalence de congruence à droite modulo H.

Les classes d'équivalence pour $\mathcal{R}_1$ forment une partition de G.
Soient $\bar{x_1}, \ldots, \bar{x_l}$ toutes les classes pour $\mathcal{R}_1$, deux à deux distinctes.
Donc : $G = \bar{x_1} \cup \ldots \cup \bar{x_l}$.
D'où : Card G = Card($\bar{x_1}$)+ Card($\bar{x_2}$)+ ... + Card($\bar{x_l}$).

Or *Card($\bar{x_i}$) = Card(H) par la proposition précédente.*
Donc $Card\ G\ =\ \underbrace{Card\ H + \ldots + Card\ H}_{l\ fois}$.
Donc $\boxed{n\ =\ lk}$.

Donc $\boldsymbol{k\ divise\ n\ et\ q\ =\ \frac{n}{k}\ nombre\ des\ classes\ pour\ \mathcal{R}_1}$.

Théorème 9 (Théorème chinois)
Soient A un anneau unitaire, I et J deux idéaux bilatères de A.
Si $I\ +\ J\ =\ A$ *(on dit que* ***I et J sont étrangers entre eux*** *).*
Alors : $\boldsymbol{A/_{I\cap J}}$ *et* $\boldsymbol{A/_I \times A/_J}$ *sont isomorphes et sont deux anneaux unitaires.*

Preuve 2

Soit $\varphi :\quad \begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z}\ \times\ \mathbb{Z}/n\mathbb{Z} \\ x\ (mod\ mn) & \longmapsto & (x\ mod\ m\ ,\ x\ mod\ n) \end{array}$

Il faut prouver que φ est un morphisme de groupe bijectif.

- *φ morphisme ?*

$$\begin{array}{rcc} \varphi\left(x(mod\ mn) + y(mod\ mn)\right) & = & \varphi\left((x+y)\,(mod\ mn)\right) \\ & = & \left((x+y)\,(mod\ m)\ ,\ (x+y)\,(mod\ n)\right) \\ & = & (x(mod\ m)\ ,\ x(mod\ n))\ +\ (y(mod\ m)\ ,\ y(mod\ n)) \\ & = & \varphi\left(x(mod\ mn)\right) + \varphi\left(y(mod\ mn)\right) \end{array}$$

Donc $\boxed{\boldsymbol{\varphi\ est\ un\ morphisme\ de\ groupe.}}$

- *φ bijectif ?*
Comme c'est une application de deux ensembles finis de même cardinal alors il suffit de montrer que l'application est soit injective, soit surjective.

Nous allons montrer ici qu'elle est injective :
c'est-à-dire :

$$\varphi\left(x(mod\ mn)\right)\ =\ \varphi\left(y(mod\ mn)\right) \Longleftrightarrow \left\{ \begin{array}{rcl} x(mod\ m) & = & y\ (mod\ m) \\ & et & \\ x(mod\ n) & = & y\ (mod\ n) \end{array} \right.$$

$$\Longleftrightarrow \begin{cases} x & = & y \ (mod\ m) & \leftrightarrow & m \mid x-y \\ x & = & y \ (mod\ n) & \leftrightarrow & n \mid x-y \end{cases}$$

Comme $(m,n)=1$ *alors* $mn \mid x-y$.
Donc $x = y \ (mod\ mn)$.

Conclusion : φ est un isomorphisme et donc le théorème Chinois est prouvé.

Théorème 10 (Equation des classes)
Soit G un groupe fini noté multiplicativement.
Soit Z(G) son centre tel que $Z(G) = \{x \in G \ / \ \forall\ y \in G\ ,\ xy = yx\}$.
Soit Ω *l'ensemble des classes de conjugaison non réduites à un singleton.*
Soit, pour chaque $x \in G$, $S_x = \{g \in G \ / \ g^{-1}xg = x\}$ *le stabilisateur de x.*

Alors $\mid G \mid = \mid Z(G) \mid + \sum_{C \in \Omega} \frac{|G|}{|S_x|}$ *(somme dans laquelle on prend un et un seul élément x dans chacune des classes C de* Ω*).*

Preuve 3

On fait opérer G sur lui-même par les automorphismes intérieurs γ_g : $\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & g^{-1}xg \end{array}$
avec $g \in G$.

On obtient ainsi une partition de G en un nombre fini d'orbites : on appelle ***orbite de x*** *la partie* $\{\gamma_g(x), g \in G\}$ *de G.*

L'orbite de x est réduite à $\{x\}$ ***si et seulement si*** $x \in Z(G)$. *Il existe donc* $\mid Z(G) \mid$ *orbites réduites à un singleton ; l'ensemble des autres constitue* Ω.

Pour chaque C de Ω, *prenant* $x \in C$, *on a* $C = \{\gamma_g(x), g \in G\}$ *et l'application* $\begin{array}{ccc} G & \longrightarrow & C \\ g & \longmapsto & \gamma_g(x) \end{array}$ *est surjective.*

Or, chaque tranche est de la forme gS_x *donc a pour cardinal* $\mid S_x \mid$.
Donc $Card(C) = \frac{|G|}{|S_x|}$ *est égal à l'indice dans G du sous-groupe* S_x *stabilisateur de x.*
D'où on obtient la formule donnée.

Théorème 11 (Théorème de Wedderburn)
Tout corps fini est commutatif.

Preuve 4
Cette preuve sera faite après le chapitre sur les Corps finis.

Chapitre 4

Théorèmes d'Arithmétique classique.

4.1 Etude de l'anneau $\mathbb{Z}$.

4.1.1 Propriétés de $\mathbb{Z}$.

Théorème 12

1. *L'anneau $(\mathbb{Z},+,\times)$ est un* ***anneau commutatif, unitaire et intègre****.*
2. *Les* ***éléments inversibles*** *de cet anneau sont 1 et -1.*
3. *L'anneau $\mathbb{Z}$ est* ***euclidien*** *pour le stathme $a \mapsto \mid a \mid$ où*

$$|a| = \begin{cases} a \text{ si } a \in \mathbb{N} \\ -a \text{ sinon} \end{cases}$$

qui satisfait les propriétés suivantes :

$$|a + b| \leq |a| + |b| \quad et \quad |ab| = |a|\,|b|\,.$$

4. *L'anneau $\mathbb{Z}$ est* ***principal****, plus précisément tout idéal I de $\mathbb{Z}$ est de la forme $n.\mathbb{Z}$ avec $n \in \mathbb{N}$ et :*
   - *l'idéal I est* ***premier*** *ssi $n = 0$ ou si n est un nombre premier.*
   - *I est* ***maximal*** *ssi n est premier.*

4.1.2 Divisibilité dans l'anneau $\mathbb{Z}$.

On pose $\mathrm{A} = \mathbb{Z}$.

Définition 16
Soit A un anneau intègre et soient $a \in A$, $b \in A \setminus \{0\}$.

1. *On dit que* ***b divise a****, noté $b \mid a$, s'il existe $c \in A$ tel que $a = b.c$.*
2. *Pour $a \neq 0$, a est dit* ***irréductible*** *si et seulement si a est premier.*
3. *Soit $x \in A \setminus \{0\}$, $u \in A^{\times}$: les éléments x.u sont les* ***associés de x****.*

4. *Un élément $p \in A$, $p \neq 0$, $p \in A^\times$ est dit* ***premier*** *si* $p \mid a.b \Rightarrow p \mid a$ *ou* $p \mid b$, $\forall\ a, b \in A$.

Lemme 2
Si A est un anneau intègre et $p \in A$, $p \neq 0$, $p \notin A^\times$
Alors p premier $\iff$ (p) est un idéal premier.

Lemme 3
Si A est un anneau intègre et $a, b \in A \setminus \{0\}$
Alors a et b sont associés $\iff a \mid b$ et $b \mid a$.

Lemme 4
Si A est un anneau intègre et $a \in A$, $p \neq 0$, $p \notin A^\times$
Alors on a : p premier $\Longrightarrow$ p irréductible.

Lemme 5 (Euclide)
Pour a,b $\in A$, $p \in P$, on a : $p \mid ab \iff p \mid a$ ou $p \mid b$.

Définition 17 (PGCD)
Soient b, c, $d \in A$, d est un pgcd de b et de c ***ssi*** *:*

1. $d \mid b$ *et* $d \mid c$.
2. $\forall a \in A\ :\ a \mid b$ *et* $a \mid c \Longrightarrow a \mid d$.

Définition 18 (PPCM)
Soient b, c, $m \in A$, m est un ppcm de b et de c ***ssi*** *:*

1. $b \mid m$ *et* $c \mid m$.
2. $\forall a \in A\ :\ b \mid a$ *etc* $\mid a \Longrightarrow m \mid a$.

Lemme 6
Soient b, c, d, $m \in A$ où d est un pgcd de b et c et m est un ppcm de b et c.
On a : $bc = dm$ (à inversible près).

Lemme 7 (Gauss)
Soient a, b, $c \in A$ et d un pgcd de a et b.
On a : $(a \mid bc$ et $(a, b) = 1) \Longrightarrow a \mid c$.

Théorème 13
Soit A un anneau principal.
Soient a, b, $d \in A$ où $a \neq 0$.
On a : d est un pgcd de a et b dans $A \iff (d) = (a, b)$.

4.1.3 Théorèmes d'Arithmétique.

Théorème 14 (Bezout)
Soient $n_1, \ldots, n_r$ des entiers naturels non nuls.
L'ensemble

$$H = \left\{ \sum_{i=1}^{r} a_i \times n_i \ / \ a_i \in \mathbb{Z} \right\}$$

est un sous-groupe de $(\mathbb{Z},+)$ qui est égale à $d.\mathbb{Z}$ où $d = pgcd(n_1, \ldots, n_r)$.

Cas particuler :
Si $r = 2$ alors on pose : $n_1 = a$ et $n_2 = b$.
Le théorème de Bezout s'écrit alors :
*Deux entiers quelconques a et b sont premiers entre eux **ssi** $\exists$ u et $v \in \mathbb{Z}$ tels que : $a \times u + b \times v = 1$.*
De plus, $H = \mathbb{Z}$ et $d = pgcd(a,b) = 1$.

Preuve 5
On cherche à prouver que l'ensemble H s'écrit sous la forme suivante :
$H = n_1\mathbb{Z} + \ldots + n_2\mathbb{Z} = d.\mathbb{Z}$ où $d = pgcd(n_1, \ldots, n_r)$.

H est un sous-groupe de $(\mathbb{Z},+)$ car
- *H est non vide,*
- *H est stable par la loi (+),*
- *Tout élément de H admet un élément symétrique.*

***D'après le théorème précédent**, H est de la forme $n\mathbb{Z}$ c'est-à-dire $H = n\mathbb{Z}$ où $n \geq 0$. Or H n'est pas réduit à 0 : $n_1, \ldots, n_r \in H$ (non nuls).*
D'où $n > 0$.

On sait aussi que $d = pgcd(n_1, \ldots, n_r)$ donc $d|n_1, \ldots, d|n_r$.
Donc $d|x, \forall x \in H = n\mathbb{Z}$.
En particulier, $n \in H$ d'où $d|n \implies d \leq n$.

***Il reste à montrer que $n|d$** :*
Faisons une division euclidienne de d par n : $d = nq + r$ avec $0 \leq r \leq n$ et n est un diviseur commun des $n_i \implies n \leq d$.

$\boxed{\underline{Conclusion} : n = d \text{ et } H = d.\mathbb{Z}}$.

4.2 Etude de l'anneau $\mathbb{Z}/n\mathbb{Z}$

On note $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}\ ,\ \overline{1}\ ,\ \ldots\ ,\ \overline{n-1}\}$ l'ensemble des classes de congruence.

Théorème 15

1. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un* ***anneau commutatif, unitaire*** *à n éléments.*
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un* ***anneau intègre*** *si et seulement si n est premier avec* $n \in \mathbb{N}$ *et* $n \geq 2$.
3. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un* ***corps*** *si et seulement si n est premier.*
4. *Les* ***éléments inversibles*** *de* $\mathbb{Z}/n\mathbb{Z}$ *sont les* $\bar{a}$ *tels que a et n soient premiers entre eux c'est-à-dire :* $(a, n) = 1$.
5. *La caractéristique de l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est* $\boldsymbol{n}$.
6. *Les propriétés de divisibilité dans* $(\mathbb{Z}, +, \times)$ *restent les mêmes dans* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Remarque 5 (Terminologie) *Pour p un nombre premier,* $\mathbb{Z}/p\mathbb{Z}$ *est noté* $\mathbb{F}_p$ *qui est donc un corps fini de cardinal p.*

Nous avons besoin d'introduire, pour la suite de ce mémoire, la notion suivante :

Indicateur ou fonction d'Euler.

Définition 19
Pour tout entier naturel $n \geq 1$, *on note* G_n *l'ensemble des entiers naturels a tels que* $(1 \leq a \leq n$ *et* $(a, n) = 1)$.
On définit l'application $\varphi(n)\ :\ \mathbb{N}^* \longrightarrow \mathbb{N}^*$ *appelée* ***fonction indicatrice d'Euler*** *par :*

$$\begin{aligned} \varphi(n) &= Card(G_n) \\ &= Card\{\ a\ /\ 1 \leq a \leq n\ et\ (a, n)\ =\ 1\} \end{aligned}$$

où (a,n) est le pgcd positif de a et de n et $\forall n \in \mathbb{N}^*$.

Quelques propriétés de $\varphi(n)$:

1. φ est multiplicative **c'est-à-dire** si pgcd(m,n) = 1 alors $\varphi(m \times n) = \varphi(m) \times \varphi(n)$.
2. $\varphi(p) = p - 1$ si p est premier.
3. $\varphi(n) = n \times \prod_{p|n}(1 - \frac{1}{p})$ où p est premier.
4. $n = \sum_{d|n} \varphi(d)$, $n \in \mathbb{N}^*$. [**Formule de Gauss**]

Proposition 16
Soit $n \in \mathbb{N}$ où $n \geq 1$. Alors, on a :

1. *La classe $\bar{a}$ d'un entier a (mod n) est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$* ***ssi*** *$(a, n) = 1$.*
2. *$\varphi(n) = \mid (Z/nZ)^* \mid$.*

Preuve 6
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau principal.

Preuve du 1. :

$\boxed{\Rightarrow}$ *On suppose que la classe $\bar{a}$ d'un entier a(mod n) est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$*
$\Leftrightarrow \bar{a}\bar{u} = \bar{1}$ où $\bar{u}$ est la classe de b(mod n) symétrique de $\bar{a}$ pour la loi $\times$
$\Leftrightarrow 1\ (mod\ n) = au\ (mod\ n)$.
Donc, par le ***théorème de Bezout****, $\exists u, v \in \mathbb{Z}$ / $au + nv = 1$.*
Donc, a et n sont premiers entre eux : $\boldsymbol{(a, n) = 1}$.

$\boxed{\Leftarrow}$ *On suppose que $(a, n) = 1$.*
Alors, par le théorème de Bezout, $\exists u, v \in \mathbb{Z}$ / $au + nv = 1$
$\Rightarrow\ au + nv = 1\ (mod\ n)\ =\ 1\ (mod\ n)$
$\Rightarrow\ au(mod\ n)\ =\ 1\ (mod\ n)$.
On passe en classe dans $\mathbb{Z}/n\mathbb{Z}$: $\bar{1} = \bar{a}\bar{u}$.
Donc ***$\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ avec $\bar{u}$ son symétrique.***

Preuve du 2. :
Chaque élément de $\mathbb{Z}/n\mathbb{Z}$ est la classe d'un entier unique $a \in \mathbb{Z}$ / $1 \leq a \leq n$.
Comme $\varphi(n)\ =\ Card\{a\ /\ 1 \leq a \leq n$ et $(a, n) = 1\}$ et par 1, la classe $\bar{a}$ d'un entier a (mod n) est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ***si et seulement si*** *$(a, n) = 1$.*
Donc, $\varphi(n)\ =\ Card\{\ \bar{a}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$ / $1 \leq a \leq n\}$.
$\Rightarrow \varphi(n)\ =\ Card\ (\mathbb{Z}/n\mathbb{Z})^*$.
$\Rightarrow \boldsymbol{\varphi(n)\ = \mid (\mathbb{Z}/n\mathbb{Z})^* \mid}$.

Théorème 16 (Euler)
Soit $n \geq 2$ un entier naturel et soit $a \in \mathbb{Z}$.
Si a et n sont des entiers premiers entre eux alors, on a : $\boldsymbol{a^{\varphi(n)} \equiv 1 (mod\ n)}$.

Preuve 7
On suppose que a et n sont premiers entre eux.
On considère l'élément $\bar{a}$ du groupe fini de cardinal n $U(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
Par la proposition (16.1) *, on a supposé que a et n sont premiers entre eux* ***alors*** *$\bar{a}.u = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.*
D'après le ***théorème de Lagrange****, son ordre divise $\varphi(n)\ = \mid (\mathbb{Z}/n\mathbb{Z})^* \mid$.*
Donc $\bar{a}^{\varphi(n)} = \bar{1}$.
$\Longrightarrow \boldsymbol{a^{\varphi(n)} \equiv 1 (mod\ n)}$.

Remarque 6 *Comme, lorsque p est premier, $\varphi(n) = p - 1$, ce théorème d'Euler est une généralisation du Petit Théorème de Fermat dont voici l'énoncé :*

Corollaire 1 (Le Petit Théorème de Fermat)
Soit p un nombre premier.
Soit a un entier relatif non divisible par p.
Alors $a^{p-1} \equiv 1(mod\ p)$.

Théorème 17 (Théorème des restes chinois)
Soient n, m deux entiers naturels ≥ 2 et premiers entre eux.
Les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes.

Théorème 18 (Wilson)
Soit $p \in \mathbb{N}^*$.
p est ***premier*** *si et seulement si* $\boldsymbol{(p-1)! = -1(mod\ p)}$ *dans $\mathbb{Z}/p\mathbb{Z}$.*

4.3 Polynômes Cyclotomiques.

Pour pouvoir étudier les polynômes cyclotomiques, nous avons besoin d'introduire la notion suivante :

4.3.1 Fonction de Möbius.

Définition 20
La fonction de Möbius est définie par :

$$\begin{array}{rccc} \mu : & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \mu(n) \end{array} = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ possède un facteur carré} \\ (-1)^r & \text{si } n \text{ est un produit de } r \text{ premiers distincts deux à deux.} \end{cases}$$

Exemples 3
- $\mu(2^3) = 0$.
- $\mu(15) = \mu(3 \times 5) = (-1)^2 = 1$.

Théorème 19

1. $\mu(nm) = \mu(m) \times \mu(n)$ *si* $(m, n) = 1$.
2. $\forall n \geq 2$, $\sum_{d|n} \mu(d) = 0$.
3. ***Formule d'inversion :***
   Soit $(G, +)$ *un groupe abélien.*
   Soient $g : \mathbb{N}^* \longrightarrow G$ *et* $f : \mathbb{N}^* \longrightarrow G$ *avec* $f(n) = \sum_{d|n} g(d)$.
   Alors

$$\boxed{g(n) = \sum_{d|n} f(d)\ \mu(\frac{n}{d}).}$$

Exemple 4

Soit $G = (\mathbb{Z}, +)$ *et soient* $g : \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \varphi(n) \end{array}$ *et* $f : \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & n \end{array}$.

On a alors :

$$n = \sum_{d|n} \varphi(d) \quad et \quad \varphi(n) = \sum_{d|n} d\ \mu(\frac{n}{d}).$$

Théorème 20
Soient $n, r \in \mathbb{N}$ *; p premier et* $q = p^r$.
On note $I_q(n) = Card\{$ *P irréductible dans* $\mathbb{F}_q[X]$ *et degré de P* $= n\}$.
On a alors :

$$\boxed{I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d)\ q^{n/d}.}$$

4.3.2 Polynômes Cyclotomiques.

Soit $n \in \mathbb{N}^*$.

Définition 21
Le polynôme $\prod_{(k,n)=1 \ et \ 1\leq k\leq n} (X - e^{\frac{2i\pi k}{n}})$ *est le* $n^{ième}$ *polynôme cyclotomique que l'on note* $\Phi_n(X)$.
Il est de degré $\varphi(n)$ *où* $\varphi(n)$ *est la fonction d'Euler définie par :* $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$ *avec* p *premier et* $n \geq 2$.

Théorème 21
$\forall\ n \geq 2$ *et* $n \in \mathbb{N}$, *on a :*

1. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
2. $\Phi_n(X) \in \mathbb{Z}[X]$ *est irréductible sur* $\mathbb{Z}[X]$.
3. $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$.

Exemple 5
$X^{10} - 1 = \Phi_1(X)\Phi_2(X)\Phi_5(X)\Phi_{10}(X)$.

On cherche les Φ_i *?*

- $X - 1 = \Phi_1(X)$.
- $X^2 - 1 = \Phi_1(X)\Phi_2(X) \Longrightarrow \Phi_2(X) = X + 1$.
- $X^5 - 1 = \Phi_1(X)\Phi_5(X) \Longrightarrow \Phi_5(X) = X^4 + X^3 + X^2 + X + 1$.
- $X^{10} - 1 = \Phi_1(X)\Phi_{10}(X)$
  $\Longrightarrow$

$$\begin{aligned}
\Phi_{10}(X) &= \frac{X^{10} - 1}{(X - 1)(X + 1)(X^4 + X^3 + X^2 + X + 1)} \\
&= \frac{(X^5)^2 - 1}{(X + 1)(X^5 - 1)} \\
&= \frac{(X^5 + 1)(X^5 - 1)}{(X^5 - 1)(X + 1)} \\
&= \frac{X^5 + 1}{X + 1} \\
&= X^4 - X^3 + X^2 - X + 1
\end{aligned}$$

Donc $\boxed{X^{10} - 1 = (X - 1)(X + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 - X^3 + X^2 - X + 1)}$.

Chapitre 5

Etude de l'anneau $\mathbb{F}_p[X]$ et construction de corps finis.

5.1 Rappels sur les corps de rupture et de décomposition d'un polynôme.

Dans ce chapitre, dans un premier temps, nous montrons comment construire des extensions de degrés finis de corps et dans un second, nous l'appliquons pour la construction de corps finis.

Définition 22
Soit K un corps.
Soit $P \in K[X]$ un polynôme irréductible non constant.
Une extension L de K est appelée ***corps de rupture de P sur K*** *s'il existe dans L une racine x de P et $L = K[X]$.*

Proposition 17
Soit $P \in K[X]$ irréductible de degré n supérieur ou égal à 1.
L'anneau $L = K[X]/_{(P)}$ est un ***corps de rupture de P****, extension de degré n sur K, si on note x la classe de X dans L. On a : $L = K[X]$.*

Définition 23
Soit K un corps.
Soit $P \in K[X]$, non constant et de degré $n \in \mathbb{N}^*$.
Une extension L de K est dite ***corps de décomposition de P sur K*** *si et seulement si :*

1. *P est scindé dans L.*
2. *L est le plus petit corps vérifiant 1.*

On le note $\mathbb{D}_{\boldsymbol{K}}(\boldsymbol{P})$.

Théorème 22 (Propriété universelle pour un corps de rupture)
Soit K un corps et P un polynôme irréductible dans $K[X]$.

1. *Il existe un corps de rupture de P.*
2. *Si $L = K(\alpha)$ et $L' = K(\beta)$ sont deux corps de rupture du polynôme P, alors L et L' sont K-isomorphes. Plus précisément, il existe un unique K-isomorphisme $t : L \longrightarrow L'$ tel que $t(\alpha) = \beta$.*

Théorème 23 (Propriété universelle pour un corps de décomposition)
Soit $P \in K[X]$ irréductible sur K alors pour toute extension M de K et pour toute racine a de P dans M, il existe un unique morphisme $\phi : K[X]/_{(P)} \longrightarrow M$ tel que :

- *$\phi(x) = a$*
- *$\phi_{|K} = id_K$.*

Proposition 18
Si $P \in K[X]$ et si $d°P = n \geq 1$ alors il existe une extension $L = \mathbb{D}_K(P)$.

Théorème 24
Soient K, K' deux corps.
Soit $\sigma : K \longrightarrow K'$ un isomorphisme de corps.
Soient $P \in K[X]$ et $\tilde{P} = \sigma(P) \in K'[X]$.
Soient $L = \mathbb{D}_K(P)$ et $L' = \mathbb{D}_{K'}\left(\tilde{P}\right)$.
On a : σ se prolonge en un isomorphisme de corps entre L et L' qui envoie les racines de P sur les racines de $\tilde{P}$.

5.2 Clôture algébrique d'un corps.

Définition et proposition 2
Soit K un corps.
Les conditions suivantes sont équivalentes :

1. *Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K.*
2. *Tout polynôme de degré ≥ 1 de $K[X]$ admet au moins une racine dans K.*
3. *Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.*
4. *Toute extension algébrique de K est identique à K lui-même.*
   *On dit alors que **K est algébriquement clos**.*
5. *Tout corps algébriquement clos est infini.*

Corollaire 2

- *Les polynômes irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1.*
- *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 qui n'ont pas de racine réelle.*

Théorème 25 (Steinitz)

1. *Tout corps commutatif K admet une clôture algébrique $\tilde{K}$.*
2. *Si $\tilde{K}_1$ et $\tilde{K}_2$ sont deux clôtures algébriques de K alors il existe un K-isomorphisme de $\tilde{K}_1$ sur $\tilde{K}_2$.*

5.3 Corps finis

5.3.1 Extensions de corps finis

Définition 24 (Extension d'un corps)
Soit K un corps.

1. *On appelle extension de K tout corps $\mathbb{K}$ tel qu'il existe un morphisme de corps J de K dans $\mathbb{K}$. La notation abréviative "$\mathbb{K}/K$", dont nous userons et abuserons dans la suite de ce mémoire, signifie : le corps $\mathbb{K}$ est un extension du corps K.*
2. *On appelle degré de l'extension $\mathbb{K}$ de K (ou $\mathbb{K}/K$) et on note : $[\mathbb{K} : K]$ la dimension de $\mathbb{K}$ comme K-espace vectoriel :*
   $[\mathbb{K} : K] = dim_K \mathbb{K}$.

5.3.2 Structure de $\mathbb{F}_p$ -e.v.

Proposition 19
Tout anneau intègre ayant un nombre fini $n \geq 2$ d'éléments est un corps.

Théorème 26
Soit F un corps fini.
Alors :

- *Sa caractéristique est un nombre premier p.*
- *Son sous-corps premier est isomorphe à $\mathbb{F}_p$.*
- *Il existe $n \in \mathbb{N}^*$ tel que $Card(F) = p^n$.*

Théorème 27 (Frobenius)
Soit K un corps fini et soit $p = carac(K)$.

Alors l'application $\varphi : \begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & x^p \end{array}$ *est un isomorphisme, appelé* ***isomorphisme de Frobenius*** *de K.*

Théorème 28
Soit K un corps fini, soit $p = carac(K)(> 0)$ ayant $q = card\ K$.
Alors :

1. $\exists\ n \in \mathbb{N}^*\ :\ q = p^n$.
2. $(K \setminus \{0\}, \times)$ *est un groupe cyclique d'ordre $q - 1$.*
3. $\forall\ x \in K\ :\ x^q = x$.
4. $K \cong \mathbb{D}_{\mathbb{F}_p}(X^q - X)$.

Remarque 7 (Terminologie)
Pour tout nombre premier p et tout $n \in \mathbb{N}^*$, il y donc existence et unicité, à isomorphisme près, d'un corps à p^n éléments. Ce corps est noté $\mathbb{F}_{p^n}$.

Corollaire 3
Le produit des éléments de $\mathbb{F}_q^*$ est égal à -1.

Théorème 29
Soient $q = p^n$ et $q' = p^m$ où $n, m \geq 1$ et p est premier.
On a : $\mathbb{F}_q \subset \mathbb{F}_{q'} \iff n$ divise m.

5.3.3 Polynômes irréductibles sur $\mathbb{F}_p$ avec p premier

Le théorème suivant justifie l'intérêt de l'étude des polynômes irréductibles de $\mathbb{F}_p$.

Théorème 30
Soient p premier, $n \in \mathbb{N}^*$.
Notons $q = p^n$.
$\mathbb{F}_q = \mathbb{F}_p[X]/(P)$, où P est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Théorème 31
- *Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.*
- *Si P est un polynôme irréductible de degré n sur $\mathbb{F}_p$* ***alors*** *P divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$ et P ne divise pas $X^{p^m} - X$, $\forall m < n$,*
  donc est scindé sur $\mathbb{F}_{p^n}$, donc son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ est aussi son corps de décomposition.

Exemple 6
P irréductible de degré 3 dans $\mathbb{F}_2[X]$.

$$\Updownarrow \text{ par le théorème précédent.}$$

P divise $X^{2^3} - X$ et P ne divise pas $X^{2^m} - X$ où $\underline{m = 1, 2}$.

$$\begin{array}{lcll} X^8 - X & = & X(X^7 - 1) & = & X(X-1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1). \\ X^4 - X & = & X(X^3 - 1) & = & X(X-1)(X^2 + X + 1). \\ X^2 - X & = & X(X-1) & & \text{inutile car } 1 \mid 2 \text{ donc } \mathbb{F}_2 \subset \mathbb{F}_4. \end{array}$$

Or *$X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$ et on cherche un polynôme P irréductible de degré 3 qui divise $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ et qui ne divise pas $X^2 + X + 1$:*

On remarque que $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \ = \ (X^3 + X^2 + 1)(X^3 + X + 1)$.

Donc il existe deux polynômes irréductibles de degré 3 sur $\mathbb{F}_2[X]$.

On peut donc en conclure qu'il existe ***deux modèles pour les corps ayant 8 éléments*** *:*

$$\mathbb{F}_2[X]/_{(X^3+X^2+1)} \quad et \quad \mathbb{F}_2[X]/_{(X^3+X+1)}.$$

Théorème 32 (Critère d'irréductibilité)
Soit $P \in \mathbb{F}_q[X]$, $d^\circ P = n$.

$$\begin{array}{rcl} P \text{ irréductible dans } \mathbb{F}_q[X] & \iff & pgcd(P, X^{q^m} - X) = 1 \ , \ \forall \ 1 \leq m \leq \frac{n}{2}. \\ & \iff & P \text{ n'a pas de racine dans } \mathbb{F}_{q^m} \ , \ \forall \ 1 \leq m \leq \frac{n}{2}. \end{array}$$

Exemple 7
Soit $P(X) = X^5 + X^3 + 1$.

Est-il irréductible sur $\mathbb{Z}[X]$ *?*

Sur $\mathbb{F}_2[X]$ *: P admet-il une racine ou pas dans* $\mathbb{F}_2 \subset \mathbb{F}_4$ *?*

$x \in \mathbb{F}_2 \ : \ P(x) \neq \overline{0}$.
$x \in \mathbb{F}_4 \backslash \mathbb{F}_2 \ : \ x^2 + x + 1 = \overline{0} \quad \Rightarrow x^2 = -x - 1 = x + 1$.

$$\begin{array}{rcl} P(x) & = & x^5 + x^3 + 1 \\ & = & x^5 + x^2 \times x + 1 \\ & = & x^5 + \underbrace{x^2 + x + 1}_{\overline{0}} \\ & = & x^5 \\ & \neq & \overline{0} \end{array}$$

Donc $X^5 + X^3 + 1$ *est irréductible dans* $\mathbb{F}_2[X]$.
Donc $\boxed{X^5 + X^3 + 1 \text{ est irréductible dans } \mathbb{Z}[X].}$

Remarque 8
Un corps K ayant p^m *éléments est isomorphe à* $\mathbb{D}_{\mathbb{F}_p}[X](X^{p^m} - X)$ *et K est isomorphe à* $\mathbb{F}_p[X]/_{(P)}$ *où P est un polynôme irréductible de degré n.*

Théorème 33
$\forall$ *p premier,* $\forall$ $n \geq 1$, *il existe un corps fini à q éléments.*
- *En particulier,* $\mathbb{F}_q = \mathbb{D}_{\mathbb{F}_q}(X^q - X)$ *est un corps à q éléments.*
- *Tout corps K à q éléments est isomorphe à* $\mathbb{F}_q$.

Applications 1 *Corps ayant* 2^3 , 3^2 *éléments.*

1. *Construction d'un corps ayant* 2^3 *éléments :*
   - ***De façon abstraite*** *:* $\mathbb{F}_8 = \mathbb{D}_{\mathbb{F}_2}(X^8 - X)$.

   - ***De façon concrète*** *:* $\mathbb{F}_8 \cong \mathbb{F}_2/_{(P)}$ *où P est un polynôme irréductible de degré 3 sur* $\mathbb{F}_2[X]$.

     P divise $X^{2^3} - X$ *et P ne divise pas* $X^{2^m} - X$ *où* $\underline{m = 1, 2}$.

     Tout d'abord, on peut factoriser $X^8 - X$ *:*
     $X^8 - X = X(X^7 - 1)$.

     Or $X^7 - 1 = \Phi_1(X)\Phi_7(X)$ *où les* Φ_i *sont des polynômes cyclotomiques.*
     - $\Phi_1(X) = X - 1$.
     - $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
       $\Rightarrow \Phi_7(X) = (X^3 + X^2 + 1)(X^3 + X + 1)$ $(mod\ 2)$.

***Finalement**, X^8-X s'écrit sous forme de produits de facteurs irréductibles :*
$X^8 - X = X(X-1)(X^3+X^2+1)(X^3+X+1)$.

Il existe donc deux polynômes irréductibles de degré 3 sur $\mathbb{F}_2[X]$:
$P_1(X) = X^3+X^2+1$ *et* $P_2(X) = X^3+X+1$.

Donc, on a : $\boxed{\mathbb{F}_8 = \mathbb{F}_2[\alpha]}$ *où α est une racine de P_1 ou P_2.*

2. *Construction d'un corps ayant 3^2 éléments :*
   - ***De façon abstraite** : $\mathbb{F}_9 = \mathbb{D}_{\mathbb{F}_3}(X^9 - X)$.*
   - ***De façon concrète** : $\mathbb{F}_9 \cong \mathbb{F}_3/_{(P)}$ où P est un polynôme irréductible de degré 2 sur $\mathbb{F}_3[X]$.*

     P divise $X^{3^2} - X$ et P ne divise pas $X^{3^m} - X$ où $\underline{m=1}$.

     Tout d'abord, on peut factoriser $X^9 - X$:
     $X^9 - X = X(X^8-1)$.

     ***Or** $X^8-1 = \Phi_1(X)\Phi_2(X)\Phi_4(X)\Phi_8(X)$ où les Φ_i sont des polynômes cyclotomiques.*
     - $\Phi_1(X) = X-1$.
     - $X^2-1 = \Phi_1(X)\Phi_2(X) = (X-1)\Phi_2(X)$
       $\Rightarrow \Phi_2(X) = (X+1)\ (mod\ 3)$.
     - $X^4-1 = \Phi_1(X)\Phi_2(X)\Phi_4(X) = (X-1)(X+1)\Phi_4(X)$
       $\Rightarrow \Phi_4(X) = (X^2+1)\ (mod\ 3)$.
     - $X^8-1 = \Phi_1(X)\Phi_2(X)\Phi_4(X)\Phi_8(X) = (X^4-1)\Phi_8(X)$
       $\Rightarrow \Phi_8(X) = (X^4+1)\ (mod\ 3)$.

     $\underline{X^4+1 \text{ est-il irréductible sur } \mathbb{F}_3[X]}$ *?*

$$\begin{aligned} X^4+1 &= (X^2+aX+b)(X^2+cX+d). \\ &= X^4+cX^3+dX^2+aX^3+acX^2+adX+bX^2+bcX+bd. \\ &= X^4+(c+a)X^3+(d+ac+b)X^2+(ad+bc)X+bd. \end{aligned}$$

Donc on obtient le système suivant :

$$\begin{cases} a+c & = & 0 \\ ac+b+d & = & 0 \\ ad+bc & = & 0 \\ bd & = & 1 \end{cases}$$

Si $bd = 1$ *alors on a deux couples solutions pour le couple* (b,d) *:*

$$(b,d) \;=\; (1,1) \text{ ou } (2,2)$$

Donc $\boxed{b = d = 1 \text{ ou } 2.}$

Donc le système devient :

$$\begin{cases} c & = & 2a & = & 2 \text{ ou } 1 \\ 2b+2a^2 & = & 0 & & \\ b & = & d & = & 1 \end{cases}$$

A partir de la deuxième équation, on obtient :

$$b = -a^2 = 2a^2$$

$$\Rightarrow \begin{cases} 2a^2 & = & 1 \\ 2a^2 & = & 2 \end{cases}$$

$$\Rightarrow \begin{cases} a^2 & = & \frac{1}{2} \text{ impossible} \\ a^2 & = & 1 \end{cases}$$

Donc $a = 1 \text{ ou } -1 \Longrightarrow \boxed{a = 1 \text{ ou } 2}$.

∗ *Si* $\boldsymbol{a = 1}$ *alors*

$$\begin{cases} b & = & d & = & 2 \\ c & = & 2 & & \end{cases}$$

Donc $\boxed{\boldsymbol{X^4 + 1 = (X^2 + X + 2)(X^2 + 2X + 2) \pmod 3.}}$

∗ *Si* $\boldsymbol{a = 2}$ *alors*

$$\begin{cases} b & = & d & = & 2 \\ c & = & 1 & & \end{cases}$$

Donc $\boxed{\boldsymbol{X^4 + 1 = (X^2 + 2X + 2)(X^2 + X + 2) \pmod 3.}}$

Finalement, on obtient :
$X^9 - X = X(X-1)(X+1)(X^2+1)(X^2+2X+2)(X^2+X+2) \pmod 3$.

On remarque, de plus, que :

$$\begin{aligned} (X+2)^2 + X + 2 + 2 &= X^2 + 4X + 4 + X + 4 \\ &= X^2 + 2X + 2 \end{aligned}$$

Donc $\mathbb{F}_9 \cong \mathbb{F}_3[X]/_{(X^2+X+2)}$.

Soit α *une racine de* X^2+X+2 *polynôme irréductible de degré 2 sur* $\mathbb{F}_3[X]$ *:* $\alpha^2 + \alpha + 2 = 0$.

Donc $\mathbb{F}_9 = \mathbb{F}_3[\alpha] = \{a\alpha + b \ / \ a, b \in \mathbb{F}_3\}$.

Donc $\boxed{\mathbb{F}_9 = \{\bar{0} \ ; \ \bar{1} \ ; \ \bar{2} \ ; \ \alpha \ ; \ \alpha + \bar{1} \ ; \ \alpha + \bar{2} \ ; \ 2\alpha \ ; \ 2\alpha + \bar{1} \ ; \ 2\alpha + \bar{2}\}.}$

5.4 Preuve du Théorème de Wedderburn

Pour pouvoir démontré le théorème de Wedderburn, nous avons besoin d'énoncer et de prouver le lemme suivant :

Lemme 8
Soit $n > 1$.
Pour tout diviseur d *de* n *distinct de* n, *le polynôme* $\Phi_n(X)$ *divise le polynôme* $\frac{X^n-1}{X^d-1}$ *dans* $\mathbb{Z}[X]$.

Preuve 8 *Ceci découle de suite des formules :*

$$X^n - 1 = \prod_{\delta|n} \Phi_\delta(X) \quad et \quad X^d - 1 = \prod_{\delta|d} \Phi_\delta(X)$$

et du fait que : $\forall m \in \mathbb{N}^* \ , \ \Phi_m(X) \in \mathbb{Z}[X]$.

Preuve 9 (du théorème de Wedderburn)
Soit F *un corps fini, supposé non commutatif.*
Le centre $Z = \{x \in F \ / \ \forall \ y \in F \ , \ xy = yx\}$ *de* F *est un sous-corps commutatif de* F.*Notons* $q = Card(Z)$.
Soit p *la caractéristique de* Z.
Alors Z *est un* $\mathbb{F}_p$*-espace vectoriel de dimension finie.*

Notons $f = [Z : \mathbb{F}_p]$ *alors* $Card(Z) = p^f$.
F *est un* Z*-espace vectoriel de dimension finie.*

Notons $n = [F : Z]$ *alors* $Card(F) = q^n$.
Pour $x \in F^* = F \backslash \{0\}$, *considérons* $C(x) = \{y \in F \ / \ xy = yx\}$ *où* $C(x)$ *est un sous-corps de* F *contenant* Z.
Donc $C(x)$ *est un* ***Z-espace vectoriel de dimension finie****.*

Notons $\delta(x) = [C(x) : Z]$ *alors* $Card(C(x)) = q^{\delta(x)}$.

On applique ***l'équation des classes*** *au groupe multiplicatif F^* de cardinal $q^n - 1$ dont le centre n'est autre que $Z^* = Z \setminus \{0\}$ de cardinal $q - 1$.*

En remarquant que pour $x \in F^*$, $S_x = \{y \in F^* \ / \ xy = yx\}$ est le groupe multiplicatif $C(x)^*$ du corps $C(x)$.
Donc $Card(S_x) = q^{\delta(x)} - 1$.
Donc $q^{\delta(x)} - 1$ divise $q^n - 1$.
Donc $\boxed{\delta(x) \text{ divise } n}$ et $\delta(x) = n$ équivaut à $x \in Z$.

On obtient donc :

$$q^n - 1 = q - 1 + \sum_{x \in \ \mathcal{R}} \frac{q^n - 1}{q^{\delta(x)-1}} \qquad (*)$$

où x parcourt un ensemble $\mathcal{R}$ formé d'un représentant de chacune des classes non réduites à un singleton.

$$\begin{array}{lrcl} \underline{\text{On a}} \ : & \mathcal{R} = \oslash & \Longleftrightarrow & F = Z \\ & & \Longleftrightarrow & [F : Z] = 1 \\ & & \Longleftrightarrow & n = 1 \end{array}$$

$\underline{\text{Supposons } n > 1}$.

$\Phi_n(q)$ divise $q^n - 1$ et, d'après le lemme précédent, $\Phi_n(q)$ divise chacun des termes de la somme de l'égalité (*).
Donc $\Phi_n(q)$ divise $q - 1$.
D'où $\mid \Phi_n(q) \mid \leq q - 1$.

Mais $\Phi_n(q) = \prod_{\xi \in \mathcal{P}_n(\mathbb{C})} q - \xi$ où $\mathcal{P}_n(\mathbb{C})$ est l'ensemble des racines primitives n-ièmes de l'unité donc une partie du cercle unité $\mathbb{U}$ et Φ_n est le n-ième polynôme cyclotomique.

Pour chaque $\xi \in \mathcal{P}_n(\mathbb{C})$, $\mid q - \xi \mid \geq \ q- \mid \xi \mid = q - 1$, avec égalité si et seulement si $\boxed{\xi = 1}$.
Or, $n > 1$ donc un au moins des ξ de $\mathcal{P}_n(\mathbb{C})$ est différent de 1.
Donc un au moins des facteurs $\mid q - \xi \mid$ est supérieur strictement à $q - 1$.

$$\begin{array}{lrcl} & \mid \Phi_n(q) & = & \prod_{\xi \in \mathcal{P}_n(\mathbb{C})} \mid q - \xi \mid \\ D'où & & > & \prod_{\xi \in \mathcal{P}_n(\mathbb{C})} (q - 1) \\ & & = & (q-1)^{\varphi(n)} \\ & & \geq & q - 1 \end{array}$$

$\Longrightarrow$ *CONTRADICTION avec le fait que $\mid \Phi_n(q) \mid \leq q - 1$.*

Ainsi $\boxed{n = 1}$ et $F = Z$: $\boxed{\boldsymbol{F \text{ est commutatif}}}$.

Chapitre 6

Tests de primalité et de composition.

A quoi reconnaît-on qu'un nombre est premier ? Que peut-on dire de la décomposition d'un entier en facteurs premiers ? Ces questions nous viennent de l'Antiquité.
Euclide, déjà, prouvait qu'il existe une infinité de nombres premiers : son célèbre argument étant que si $p_1, p_2, \cdots, p_n$ est un ensemble fini de nombres premiers alors $1 + p_1 p_2 \cdots p_n$ n'est divisible par aucun des p_i. Depuis, la fascination pour l'étude de la nature de la décomposition en facteurs premiers n'a cessé d'augmenter. Cependant, l'approche algorithmique de la question, **c'est-à-dire** comment fait-on concrètement pour décider qu'un entier est premier et comment le factorise-t-on s'il ne l'est pas, est une préoccupation plus récente.

Soit n un entier positif. On a deux problèmes :

1. déterminer si n est premier.
2. si n est composé, le factoriser.

Nous allons étudier ces deux problèmes et remarquer qu'il existe de nombreux tests qui permettent de les résoudre :

- les **tests déterministes** qui donnent une réponse exacte -oui ou non- à la question "est-ce que ce nombre est premier ?"
- les **tests commerciaux ou probabilisites** qui donnent la même réponse avec une certaine probabilité.

6.1 Nombres premiers et congruences

6.1.1 Tests de divisibilité

On connaît depuis l'école primaire le test de divisibilité par 3 : si $m_r m_{r-1} \dots m_0$ est l'écriture en base 10 du nombre n, alors n est divisible par 3 si et seulement si la somme $m_r + m_{r-1} + \dots + m_0$ est divisible par 3.
Ce résultat découle de la théorie des congruences :
en effet, comme $n = m_r 10^r + m_{r-1} 10^{r-1} + \dots + m_0 10^0$ et $10 \equiv 1 (mod\ 3)$,
on a $n \equiv m_r + m_{r-1} + \dots + m_0 (mod\ 3)$.
Tous les tests de divisibilité se démontrent de la même façon.

6.1.2 Nombres pseudopremiers

Nous rappelons l'énoncé du Petit Théorème de Fermat parce qu'il est très important de le connaître pour les tests qui vont suivre :

Théorème 34 (Le petit théorème de Fermat)
Si p est un nombre premier alors, pour tout entier a, ***on a*** *: $a^p \equiv a(mod\ p)$.*

Remarque 9 *La réciproque de ce théorème n'est pas exacte en général. Elle l'est cependant dans un grand nombre des cas comme nous allons le voir.*
Le premier contre-exemple est dû au mathématicien français Pierre Frédéric Sarrus qui, en 1819, a remarqué que $2^{341} - 2$ est divisible par 341, bien que 341 ne soit pas premier : il se décompose en produit de nombres premiers : 11×31.

Définition 25 (Nombre pseudopremier)
Un nombre a est ***pseudopremier*** *en base b s'il est composé, c'est-à-dire qu'il s'écrit comme produit de nombres premiers, et s'il satisfait $b^a \equiv b(mod\ a)$.*

Théorème 35
$\forall \in \mathbb{N}^*$, il existe une infinité de nombres pseudopremiers en base b.

Remarques 3 *Le nombre* ***341 est pseudopremier en base 2 mais pas en base 3****. On pense que c'est la rareté des nombres pseudopremiers en base 2 et en base 3 qui a fait croire longtemps à la validité de la réciproque du théorème de Fermat.*
Il y a cependant des nombres pseudopremiers en toute base, par exemple le nombre ***561****, découvert par R.D. Carmichael en 1909. Cette découverte nous permet de définir les nombres de Carmichael :*

Définition 26 (Nombres de Carmichael)
Un nombre composé a est un ***nombre de Carmichael*** *s'il est pseudopremier en toute base.*

Remarques 4 *Les nombres pseudopremiers sont rares comparativement aux nombres premiers.*

- *Il y a exactement 882 206 716 nombres premiers inférieurs à 20 milliards.*
- *Il n'y a que 49 865 nombres pseudopremiers en base 2.*

6.1.3 Nombres de Mersenne

Mersenne (1588-1648) fut un moine minime, enseignant la philosophie à Nevers avant de s'établir à Paris.D'un esprit curieux, il s'est intéressé à la mécanique et aux mathématiques, plus précisément à la primalité des nombres de la forme $\mathbf{2^n - 1}$. Ces nombres étaient connus depuis Euclide, en liaison avec les nombres parfaits et euclidiens, mais depuis le $17^{ième}$ siècle, en hommage à Mersenne, ils sont notés M_n et appelés **nombres de Mersenne**.

Remarques 5 ***Si M_n est premier alors n est premier.***

En effet : si n, n_1, n_2 sont des entiers positifs alors, dans $\mathbb{Z}[X]$, on a $X-1 \mid X^n-1$ et $X^{n_1}-1 \mid X^{n_1 n_2}-1$. On en déduit pour a entier positif :

- *Si $a > 2$, $a^n - 1$ n'est pas premier.*
- *Si $a = 2$ et si $n = n_1 n_2$ alors $2^{n_1} - 1 \mid 2^{n_1 n_2} - 1$.*

Il en résulte que si $a^n - 1$ est premier alors $a = 2$ et n est premier.

Exemples 4 *Voici la liste des plus grands nombres premiers de Mersenne :*

Rang	***Mersenne***	***Premier***	$\mathbf{10^n}$ ***avec n=***	***Date de découverte***
1	*42*	$2^{25964951}-1$	*7 816 230*	*2005*
2	*41*	$2^{24036583}-1$	*7 235 733*	*2004*
3	*40*	$2^{20996011}-1$	*6 320 430*	*2003*
4	*39*	$2^{13466917}-1$	*4 053 946*	*2001*
5	*38*	$2^{6972593}-1$	*2 098 960*	*1999*
6	*37*	$2^{3021377}-1$	*909 526*	*1998*
7	*36*	$2^{2976221}-1$	*895 932*	*1997*
8	*35*	$2^{1398269}-1$	*420 921*	*1996*
9	*34*	$2^{1257787}-1$	*378 632*	*1996*
10	*33*	$2^{859433}-1$	*258 716*	*1994*
11	*32*	$2^{756839}-1$	*227 832*	*1992*
12	*31*	$2^{216091}-1$	*65 050*	*1985*
13	*30*	$2^{132049}-1$	*39 751*	*1983*
14	*29*	$2^{110503}-1$	*33 265*	*1988*
15	*28*	$2^{86243}-1$	*25 962*	*1982*
16	*27*	$2^{44497}-1$	*13 395*	*1979*
17	*26*	$2^{23209}-1$	*6 987*	*1979*
18	*25*	$2^{21701}-1$	*6 533*	*1978*
19	*24*	$2^{19937}-1$	*6 002*	*1971*
20	*23*	$2^{11213}-1$	*3 376*	*1963*
21	*22*	$2^{9941}-1$	*2 993*	*1963*
22	*21*	$2^{9689}-1$	*2 917*	*1963*
23	*20*	$2^{4423}-1$	*1 332*	*1961*
24	*19*	$2^{4253}-1$	*1 281*	*1961*

Remarque 10 *Les plus grands nombres premiers connus sont des* ***nombres de Mersenne****.*

6.1.4 Nombres de Fermat

Un nombre premier de Fermat est un nombre premier de la forme $2^{2^n}+1$ pour $n \geq 0$.
En 1637, Fermat a affirmé que les nombres $F_n = 2^{2^n}+1$, pour $n \geq 0$, sont premiers. Cet énoncé est vrai jusqu'à n=5. En fait :

$$\boldsymbol{F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537} \text{ sont premiers.}$$

Mais, Euler a démontré que $\boldsymbol{F_5}$ **est composé** : $F_5 = 641 \times 6700417$.
On sait maintenant que les F_n, pour $5 \leq n \leq 30$ sont composés. D'autre part, il n'est pas difficile de prouver que si un nombre p est premier et si p-1 est une puissance de 2 alors il existe un entier n tel que $p = 2^{2^n}+1$ c'est-à-dire que **p est un nombre premier de Fermat**.

6.2 Tests déterministes

6.2.1 Le $(n-1)$-test.

Le $(n-1)$-test est un test de primalité des nombres n tels que l'on connaît la factorisation primaire de $n-1$.C'est le cas des nombres de Fermat $F_k = 2^{2^k}+1$.
L'énoncé suivant est essentiellement dû à Lucas (1876) mais Lehmer en a simplifié les hypothèses.

Théorème 36 (Test de primalité de Lucas-Lehmer)
Soit n un entier > 1.
S'il existe un entier a tel que, pour tout facteur premier p de $n-1$,

$$a > 1\ ,\ a^{n-1} \equiv 1\ (mod\ n)\ et\ a^{(n-1)/p} \neq 1 (mod\ n), \qquad (A.1)$$

alors n est premier.

Pour les nombres de Fermat $F_n = 2^{2^n}+1$, on a un test dû à Pépin en 1877.

Théorème 37 (Pépin)
Pour $n \geq 1$, *on a :* F_n *est premier* $\Leftrightarrow\ 3^{(F_n-1)/2} \equiv -1\ (mod\ F_n)$.

6.2.2 Le $(n+1)$-test.

Théorème 38 (Théorème de Lucas-Lehmer sur les nombres de Mersenne)
Soient
- *s un nombre premier impair,*
- *$n = 2^s - 1$,*
- *a un entier tel que n soit premier avec $a^2 - 4$.*

On définit par récurrence une suite d'entiers, (L_i) où $i \geq 1$, dite suite majeure de Lucas, comme suit :
$L_1 = a$, $L_{i+1} = L_i^2 - 2$.
Alors on a : $L_{s-1} \equiv 0 (mod\ n) \iff n$ est premier.

Les suites de Lucas

Définition 27
Soit A un anneau et a un élément de A.
*La **suite de Lucas** de l'anneau A, associée à a, est la suite $(V_n)_{n\geq 0}$, définie par :*
- *Conditions initiales : $V_0 = 2.1_A$, $V_1 = a$.*
- *Formule de récurrence : $V_{n+1} = aV_n - V_{n-1}$, pour $n \geq 2$.*

Lemme 9
Soit A un anneau et a un élément de A.
on considère la suite de Lucas (V_n) associée à a.

1. *S'il existe un élément inversible x de A tel que $x + x^{-1} = a$, alors $V_n = x^n + x^{-n}$ pour tout $n \geq 0$.*
2. *Réciproquement, si (V_n) est la suite de Lucas associée à a, il existe une extension d'anneaux $A \hookrightarrow B$ telle que l'anneau B contienne un élément inversible x vérifiant $x + x^{-1} = a$.*

Remarque 11 *On est donc habilité, pour étudier les propriétés d'une suite (V_n) de Lucas, à supposer l'existence d'un élément inversible x tel que la relation $V_n = x^n + x^{-n}$ soit vérifiée pour tout n. On obtient ainsi les relations suivantes :*

$$\begin{aligned} V_n V_m &= V_{n+m} + V_{n-m} \\ V_{2n-1} &= V_n V_{n-1} - a \\ V_{2n} &= V_n^2 - 2 \\ V_{2n+1} &= aV_n^2 - V_n V_{n-1} - a \\ V_n = 2 &\iff x^n = 1 \end{aligned}$$

Théorème 39 (Critère de primalité de Lucas-Lehmer)
Soient :

- *n un entier impair > 1 tel qu'on connaisse la décomposition de $n+1$ en facteurs premiers,*
- *a un entier tel que $pgcd(n, a^2 - 4) = 1$,*
- *V_n la suite de Lucas définie par :*

$$V_0 = 2\ ,\ V_1 = a \text{ et la formule de récurrence } :\ V_{n+1} = aV_n - V_{n-1}. \qquad (A.2)$$

Si $V_{n+1} \equiv 2(mod\ n)$ et $pgcd(V_{(n+1)/q} - 2, n) = 1$ pour tout facteur premier q de $n+1$, alors n est premier.

Théorème 40
Soit s un entier impair > 1, $n = M_s = 2^s - 1$, le nombre de Mersenne et (L_n) la suite majeure de Lucas. Alors on a :

$$n \text{ est premier} \iff L_{s-1} \equiv 0(mod\ n).$$

6.3 Tests probabilistes

6.3.1 Test de Solovay-Strassen

Le symbole de Jacobi

Définition 28
Pour m impair $\in \mathbb{N}$ et $n \in \mathbb{Z}$; le symbole de Jacobi $\left(\frac{n}{m}\right)$ est défini comme suit :

1. *Si $PGCD(n, m) > 1$, $\left(\frac{n}{m}\right) = 0$.*
2. *Si $m = 1$, $\left(\frac{n}{m}\right) = 1$.*
3. *Si $m = \prod_{i=1}^{n} (p.i)^{\alpha_i}$ et $PGCD(n, m) = 1$, $\left(\frac{n}{m}\right) = \prod_{i=1}^{n} \left(\frac{n}{p.i}\right)^{\alpha_i}$.*

Propriétés 1
Si m et n sont deux nombres impairs positifs :

1. $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$ *si* $a \equiv b\ mod\ m$.
2. $\left(\frac{a}{m}\right) . \left(\frac{b}{m}\right) = \left(\frac{ab}{m}\right)$.
3. $\left(\frac{a}{m}\right) . \left(\frac{a}{n}\right) = \left(\frac{a}{mn}\right)$.
4. $\left(\frac{a^2}{m}\right) = 1$ *si* $PGCD(a, m) = 1$.
5. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.
6. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.
7. $\left(\frac{m}{n}\right) . \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \times \frac{n-1}{2}}$ *si* $PGCD(n, m) = 1$.

Principe du test de Solovay-Strassen

On aurait pu souhaiter que, pour tout n composé, il existe une proportion indépendante de n du choix de "l'aléa" a donnant une réponse négative au test de Fermat. Ce n'est pas le cas, cependant, comme le montre l'existence des nombres de Carmichael.
Le test suivant est plus efficace car il n'a pas cet inconvénient. Il s'agit, plutôt que d'appliquer une "réciproque" du théorème de Fermat, de faire appel au théorème d'Euler. Ainsi, on obtient le **Test de Solovay-Strassen** :

1. Choisir a au hasard tel que $1 \leq a \leq n-1$.
2. Calculer $a^{(n-1)/2}(mod\ n)$.
3. Calculer le symbole de Jacobi $(\frac{a}{n})$.
4. L'entier n satisfait au test si $a^{(n-1)/2}(mod\ n) \equiv (\frac{a}{n})(mod\ n)$ c'est-à-dire l'entier n est premier et dans le cas contraire, l'entier n est composé.

Corollaire 4
Si n n'est pas premier et si a est choisi aléatoirement dans $(\mathbb{Z}/n\mathbb{Z})^*$*, alors la probabilité que n satisfasse le test de Solovay-Strassen est inférieure à* $\frac{1}{2}$.

On a donc une probabilité $\geq 1 - \frac{1}{2^r}$ de déceler en r applications du test la non-primalité d'un quelconque entier n.

6.3.2 Test de Miller-Rabin

Le Test de Miller-Rabin est un raffinement du test de Solovay-Strassen qui permet de déterminer si ce nombre n est composé ou premier avec une probabilité x et qui se fonde sur la remarque suivante :

Soit n un entier impair donné.
Si $a^{(n-1)/2} \equiv 1(mod\ n)$ et si $\frac{n-1}{2}$ est encore pair, alors $a^{(n-1)/4}$ est une racine de $1(mod\ n)$ et vaut donc 1 ou -1 dans le cas où n est premier.

Plus généralement, si on examine les racines successives de $1(mod\ n)$: $a^{(n-1)/2}, a^{(n-1)/4}$, $a^{(n-1)/8}, \ldots, a^{(n-1)/2^s}$ tant que c'est possible, c'est-à-dire jusqu'au premier s tel que $(n-1)/2^s$ est impair, alors, si n est premier, la première racine différente de 1 que l'on obtient doit être -1.

Cette constatation mène au test suivant :

1. On écrit n-1 sous la forme n-1=$2^s t$, où t est impair.
2. On tire un entier aléatoire a, 1≤a≤n-1.
3. b← a^t (mod n)
4. **SI** $b \equiv 1(mod\ n)$, alors n est premier. **FIN** $(A.3)$
5. **POUR** i=0 jusqu'à s-1 **FAIRE**

   SI b≡ -1 (mod n), alors n est premier. **FIN**
   SINON b← b^2 (mod n).
   FIN POUR
6. n est composé. **FIN**

Définition 29
On dit que ***n passe le test de primalité de Miller-Rabin en base b*** *si les deux résultats suivants sont vérifiés :*
- $b^{n-1} \equiv 1\ (mod\ n)$.
- *Si le premier élément de (S) n'est pas égal à 1, et* $b^{2^r t}$ *(mod n) est le premier élément égal à 1, alors l'élément précédent* $b^{2^{r-1}t}$ *(mod n) est n-1.*

Définition 30
Un entier n est ***pseudopremier fort*** *en base b, si n est composé impair et s'il passe le test de Miller-Rabin en base b.*

Définition 31
Soit n un entier composé impair et b dans l'intervalle $[1, n-1]$.
Si n ne passe pas le test de Miller-Rabin en base b, alors on dit que b est un ***temoin de n****, c'est-à-dire témoin que n est composé.*
On notera t(n) le nombre de témoins de n et $b(n) = n-1-t(n)$ *le nombre des bases pour lesquelles le nombre n passe le test.*

Exemples 5

1. *Le nombre 9 à 6 témoins.*
2. *Considérons le nombre* $n = 341$ *et la base* $b = 2$.
   On a $340 = 2^2 \times 85$.
   Exécutons le test de Miller-Rabin. Nous obtenons la suite (S) suivante :

   $$2^{85} \equiv 32,\ 2^{170} \equiv 1,\ 2^{340} \equiv 1\ (mod\ 341).$$

   On voit que le nombre 1 admet le nombre 32 comme racine carrée qui est égal à 2^{85} $(mod\ 341)$. *Or,* $32 \neq \pm 1\ (mod\ 341)$.
   Donc 341 est composé : $341 = 11 \times 31$ *et le nombre 2 est un témoin de 341.*

3. *Prenons* $n = 91$ *avec la base* $b = 10$*, alors* $90 = 2 \times 45$ *et*

$$10^{45} \equiv -1,\ 10^{90} \equiv 1\ (mod\ 91).$$

Le nombre 91 passe le test, pourtant il est composé : $91 = 7 \times 13$*. Il est donc* ***pseudopremier fort en base 10****.*

Remarques 6

1. *Si n est premier alors n passe le test de Miller-Rabin. C'est essentiellement grâce au théorème de Fermat dans le corps* $\mathbb{F}_n$*.*
2. *Si le premier résultat n'est pas vérifié alors le théorème de Fermat n'est pas vrai dans* $(\mathbb{Z}/n\mathbb{Z})^*$ *donc n n'est pas premier.*
3. *Si le second résultat n'est pas vérifié, c'est qu'il existe dans l'anneau* $(\mathbb{Z}/n\mathbb{Z})$ *un élément u tel que* $u \neq \pm 1$ *et* $u^2 = 1$*, ce qui n'est pas possible dans un corps, donc n n'est pas premier.*
4. *Si n passe le test en une base b, alors l'entier n est premier avec une probabilité supérieure à* $\frac{3}{4}$*.*
5. *Si n passe les tests en k différentes base b, choisis au hasard, alors n est premier avec une probabilité supérieure à* $1 - (\frac{1}{4})^k$*.*

Les deux derniers résultats découlent d'un théorème démontré en 1976 par Rabin et dont une forme équivalente est la suivante :

Théorème 41 (Rabin)
Pour chaque nombre impair composé $n > 9$*, le nombre de témoins de n vérifie* $\frac{t(n)}{n-1} \geq \frac{3}{4}$*.*

Remarque 12 *Ce théorème implique que si n est un nombre composé impair* > 9*, alors au moins* $\frac{3}{4}$ *des entiers de* $[2, n-1]$*, sont des témoins de n. La probabilité que l'on échoue à trouver un témoin de n est donc* $< \frac{1}{4}$*. On peut itérer l'algorithme. Au bout de k itérations indépendantes, la probabilité de ne pas trouver de témoin est donc* $< \frac{1}{4^k}$*, ce qui est très faible si* $k \geq 10$*.*
Cet algorithme est assez rapide. Le calcul d'une puissance b^m *(mod n) utilisant approximativement* $\frac{3}{2}.\ln_2(m)$ *multiplications où* $\ln_2$ *est le logarithme en base 2, on démontre que si* $n - 1 = 2^s t$*, avec t impair, alors l'algorithme nécessite un temps inférieur à* $k(2\ln_2(n) + t\ln_2(n))$*, k étant le nombre d'itérations.*

Théorème 42 (Test de composition)
Si *n ne passe pas le test de Miller pour une certaine valeur a,* ***alors*** *n est composé.*

Le test de Miller-Rabin est véritablement une amélioration du test de Solovay-Strassen. Le calcul du symbole de Jacobi dans le second test n'apporte aucune information supplémentaire. En effet :

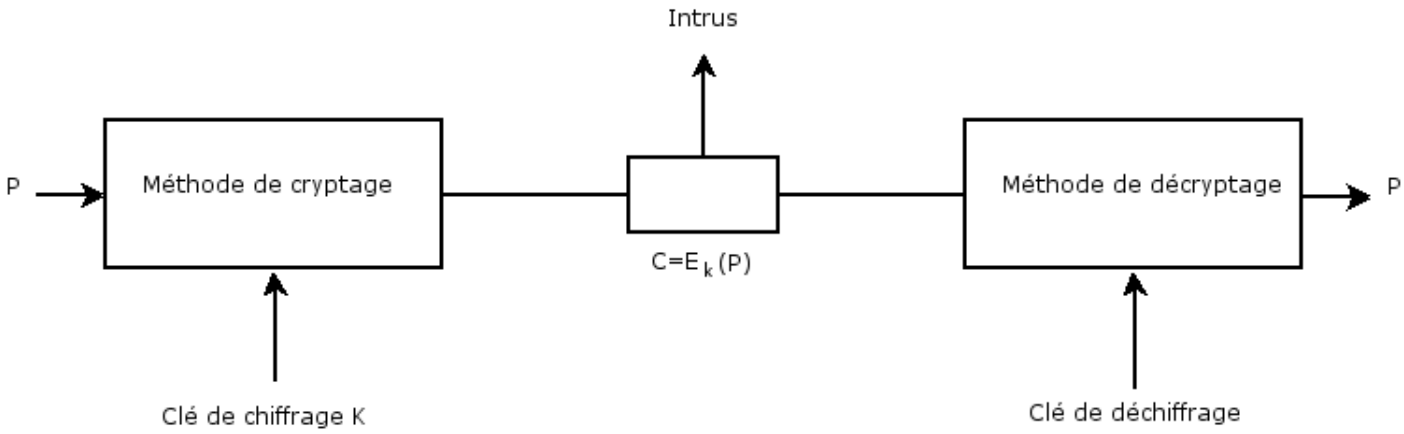
Proposition 20
Si n satisfait au test de Miller-Rabin pour un entier a modulo n, alors il satisfait aussi au test de Solovay-Strassen pour le même a.

Proposition 21
Si n n'est pas premier et si a est choisi aléatoirement dans $(\mathbb{Z}/n\mathbb{Z})^*$*, alors la probabilité que n satisfasse le test de Miller-Rabin est inférieure à* $\frac{1}{4}$.

Chapitre 7

Fondements de la Cryptographie.

Le principe de la cryptographie est représenté par la figure suivante :



Modèle de cryptage

Lors de l'opération de chiffrage (ou cryptage), le *texte clair* P est transformé par une fonction E paramétrisée par une clé K pour ainsi obtenir un cryptogramme $C = E_K(P)$. Ce cryptogramme est alors transmis au receveur qui applique l'algorithme de déchiffrage (ou décryptage) D, inverse de celui de cryptage : $P = D(C) = D(E_K(P))$. On suppose que "l'intrus" écoute et peut reproduire fidèlement le cryptogramme complet. Il ne connaît cependant pas la clé de chiffrage et ne peut retrouver aisément le message en clair bien que l'on suppose qu'il connaisse l'algorithme utilisé. Cette hypothèse est connue sous le nom d "hypothèses de Kerckhoffs". Parfois, l'intrus ne se contente pas d'écouter le canal de communication - intrus passif - , mais il peut altérer les messages ou injecter ses propres messages dans le canal de communication - intrus actif-. L'art de composer des cryptogrammes est la *cryptographie* et l'art de les briser est la *cryptanalyse*.

7.1 Cryptographie à clé secrète

Depuis l'invention du *one-time pad*, la cryptographie s'est développée autour de l'élaboration de schémas dans lesquels un clé, relativement courte, peut être utilisée

pour chiffrer de longs messages tout en assurant un niveau raisonnable de sécurité. Nous présentons dans cette section les deux grandes familles de systèmes modernes à clé secrète : les chiffrements à flots, en particulier ceux basés sur des registres à décalage, et les chiffrements par blocs.

7.1.1 Schémas de chiffrement à flot

Un schéma de chiffrement à flot chiffre le message bit à bit, par une transformation qui varie au cours du temps. De tels schémas sont simples à implémenter et en général, plus rapides que les chiffrements par blocs. De plus, lorsque la taille mémoire est limitée ou lorsque les bits du message doivent être chiffrés dès réception, leur utilisation s'impose. En outre, ils sont adaptés à des contextes dans lesquels les erreurs de transmission sont fréquentes.
Dans tout schéma de chiffrement à flot, un **flot de clé** est généré et combiné avec le message. Ces deux opérations ne sont pas forcément indépendantes : lorsqu'elles le sont, on dit que ce schéma est **synchrone** et dans le cas contraire, on dit qu'il est **asynchrone**.
Ces appellations viennent du fait que, dans les schémas synchrones, le déchiffrement correct nécessite que les dispositifs à chaque extrémité de la communication soient dans le même état ; dans les schémas asynchrones, le déchiffrement correct peut-être automatiquement rétabli après seulement un nombre fixé de bits du clair perdus.
Les principaux chiffrements à flots asynchrones sont construits à partir de chiffrements par blocs, dans un mode de rétroaction à un bit.

Nous allons étudier plus précisément les méthodes de génération d'un flot de clé à partir de registres à décalage. Leur utilisation dans un schéma de chiffrement à flot synchrone étant en général réalisée en combinant de manière simple chaque bit de la sortie du générateur de clé avec chaque bit du clair.

Les registres à décalage

Définition 32
Un registre à décalage de longueur L est constitué de L cases mémoire numérotées de 0 à $L-1$, chacune pouvant contenir un bit, et ayant une entrée et une sortie, et d'une horloge contrôlant le mouvement des données. A chaque coup d'horloge,

- *un bit de rétroaction s est calculé par combinaison des bits des cases de 0 à $L-1$,*
- *le contenu de la case 0 sort du registre pour former la séquence de sortie,*
- *le contenu de la case i passe dans la case $(i-1)$, $1 \leq i \leq L-1$,*
- *la case $L-1$ est remplie avec le bit s.*

Lorsque la combinaison est un simple "xor" de certaines des cases du registre, on parle de rétroaction linéaire.

Pour fonctionner, un registre doit être au préalable être rempli avec une séquence de L bits $[s_{L-1}, \ldots, s_0]$, appelée **état initial** du registre. Il est à noter que les L premiers bits de la séquence produite par le registre sont $s_0, \ldots, s_{L-1}$.
Les registres à décalage à rétroaction linéaire (LFSR) sont les registres les plus utilisés pour la génération d'un flot de clé. Par leur simplicité d'implémentation et

par le bon choix des paramètres, ils produisent des séquences ayant des propriétés intéressantes comme nous le verrons par la suite.
Nous étudions maintenant la classe de registres LFSR :

Un LFSR est complètement caractérisé par sa longueur L et son **polynôme de rétroaction**

$$C(x) = 1 + c_1 x + \ldots + c_L x^L \quad , \quad c_i \in \mathbb{F}_2 \ , \ 1 \leq i \leq L,$$

tel que le bit s soit une combinaison linéaire des cases i , $1 \leq i \leq L-1$, pour i vérifiant $c_{L-i} = 1$. Autrement dit, si on note $[s_{L-1}, \ldots, s_0]$ l'état initial du registre, et s_j , $j \geq L$, le bit de réttroaction à un instant donné, on a alors :

$$s_j = \sum_{i=1}^{L} c_i s_{j-1} mod\ 2.$$

La séquence produite, résultat d'un algorithme déterministe effectué par un dispositif ayant un nombre fini d'états, est ultimement périodique c'est-à-dire il existe n_0 tel que la séquence $\{s_j\}_{j \geq n_0}$ est périodique. Si $C(x)$ est de degré L ($c_L = 1$) alors on peut montrer que la séquence est périodique : $n_0 = 0$.
Dans la suite, nous supposerons que $c_L = 1$.
Etant donné qu'un LFSR de longueur L peut se trouver dans 2^L états différents et que l'état initial $s_i = 0,\ 0 \leq i \leq\leq L-1$ donne la séquence nulle, la période de la séquence générée est au plus $2^L - 1$.
Suivant la nature de $C(x)$, il est possible de générer des séquences de période maximale. Nous allons alors définir la notion de **polynôme primitif** :

Définition 33
Un polynôme $f(x)$ de degré m dans $\mathbb{F}_q[x]$ est dit primitif s'il est irréductible dans $\mathbb{F}_q[x]$ et si le plus petit entier n vérifiant $f(x) \mid x^n - 1$ est égal à $q^m - 1$.

On a alors les propriétés suivantes :

Proposition 22
Soit $C(x) \in \mathbb{F}_2[x]$ le polynôme de rétroaction d'un LFSR de longueur L.
- *Si $C(x)$ est irréductible dans $\mathbb{F}_2[x]$, chacun des $2^L - 1$ états initiaux non nuls de LFSR produit une séquence de sortie dont la période est égale au plus petit entier n tel que $C(x) \mid x^n - 1$.*
- *Si $C(x)$ est primitif alors chacun des $2^L - 1$ états initiaux non nuls de LFSR produit une séquence de sortie de période maximale $2^L - 1$.*

Dans le cas où $C(x)$ est primitif, le LFSR associé est dit **de longueur maximale** et la séquence générée à partir d'un état initial non nul est appelée **m-séquence**.

Générateurs de flots de clés basés sur des LFSR

Bien que les propriétés de la séquence produite dans le cas où le polynôme de rétroaction est primitif soient intéressantes, un LFSR ne peut être utilisé directement pour produire un flot de clé : ces propriétés sont seulement nécessaires. En effet, ce type de générateur est prédictible dans le sens où si on en connaît une sous-séquence suffisamment longue, on peut retrouver le polynôme de rétroaction du registre et donc, générer le reste de la séquence. Plus précisément, si on note s la séquence générée par un LFSR de taille L et si on connaît une sous-séquence $s^n = s_k, s_{k+1}, \ldots, s_{k+n-1}$ avec $k \geq 0$ de taille $n \geq 2L$, alors la résolution du système de L équations à L inconnues $c_1, \ldots, c_L$ sur $\mathbb{F}_2$ suivant :

$$\begin{pmatrix} s_k & s_{k+1} & \cdots & s_{k+L-1} \\ s_{k+1} & s_{k+2} & \cdots & s_{k+L} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ s_{k+L-1} & s_{k+L} & \cdots & s_{k+2L-2} \end{pmatrix} \begin{pmatrix} c_L \\ c_{L-1} \\ . \\ . \\ . \\ c_1 \end{pmatrix} \begin{pmatrix} s_{k+L} \\ s_{k+L+1} \\ . \\ . \\ . \\ s_{k+2L-1} \end{pmatrix}$$

permet de retrouver le polynôme de rétroaction $C(x) = 1 + \sum_{i=1}^{L} c_i x^i$ du LFSR. En effet, on peut montrer que si s^n a été générée par un polynôme irréductible de $\mathbb{F}_2[x]$, alors ce système admet une solution unique dans $\mathbb{F}_2^L$. Bien sûr, même si on dispose de s^n, on ne connaît pas L. On peut alors construire un système d'équations linéaires de taille plus grande que nécessaire, dont la résolution fournit une solution, les colonnes de ce système n'étant pas indépendantes. Mais, le point important est que le LFSR est totalement connu dès lors que n est suffisamment grand.

La simplicité d'implantation des LFSR demeure un atout évident. Leur vulnérabilité aux attaques à clair connu étant dûe à leur linéarité, l'idée pour pouvoir néanmoins les utilser est de les "détruire". Trois méthodes sont employées :

- utiliser plusieurs LFSR dont les sorties sont combinées à l'aide d'une fonction non-linéaire f. La sortie de f constitue alors le flot de clé.
- utiliser plusieurs LFSR dont l'un sert à choisir la sortie du LFSR qui sera utilisée à un instant donné.
- utiliser un seul LFSR : le flot de clé étant obtenu par combinaison du contenu de ses cases mémoire par une fonction non-linéaire.

La génération d'un flot de clé par la première méthode est sujette aux attaques par corrélation de Siegenthaler dont nous écrivons brièvement le principe :

On se place dans le cadre d'une attaque à clair connu et on suppose que le clair est combiné avec le flot de clé par un simple "xor" pour produire le chiffré. On dispose donc d'une sous-séquence de taille N de la sortie de f, notée $S^N = S_1, \ldots, S_N$. On note $R_i,\ 1 \leq i \leq n$, les n LFSR du système, chaque R_i étant de longueur maximale.
Soit $L_i,\ 1 \leq i \leq n$, les tailles respectives de ces LFSR.
On suppose également que les polynômes de rétroaction et que la fonction f sont publics. En fait, seules les initialisations des registres sont secrètes.
Le nombre de clés possibles est donc $\prod_{i=1}^{n} 2^{L_i} - 1$.

Soit $1 \leq i \leq n$.
On note X_i la variable aléatoire prenant les valeurs de sortie R_i. D'après les propriétés des m-séquencess précédentes, on peut supposer que X_i suit la loi uniforme dans $\mathbb{F}_2$ et, si on choisit les polynômes de rétroaction de manière indépendante, que les X_i sont indépendantes. On pose alors

$$p_i = P(\{f(X_1, \ldots, X_m) = X_i\}).$$

Soit $s_1^i, \ldots, s_N^i$, N bits de sortie de R_i. On définit la corrélation entre la sortie de R_i et f par :

$$\alpha_i = \sum_{j=1}^{N} (1 - 2(S_j + s_j^i)).$$

On peut montrer que la variable aléatoire prenant comme valeur α_i admet pour moyenne une fonction de p_i égale à 0 si $p_i = \frac{1}{2}$.
L'attaque de Siegenthaler consiste donc à essayer toutes les initialisations possibles pour R_i et à calculer, pour chacune d'elles, la corrélation α_i entre la suite générée par R_i et S^N. Si l'initialisation de R_i est incorrecte alors la valeur trouvée correspond à une corrélation entre S^N et une suite aléatoire indépendante des entrées de f, donc sa moyenne est proche de 0. Si sa moyenne dépasse un certain seuil, on considère que l'on a trouvé l'initialisation correcte.

Si on dispose d'une corrélation entre la sortie de f et celle de chacun des n registres R_i indépendamment, les états initiaux de chacun des registres peuvent être retrouvés avec un coût total d'au plus $\sum_{i=1}^{n} (2^{L_i} - 1)$ essais, ce qui est bien inférieur à celui de la recherche exhaustive. On peut également exploiter des corrélations entre la sortie de f et les sorties d'un sous-ensemble de LFSR simultanément.

Ceratines fonctions dites sans corrélation résistent à ce type d'attaques : de manière informelle, une fonction booléenne sans corrélation d'ordre t est telle que la distribution de sa sortie est inchangée même si on fixe jusqu'à t bits de son entrée.
Dans le contexte qui nous intéresse, une fonction f sans corrélation d'ordre 1 résiste donc à l'attaque consistant à corréler la sortie d'un registre avec sa sortie, puisqu'il faudra comparer la sortie de f avec celle d'au moins deux registres pour observer un biais statistique. Plus généralement, une fonction sans corrélation d'ordre t résiste aux attaques par corrélation exploitant les sorties d'au plus t registres simultanément.

Ainsi, ces méthodes de génération de flots de clés implémentées avec des paramètres bien choisis comme les tailles suffisamment grandes des LFSR semblent résister aux attaques connues.

Dans chacune de ces utilisations, les polynômes de rétroaction peuvent être rendus publics ou non. S'ils sont rendus publics alors les attaques statistiques sont en général plus faciles à mener et dans le cas contraire, ils doivent être choisis uniformément et aléatoirement parmi les polynômes primitifs d'un degré donné.
Une façon peu coûteuse d'implémenter un LFSR est de choisir un polynôme creux,

en particulier un trinôme. Néanmoins, il existe des attaques spécifiques basées sur la creusité des polynômes de rétroaction. Leur utilisation est donc peu recommandée.

7.1.2 Schémas par blocs

Nous allons maintenant nous intéresser à un type de chiffrement à clé secrète, appelée chiffrement par blocs. Dans un tel procédé, le message est découpé en blocs de taille fixe et chiffré bloc par bloc. Formellement :

Définition 34
Soit $n, l \in \mathbb{N}^*$ avec n la taille des blocs et $K \subseteq \mathbb{F}_2^l$.
Un chiffrement par blocs est une fonction $E : \mathbb{F}_2^n \times K \to \mathbb{F}_2^n$ telle que, pour tout $k \in K$, la fonction $E(., k) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ est inversible. La fonction inverse $E(., f)^{-1}$ dite fonction de déchiffrement est notée $D(., k)$.

Notons que les chiffrements par transposition et substitution sont des exemples de chiffrement par blocs : les blocs sont réduits à une lettre dans le cas de la substitution simple.

Complexité d'une attaque d'un schéma de chiffrement par blocs :
La meilleure mesure de sécurité pour un schéma de chiffrement actuel est la complexité de la meilleure attaque connue. On distingue divers types de complexité :

- La complexité des données : c'est le nombre moyen d'unités de données nécessaires pour mener à bien l'attaque. L'unité de données est souvent un bloc de message.
- La complexité en espace : c'est le nombre moyen d'unités de données que l'on doit stocker durant l'attaque.
- La complexité en temps : c'est le nombre moyen d'opérations nécessaires à l'attaque.

La complexité d'une attaque est alors définie comme la plus coûteuse des trois.
Pour un chiffrement par blocs de taille n, une attaque en complexité de données 2^n est toujours possible ; en effet, la fonction de chiffrement est complètement caractérisée par la donnée des chiffrés des 2^n clairs possibles. Pour un chiffrement avec une clé de l bits, une attaque dont la complexité en temps est 2^l est toujours possible par recherche exhaustive sur la clé.
Ainsi, la taille effective de la clé doit être suffisamment grande pour rendre la recherche exhaustive infaisable et la taille des blocs suffisamment grande aussi pour empêcher la construction de dictionnaires.

Le chiffrement par transposition ou substitution n'offre pas un niveau acceptable de sécurité. La substitution ajoute de la confusion au procédé de chiffrement, c'est-à-dire qu'elle a pour but de masquer la relation entre le clair et le chiffré. La transposition ajoute de la diffusion au chiffrement, dans le sens où elle sert à "éparpiller" la redondance du message, par permutation des bits de celui-ci. On voit donc que ces deux opérations n'offrent pas le même type de sécurité. Tout en n'étant pas satisfaisantes individuellement, celles-ci peuvent être combinées pour construire des

chiffrements sûrs, l'idée étant de bénéficier de la sécurité partielle et complémentaire de chacune.

Définition 35

1. *On appelle* ***chiffrement produit*** *un chiffrement par blocs qui combine plusieurs transformations élémentaires. Ces transformations peuvent être des transpositions, des substitutions, des opérations linéaires ou arithmétiques.*
2. *Un* ***chiffrement itératif par blocs*** *est un chiffrement résultant de l'application itérée d'une fonction F à chaque bloc du clair, F étant un chiffrement produit. Chaque application de F est appelée* ***tour****. Un tel chiffrement est caractérisé par :*
   - *son nombre de tours,*
   - *la taille des blocs,*
   - *la taille de la clé.*

Dans un chiffrement itératif par blocs, chaque tour fait intervenir une sous-clé qui est dérivée de la clé de départ. Pour rendre le chiffrement inversible, la fonction F doit être une bijection et ceci pour chaque sous-clé.

Il existe essentiellement deux structures de chiffrement itératif par blocs :

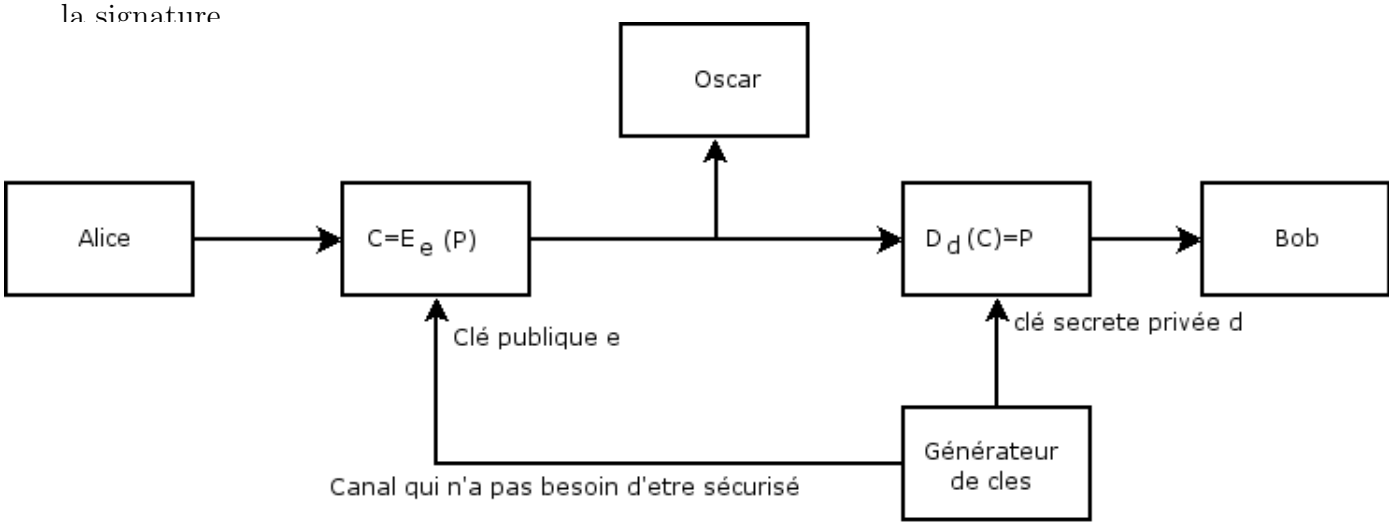
- La première est appelée **réseau de substitution-permutation** ou **réseau-SP** : dans cette structure, F ne fait intervenir que des substitutions et des permutations. Le chiffrement à clé secrète AES est construit sur ce modèle.
- La deuxième structure est appelée schéma de Feistel. Elle est à la base de nombreux systèmes à clé secrète comme l'algorithme DES.

7.2 Cryptographie à clé publique

Nous présentons dans cette section les fondements de la cryptographie à clé publique. Nous introduisons d'abord les notions de problème difficile et de fonction à sens unique et de factorisation entière, puis, nous décrivons les schémas RSA, Diffie-Hellman, El Gamal en insistant sur l'équivalence ou non de leur sécurité avec la difficulté des problèmes sur lesquels ils reposent : la factorisation entière et l'extraction de logarithmes discrets. Ces différents schémas sont appelés *"Schémas asymétriques" ou "Schémas à clé publique"*.

Nous allons voir dans cette section que la cryptographie à clé publique fournit une méthode élégante pour réaliser la distribution des clés. En effet, nous avons vu précédemment que les cryptosystèmes à clé privée utilisaient la même clé au chiffrage et au déchiffrage : $e = d$. un tel cryptosystème requiert donc la communication à l'avance de la clé secrète entre l'expéditeur et le récepteur, ce qui est une opération délicate, surtout si la clé doit être donnée à un grand nombre d'utilisateurs. Si la clé tombe entre les mains de l'ennemi, le système entier est compromis.

Un cryptosystème à clé publique élimine ce problème en permettant l'utilisation d'une clé différente au cryptage et au décryptage : $e \neq d$. La clé e est publique tandis que la clé d est secrète. De cette manière, la clé de cryptage e peut être transmise à travers le canal de communication non sûr puisque l'ennemi la connaît.
Mais, nous verrons également que, bien qu'ayant été motivée par ce problème, cette branche de la cryptographie a beaucoup d'autres applications comme le chiffrement, la signature



Chiffrage asymétrique

7.2.1 Problèmes difficiles et fonctions à sens unique.

Pour construire des schémas dans lesquels l'algorithme de chiffrement peut être rendu public, tout en préservant le caractère secret de l'algorithme de déchiffrement,

on a recours à des fonctions à sens unique : de manière intuitive, ce sont des fonctions faciles à calculer mais difficiles à inverser.

Définition 36
Une fonction $f : X \longrightarrow Y$, est dite ***à sens unique*** *si*
- $\forall\ x \in X$, $f(x)$ *est calculable en temps polynomial.*
- *Pour presque tout $y \in Im(f)$, il est infaisable de façon calculatoire de trouver $x \in X$ tel que $f(x) = y$.*

7.2.2 Factorisation entière.

La difficulté de factoriser un nombre entier n croît évidemment avec la taille de n. L'algorithme le plus simple de factorisation consiste en la division de n par tous les premiers jusqu'à $\sqrt{n}$: il est appelé **Crible d'Erasthostène**. La complexité d'un tel algorithme est $\sqrt{n}$ dans le pire des cas.
Pour n de l'ordre de 2^{40}, c'est une méthode tout à fait acceptable, mais, en cryptographie, on s'intéresse à des nombres de beaucoup plus grande taille : de l'ordre de 2^{500} et donc, à des méthodes de factorisation plus puissantes.
Actuellement, le meilleur algorithme de factorisation d'un entier quelconque possède une complexité en $\Theta(exp((c + \theta(1))(ln\ n)^{1/3}(ln\ ln\ n)^{2/3}))$ *où* $c \approx 1,923$.
Il permet de factoriser des nombres jusqu'à 158 chiffres décimaux c'est-à-dire : 525 bits.

La factorisation, bien qu'ayant connu des progrès considérables depuis ces dernières années, reste donc encore un problème "difficile" sous réserve de choisir des entiers de taille convenable.

Nous définissons alors une fonction à sens unique basée sur la factorisation de la manière suivante :
Soit $n \in \mathbb{N}^*$ / $n = p \times q$ avec p et q deux premiers de même taille.

$$\text{Soit}\quad F : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & x^e\ mod\ n \end{array} \qquad \text{avec } e \text{ / } (e, (p-1)(q-1)) = 1.$$

Alors, étant donnés (n, e) :
- F est calculable en temps polynomial.
- Pour $y \in \mathbb{Z}/n\mathbb{Z}$, le problème consistant à trouver $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $F(x) = y$ n'admet pas de solution en temps polynomial, sous l'hypothèse que n soit difficile à factoriser.

Ainsi, la fonction F pourrait être utilisée pour chiffrer des messages, l'opération de chiffrement $F(m) = m^e\ (mod\ n)$ ne faisant intervenir que des données publiques et l'opération inverse étant "infaisable".
Néanmoins, ce schéma n'est pas très pratique : en effet, personne ne peut déchiffrer $F(m)$. Or, on souhaite que le destinataire légitime du message puisse le faire.

Pour cela, nous allons introduire une propriété suppléméntaire requise pour une fonction à sens unique :

Définition 37
Une fonction $f : X \longrightarrow Y$ est dite ***à sens unique avec trappe*** *si :*
- *f est à sens unique,*
- *connaissant une information supplémentaire appelée trappe, le calcul, pour tout $y \in Im(f)$, de $x \in X$ tel que $f(x) = y$ est réalisable en temps polynomial.*

De telles fonctions - ou plus exactement des candidates car aucune fonction n'a à ce jour mathématiquement été prouvée à sens unique - sont construites à partir de problèmes difficiles. Je présente maintenant les principaux problèmes difficiles utilisés en cryptographie :
- les fonctions à sens unique qui en découlent,
- des exemples de cryptosystèmes induits par ces fonctions.

Une première application : le stockage des mots de passe

Considérons le problème de l'accès d'un ordinateur contrôlé par un mot de passe. Il est dangereux de stocker en l'état une liste des mots de passe des utilisateurs autorisés, dans la mesure où il serait très difficile de maintenir cette liste secrète.
l'astuce suivante est une des premières utilisations cryptographiques des fonctions à sens unique.
On prend une telle fonction f et on stocke dans la mémoire de la machine non pas x mais $f(x)$ pour chaque mot de passe x d'un utilisateur autorisé.
Un utilisateur accède à la machine en présentant un mot de passe x et celle-ci vérifie l'autorisation d'accès en calculant $f(x)$ puis en comparant le résultat à la liste des $f(x)$ en sa possession : elle accepte la connexion si $f(x)$ coïncide avec un de la liste.
Ainsi, un fraudeur doit, pour réussir, trouver un a tel que $f(a)$ soit égale à un des $f(x)$ stockés par la machine.
Ceci est infaisable avec une puissance de calcul limitée, même lorsqu'on connaît les $f(x)$ et la fonction f.

7.2.3 L'exponentiation modulaire

Une fonction à sens unique très utilisée

Il s'agit de passer maintenant à des candidats concrets. Une fonction considérée comme difficilement inversible est l'exponentiation modulo un nombre premier p. Elle est souvent appelée exponentielle discrète ou modulaire.
La fonction est construite de la façon suivante :

1. On se donne un grand nombre premier p et un nombre α primitif modulo p
2. On définit f telle que : $\begin{array}{ccc} \mathbb{Z}_p^* & \longrightarrow & \mathbb{Z}_p^* \\ x & \longmapsto & f(x) = \alpha^x \end{array}$

où α est choisi de préférence primitif pour que f soit bijective.

Tous les algorithmes connus pour inverser cette fonction, c'est-à-dire calculer le logarithme discret, nécessitent un temps de calcul non polynomial en $log(p)$.

7.2.4 Le protocole de Diffie-Hellman

La cryptographie moderne, fondée donc sur les fonctions à sens unique, a connu son véritable début lors de la parution en 1976 de l'article de Diffie-Hellman "New directions in Cryptography".
Les auteurs y résolvent grâce à l'exponentiation modulaire un problème de partage de secret considéré jusqu'alors insoluble.

Le principe

Alice et Bob ne disposent pour communiquer que d'un canal non sûr c'est-à-dire non protégé des écoutes indiscrètes.
Ils souhaitent cependant communiquer de manière confidentielle. Il leur faut se mettre d'accord publiquement sur un procédé de communication assurant la confidentialité. Si l'on accepte que cette confidentialité ne soit garantie que par la limitation de la puissance de calcul adverse, ce problème admet une solution très simple et très ingénieuse.
Il suffit qu'Alice et Bob se mettent d'accord sur un nombre secret S qui leur servira, par exemple, de clé pour un système de chiffrement traditionnel. Il faut bien entendu ni transmettre S sur le canal , ni transmettre d'informations permettant de déterminer S.

Voici la solution proposée :

- Alice et Bob se mettent d'accord publiquement - sur le canal - sur un grand nombre premier p et sur une racine primitive α modulo p.
- Alice choisit secrètement et aléatoirement un nombre a qu'elle gardera secret.
- Mais, elle transmet à Bob et à qui veut le lire, le nombre $\alpha^a mod\ p$.
- Bob se choisit de même un nombre secret b et il transmet α^b.
- Alice et Bob décident ensuite que leur secret commun sera $S = \alpha^{ab} mod\ p$.
- Alice accède à S en élevant α^b à la puissance son nombre secret a et Bob élève α^a à la puissance b.

On ne voit pas comment, à partir des seules indications transmises publiquement, $(p, \alpha, \alpha^a, \alpha^b)$, on peut obtenir α^{ab} sans calculer un logarithme modulo p ou faire un quelconque calcul d'une complexité démesurée.

Remarques 7

1. *La sécurité du système est calculatoire. Elle repose sur deux hypothèses :*
   - *La puissance de calcul de l'adversaire doit être limitée.*
   - *Avec une puissance de calcul et un temps limités, il n'est pas possible d'inverser la fonction exponentielle et de trouver α^{ab} à partir de $(p, \alpha, \alpha^a, \alpha^b)$.*
2. *Deux propriétés de l'exponentielle sont en fait utilisées : la difficulté de l'inverser et la commutativité de l'exponentiation $(\alpha^a)^b = \left(\alpha^b\right)^a$.*

7.2.5 Le système d'El Gamal

Le protocole de Diffie-Hellman a ouvert la voie à toute une série d'algorithmes cryptographiques nouveaux.
Un des premiers concepts à émerger est celui de système de chiffrement à clé publique. L'idée est de rompre la symétrie du chiffrement et du déchiffrement. Dans un système traditionnel, la connaissance de la fonction de chiffrement f implique la connaissance de la fonction de déchiffrement f^{-1}.
Mais, connaître une fonction, dans notre contexte, signifie disposer d'un algorithme efficace pour la calculer. Or, nous avons vu précédemment qu'on ne sait pas transformer un algorithme efficace qui calcule f en un algorithme efficace qui calcule f^{-1}.
Si l'on peut en outre donner au destinataire un algorithme secret qui calcule f^{-1} alors il n'y a plus besoin de garder secrète la fonction de chiffrement f.
On a alors réalisé un système dit à clé publique ou asymétrique :
Seul le destinataire possède le secret permettant de déchiffrer. C'est le grand avantage d'un tel système : plus besoin de se préoccuper d'un partage de secret toujours délicat.

Remarque 13 *On dit parfois d'une telle transformation f qu'elle est à sens unique à porte dérobée (ou avec trappe). En l'absence d'un certain secret, elle est effectivement difficile à inverser. Dans le cas contraire, l'inversion est facile.*

Passons à la réalisation concrète. Le système d'El Gamal est fondé sur la fonction exponentielle et se rapproche conceptuellement le plus du protocole de Diffie-Hellman.

Le destinataire potentiel, Bob, possède deux clés :
- une clé secrète : un nombre s.
- une clé publique : un nombre premier p, un entier α primitif modulo p et l'entier modulo p donné par $P = \alpha^s$.

Chiffrement.

Toute personne souhaitant envoyer un message M à Bob doit disposer d'un moyen de connaître les éléments de sa clé publique. Pour chiffrer le message $M \in \mathbb{Z}_p^*$, on procède ainsi :
On tire au hasard un nombre k modulo p et on calcule $C_1 = \alpha^k mod\ p$ et $C_2 = MP^k\ mod\ p$.
Le message chiffré est le couple (C_1, C_2).

Pour décrypter c'est-à-dire recouvrer M sans la clé secrète, il faut découvrir P^k. On peut chercher l'exposant k mais, pour cela, on ne dispose que de $C_1 = \alpha^k$ et on se trouve confronté au calcul de logarithme discret.

Déchiffrement.

En revanche, si l'on est le destinataire légitime du message et que l'on dispose de la clé secrète s, on détermine facilement P^k par le calcul suivant : $P^k = \alpha^{sk} = C_1^s \ mod \ p$.
le message M est donc donné par $M = \frac{C_2}{C_1^s} \ mod \ p$.

Soulignons la dissymétrie du protocole : si Alice et Bob veulent communiquer de manière confidentielle , chacun utilisera pour chiffrer son message la clé publique de l'autre. Pour déchiffrer, chacun utilisera sa propre clé secrète.

Remarque 14 *La fonction de chiffrement $f : M \mapsto C$ n'est pas à proprement parler une fonction puisqu'à un message clair M correspondent potentiellement plusieurs cryptogrammes. On continuera tout de même à parler de fonction ou de fonction à sens unique dans ce cas.*

Inconvénient et avantage du système El Gamal.

1. Inconvénient : le message chiffré est deux fois plus long que le message original.
2. Avantage : l'introduction de l'aléa k permet au même message M chiffré deux fois à des moments différents de se traduire par des cryptogrammes différents.

7.2.6 Le système RSA

Le système de cryptage RSA a été inventé en 1978 par Ronald **R**ivest, Adi **S**hamir, et Leonard **A**dleman. Ils avaient décidé de travailler ensemble pour établir qu'un nouveau système de codage révolutionnaire, dénommé "système à clé publique" que W.Diffie et M.Hellman venaient d'inventer, était une impossibilité logique (autrement dit, que tout système de cryptage de cette nature présentait des failles). Ils ne réussirent pas dans leur projet, mais, au contraire, découvrirent un nouveau système à clé publique qui supplanta vite celui de W.Diffie et M.Hellman. Il est fondé sur la difficulté de factoriser des grands nombres et la fonction à sens unique utilisée est la fonction puissance.

Le principe

La clé secrète est constituée de deux grands nombres premiers p et q.
La clé publique est constituée du produit $n = pq$ et d'un entier e inversible modulo $\varphi(n)$.
Le chiffrement d'un message, représenté par un entier M modulo n, se fait par la transformation suivante : $M \longmapsto M^e \ mod \ n$.

Pour déchiffrer, il faut savoir calculer la fonction réciproque. Or, celle-ci est tout simplement : $M \longmapsto M^d \ mod \ n$ où d est l'inverse de $e \ mod \ \varphi(n)$ c'est-à-dire : $ed \equiv 1 \ mod \ \varphi(n)$.
En effet, rappelons que d'après le théorème d'Euler : si M est inversible modulo n alors $M^{\varphi(n)} \equiv 1 \ mod \ n$.

On a donc : $(M^e)^d = M^{ed} = M \ mod \ n$.

Si M est inversible modulo n alors on a, par exemple, $M = 0 \ (mod \ p)$ et M est inversible modulo q.
Dans ce cas, $M^{\varphi(n)} = 0 \ (mod \ p)$ et $M^{\varphi(q)} = 1 \ (mod \ q)$ ***par le théorème de Fermat***.
De plus, comme $\varphi(n) = \varphi(p)\varphi(q)$ alors $M^{\varphi(n)} = 1 \ (mod \ q)$.

On en déduit que, puisque $ed = 1 \ (mod \ \varphi(n))$, $M^{ed} = 1 \ (mod \ q)$ et $M^{ed} = 0 \ (mod \ \varphi(n))$.
D'après le théorème chinois, on obtient la même égalité que précédemment :

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

Notons que, si l'on connaît $\varphi(n)$, il est alors facile de calculer l'exposant d à partir de e en appliquant l'algorithme d'Euclide étendu.

Notons aussi que : $\begin{array}{rcl} \varphi(n) & = & (p-1)(q-1) \\ & = & pq - (p+q) + 1 \\ & = & n - (p+q) + 1 \end{array}$
Cela veut dire que non seulement on obtient $\varphi(n)$ dès que l'on possède p et q, mais, réciproquement, si l'on connaît $\varphi(n)$ alors on dispose de $p+q$, de pq et on en déduit p et q.
En résumé, connaître $\varphi(n)$ équivaut à connaître la factorisation de n. Mais, comme on ne sait pas factoriser efficacement les grands entiers, on ne peut alors pas accéder à $\varphi(n)$ et à l'exposant caché d.

Avantages

Les cryptosystèmes à clé publique comme RSA, comparés à ceux à clé privée, peuvent être utilisés dans un mode signature. Pour cela, il suffit d'"inverser" le rôle des exposants e et d.
Le détenteur de la clé secrète, c'est-à-dire de la factorisation de n ou de l'exposant secret d, peut signer un message M en prouvant qu'il détient d. Pour cela, il envoie en même temps que le message M la signature M^d. Pour vérifier l'authenticité de la signature, il suffit de l'élever à la puissance e (l'exposant public) et de vérifier que $(M^d)^e = M$.

Remarque 15 *Ce phénomène est très général. Chaque fois que les fonctions de chiffrement f et de déchiffrement f^{-1} d'un système cryptographique asymétrique sont bijectives, le détenteur de l'algorithme secret qui calcule f^{-1} peut l'utiliser pour signer ses messages.*
Une signature d'in message M prend simplement la forme $S = f^{-1}(M)$ et l'équation de vérification est $M = f(S)$.

Inconvénients

RSA et les schémas de chiffrement à clé publique en général étant significativement plus lents que les schémas symétriques, c'est-à-dire de chiffrement à clé privée, on ne les utilisera en pratique que pour le transport de clés secrètes ou pour le chiffrement de données de petite taille.

Sécurité

Nous allons voir dans ce chapitre les précautions élémentaires à prendre lors de la mise en oeuvre du système RSA, ainsi que les principales attaques connues.

Premières précautions. Dans un premier temps, il convient de choisir un module n de taille 1024 bits ou plus, en particulier si le système est destiné à être utilisé sur une longue durée.
Les nombres premiers p et q devront être sélectionnés de telle sorte que factoriser n soit difficile. Ainsi, p et q devront être approximativement de même taille.
Pour rendre les méthodes de factorisation de type (p-1) inefficaces, on peut également imposer que $p-1$, $p+1$, $q-1$ et $q+1$ aient chacun un grand facteur premier. Cependant, si p est de grande taille et est choisi aléatoirement, il est probable que $p-1$ et $p+1$ possèdent de grands facteurs premiers. En pratique, on peut donc choisir p et q aléatoirement dans les tailles requises.

Une efficacité plus ou moins durable. RSA ne garantit pas que le message ne sera jamais déchiffré, il garantit seulement qu'il faudra beaucoup de temps avant de prendre connaissance du message. Il est donc conseillé de changer régulièrement de clé.

Attaque de l'homme au centre. Supposons que Cédric souhaite connaître les messages qu'Alice envoie à Bernard. Il lui suffit de choisir de nouvelles clés publique (e',n') et privée (d',n') et de les envoyer à Alice en lui faisant croire que ce sont les clés de Bernard. De cette façon, Cédric, qui intercepte tous les messages provenant d'Alice, peut alors les déchiffrer, les lire, puis les chiffrer avec l'ancienne clé de Bernard, qui n'est au courant de rien. Bernard reçoit alors le message et parvient lui aussi à le lire, mais sans se douter que quelqu'un d'autre l'a lu entre-temps.
Il est donc très important pour Alice et Bernard de toujours s'assurer que personne ne tente de modifier les paramètres en faisant plusieurs vérifications.

Exposant $e = 3$. Pour accélérer l'opération de chiffrement, on peut penser à utiliser un exposant public e petit, par exemple $\boxed{e=3}$.
Ce choix permet de réduire le calcul de m^e (mod n) à un carré et une multiplication modulaires. Décrivons une attaque très simple exploitant le fait que $e = 3$:
Supposons qu'Alice veuille envoyer le même message M à Bob (de module n_1), Cédric(n_2), et David (n_3) qui partagent tous les trois le même exposant e. Elle regarde leur clé publique dans l'annuaire, puis envoie aux personnes concernées :

$$\begin{cases} c_1 &= M^3 \ (mod\ n_1) \\ c_2 &= M^3 \ (mod\ n_2) \\ c_3 &= M^3 \ (mod\ n_3) \end{cases}$$

aux entités concernées.
On suppose que les n_i, $1 \leq i \leq 3$, sont deux à deux premiers, ce qui est très probablement le cas si les premiers entrant dans la construction des n_i sont choisis aléatoirement. Elodie, qui écoute les communications d'Alice, intercepte les trois chiffrés c_i. En résolvant, par le théorème chinois, le système de congruences :

$$\begin{cases} x &\equiv c_1 \ (mod\ n_1) \\ x &\equiv c_2 \ (mod\ n_2) \\ x &\equiv c_3 \ (mod\ n_3) \end{cases}$$

elle obtient $x \equiv M^3 \ (mod\ n_1 n_2 n_3)$.
Or, $M^3 < n_1 n_2 n_3$, car $M < n_i \ \forall i \in$1,2,3.
Donc $\boxed{x = M^3}$.
IL ne reste plus qu'à calculer $x^{\frac{1}{3}}$ pour retrouver M.
Ceci montre que $e = 3$ ne doit pas être utilisé si le même message doit être envoyé plusieurs fois.

D'une manière générale, les exposants publics petits sont à éviter : en effet, si on souhaite chiffrer de petits messages $M < n^{\frac{1}{e}}$, alors on peut retrouver M à partir de c en calculant $c^{\frac{1}{e}}$.

Pour empêcher ce type d'attaque et aussi le chiffrement de messages courts, on peut néanmoins "saler" le message avant de l'envoyer, c'est-à-dire : concaténer à M une chaîne binaire pseudo-aléatoire qui est différente pour chaque envoi.
Le choix de e assez grand, ajouté à la précaution de chiffrer des messages de taille approximativement égale à celle de n (par salage éventuel), permet de contrer les attaques précédentes tout en rendant l'opération de chiffrement efficace.

Attaques multiplicatives Cette attaque exploite la propriété "homomorphique" de RSA, à savoir

$$(m_1 m_2)^e (\text{mod n}) \equiv (m_1^e \text{ mod n})(m_2^e \text{ mod n}) \text{ mod n} \equiv c_1 c_2 \text{ mod n}.$$

Autrement dit, le chiffré du message $m_1 m_2$ est égal au produit des chiffrés de m_1 et de m_2. Supposons que Cédric veuille connaître le clair m correspondant à un chiffré c destiné à Bob. Il peut monter l'attaque à chiffré choisi adaptative suivante :
Il choisit $x \in \mathbb{Z}_n^*$ et demande à Bob le clair correspondant au chiffré $\bar{c} = cx^e (mod\ n)$ (il masque c à l'aide de x).
Bob calcule alors $\bar{m} = \bar{c}^d$ (mod n), et l'envoie à Cédric.
Or $\bar{m} \equiv c^d x^{ed} (mod\ n) \equiv mx (mod\ n)$. A partir de $\bar{m}$, Cédric retrouve aisément m en enlevant le masque x.
Un moyen de contrer cette attaque est d'imposer un format particulier aux messages clairs.
Ainsi, si m possède ce format alors il est très peu probable que mx le possède aussi.

Bob refusera alors de fournir le clair $\bar{m}$ correspondant à $\bar{c}$, car il n'aura pas la forme requise.

Petit exposant d Le choix d'un petit exposant d permet de réduire le coût du déchiffrement. Néanmoins, si $d < n^{0,292}$, on peut retrouver p et q à partir de (n, e), par un algorithme dû à Boneh et Durfee en 1999. On choisira donc d de taille approximativement égale à celle de n.

Influence de la taille de bloc Le choix de la taille de bloc n'est pas anodin. En effet, si on choisit de façon naïve une taille de bloc égale à 1, le chiffrement par RSA n'est rien de plus qu'une simple substitution, car chaque bloc (et donc chaque caractère) sera toujours chiffré de la même manière. Une attaque basée sur la fréquence d'apparition des lettres dans une langue donnée permet alors de déchiffrer très rapidement le message original.

7.3 Application au cryptosystème à clé publique RSA.

Le système R.S.A. est le système à clés publiques le plus utilisé. Il a été inventé en 1978 par R. Rivest, A. Shamir et L. Adleman. Il est basé sur la difficulté de factoriser les grands nombres ou de savoir s'ils sont premiers.
Nous rappelons dans un premier temps son principe de façon concrète et dans un second, nous effectuerons des tests de RSA en fonction de la taille des blocs.

7.3.1 Création des clés

- Une personne A choisit ou génère deux grands nombres premiers p et q d'à peu près même taille.
- Elle calcule $n = p \times q$ et $\Phi(n) = (p-1)(q-1)$.
- Elle choisit $e \in \mathbb{N}$ / $1 < e < \Phi(n)$ et $pgcd(e, \Phi(n)) = 1$.
- Elle calcule $d \in \mathbb{N}$, un entier unique / $1 < d < \Phi(n)$ et $e.d \equiv 1 (mod\ \Phi(n))$.
- Elle publie la clé (n, e) dans le guide des clés publiques et garde secrète sa clé privée d.

Remarque 16 *La terminologie "clé privée" vient du fait que si n et e sont donnés $\Rightarrow$ clé publique (n, e) alors, les nombres p et q sont gardés secrets et il est en général très difficile de déterminer d $\Rightarrow$ clé privée (p, q, d).*

Définition 38
Le couple (n, e) est la clé publique d'une personne A et l'entier d est sa clé privée où :

- $n \longleftrightarrow$ *module,*
- $e \longleftrightarrow$ *exposant de cryptage,*
- $d \longleftrightarrow$ *exposant de décryptage.*

7.3.2 Algorithme de cryptage

Une personne A veut envoyer un message m à la personne B.
Elle exécute alors les étapes suivantes :

- se procurer la clé publique (n, e) de B.
- transformer son message m en une suite de nombres M appartenant à l'intervalle $[0, n-1]$.
- calculer, pour chacun des nombres M, le nombre $c = M^e(modn)$.
- envoyer à B le message codé formé du nombre c ou de la concaténation de ces nombres c.

Remarque 17 *On considère que le message est un nombre dans* $[0, n-1]$ *et que c, le message codé, se trouve dans le même intervalle.*

7.3.3 Algorithme de décryptage

A l'arrivée du message codé c, la personne B décrypte le message c en effectuant $c^d(modn)$. Ce décryptage est correct grâce au résultat suivant :

Proposition 23
Soit M la suite de nombres du message $\in [0, n-1]$.
Soit e l'exposant de cryptage $\in [1, \Phi(n)]$.
Soit $n \in \mathbb{N}$ *tel que* $n = p.q$.
Soit d l'exposant de décryptage $\in [1, \Phi(n)]$.
Alors on a : $(M^e)^d \equiv M(modn)$.

Preuve 10
On rappelle les relations : $n = pq$, $\Phi(n) = (p-1)(q-1)$ *et pgcd(*$\Phi(n)$*,e) = 1.*
Il existe un entier u tel que $ed = 1 + \Phi(n)u$. *On a donc :*

$$c^d = (M^e)^d \equiv M^{ed} \equiv c^{1+\Phi(n)u} \ (mod\ n).$$

- *Supposons que* $p \nmid M$, *alors, par le petit théorème de Fermat, on a :* $M^{p-1} \equiv 1(mod\ p)$. *En élevant les deux membres de cette congruence à la puissance* $u(q-1)$ *et en multipliant par M, on obtient :*

$$M^{ed} \equiv M^{1+u(p-1)(q-1)} \equiv M(mod\ p).$$

- *Cette congruence est aussi exacte si* $p \mid M$ *car alors les deux membres sont nuls modulo p.*

De même, on a :$M^{ed} \equiv M(mod\ q)$.
Comme p et q sont premiers distincts alors $\boldsymbol{M^{ed} \equiv M(mod\ n)}$.

7.3.4 Sécurité du système

Une personne adversaire Z a intercepté le message codé c et veut le décrypter. Elle sait aussi que le message est envoyé à B.
Elle essaie d'abord de calculer le nombre d de B (exposant de cryptage), connaissant le couple (n, e) de B.
Pour pouvoir déterminer d de B, on a besoin du résultat suivant :

Théorème 43 *Les deux problèmes suivants :*

1. *calculer le nombre d, connaissant le couple (n,e)*
2. *factoriser n*

sont équivalents dans le sens où une solution de l'un conduit à une solution de l'autre.

Preuve 11
On sait qu'une solution du second problème conduit à une solution du premier problème.
Réciproquement, supposons connu un nombre d tel que $ed - 1$ *soit pair et* $a^{ed-1} \equiv 1(mod\ n)$*, pour tout a de* U_n*.*

Pour au moins la moitié des éléments a de U_n*, on a* $a^{(ed-1)/2} \neq \pm 1(mod\ n)$*, d'après le théorème de Shor.*

1. *On détermine alors, à l'aide d'une recherche au hasard, un élément a de* U_n *tel que* $a^{(ed-1)/2} \neq \pm 1(mod\ n)$*.*
2. *Cela implique que pgcd(*$n, a^{(ed-1)/2}$*) est un facteur non trivial de n. Donc, il est égal à p ou q. En calculant ce pgcd, on factorise n.*

7.3.5 Implémentation de RSA

J'ai réalisé une implémentation du cryptosystème RSA sous Maple. Voici le fichier obtenu :

```
> restart;
```

```
> chiffrement := proc(message)
> local taille,resultat,i,num;
> num :=
> table(["a"="01","b"="02","c"="03","d"="04","e"="05","f"="06","g"="07",
> "h"="08","i"="09","j"="10","k"="11","l"="12","m"="13","n"="14","o"="15
> ","p"="16","q"="17","r"="18","s"="19","t"="20","u"="21","v"="22","w"="
> 23","x"="24","y"="25","z"="26","A"="27","B"="28","C"="29","D"="30","E"
> ="31","F"="32","G"="33","H"="34","I"="35","J"="36","K"="37","L"="38","
> M"="39","N"="40","O"="41","P"="42","Q"="43","R"="44","S"="45","T"="46"
> ,"U"="47","V"="48","W"="49","X"="50","Y"="51","Z"="52","
> "="53",","="54","?"="55",";"="56","."="57",":"="58","/"="59","!"="60",
> "*"="61","
> %"="62","="="63",")"="64","("="65","-"="66","&"="67","é"="68","
> è"="69","à"="70","+"="71","ê"="72"]):
> if not type(message,string) then ERROR(‘le message doit etre une
> chaine de caracteres‘) fi;
> taille := length(message);
> resultat:="";
> if taille = 0 then RETURN("") fi;
> for i from 1 to taille do
> resultat := cat(resultat,num[substring(message,i..i)]);
> od;
> end:
```

La fonction chiffrement créée une chaine numérique à partir d'une chaine de caractères.

Exemple :

```
> rest:=chiffrement("Bonjour mon ami !!");
```

rest := "28151410152118531315145301130953606O"

```
> dechiffrement := proc(message)
> local taille,resultat,i,num;
> num :=
> table(["01"="a","02"="b","03"="c","04"="d","05"="e","06"="f","07"="g",
> "08"="h","09"="i","10"="j","11"="k","12"="l","13"="m","14"="n","15"="o
> ","16"="p","17"="q","18"="r","19"="s","20"="t","21"="u","22"="v","23"=
> "w","24"="x","25"="y","26"="z","27"="A","28"="B","29"="C","30"="D","31
> "="E","32"="F","33"="G","34"="H","35"="I","36"="J","37"="K","38"="L","
> 39"="M","40"="N","41"="O","42"="P","43"="Q","44"="R","45"="S","46"="T"
> ,"47"="U","48"="V","49"="W","50"="X","51"="Y","52"="Z","53"="
> ","54"=",","55"="?","56"=";","57"=".","58"=":","59"="/","60"="!","61"=
> "*","62"="
> %","63"="=","64"=")","65"="(","66"="-","67"="&","68"="é","69"="
> è","70"="à","71"="+","72"="ê"]):
> if not type(message,string) then ERROR(‘le message doit etre une
> chaine de caracteres‘) fi;
> taille := length(message)/2;
> resultat:="";
> if taille = 0 then RETURN("") fi;
> for i from 1 to taille do
> resultat :=
> cat(resultat,num[substring(message,((i-1)*2)+1..((i-1)*2)+2)]);
> od;
> end:
```

La fonction déchiffrement est la fonction inverse de la fonction chiffrement.

Exemple, en reprenant le chiffre obtenu précédemment on retrouve le message original :

```
> dechiffrement(rest);
```

"Bonjour mon ami!!"

```
> generation_tableau_blocs:=proc(taille_blocs,message)
> local tmp,message2,taille,tab,tab2,i;
> message2:=message;
> tmp:=" ";
> while ((length(message2) mod(taille_blocs)) <> 0) do
> cat(message2,tmp);
> message2:=%;
> od;
> taille:=length(message2)/taille_blocs;
> tab:=Array(1..taille);
> for i from 1 to taille do
> tab[i]:=substring(message2,((i-1)*taille_blocs+1)..(((i-1)*taille_bloc
> s+1)+taille_blocs-1));
> od;
> tab2:=Array(1..taille);
> for i from 1 to taille do
> tab2[i]:=chiffrement(tab[i]);
> od;
> return tab2;
> end:
```

La fonction generation_tableau_blocs renvoie un tableau de chaînes de caractères de taille taille_blocs. Ce tableau représente la chaîne originale coupée en blocs. Si le dernier bloc n'est pas complet, on rajoute des espaces à la fin. Chaque bloc est chiffré grâce à la fonction chiffrement.

Exemple :

```
> tmp:=generation_tableau_blocs(3,"Coucou les gens !!");
```

$tmp :=$ ["291521", "031521", "531205", "195307", "051419", "536060"]

```
> generation_cle:=proc()
> local tmp,p,q,n,phi_n,e,d,flag,iterations,resultat;
> p:=nextprime((rand(10^10..10^100)()));
> q:=nextprime((rand(10^10..10^100)()));
> n:=p*q;
> phi_n:=(p-1)*(q-1);
> flag:=false;
> iterations:=0;
> while flag=false do
> e:=(rand(1..(phi_n-1))());
> if igcdex(e,phi_n)=1 then flag:=true fi;
> iterations:=iterations+1;
> od;
> resultat:=Array(1..3);
> resultat[1]:=292078830633211;
> resultat[2]:=93911173437539;
> resultat[3]:=20934059;
> return resultat;
> end:
```

Cette fonction génère une clé RSA aléatoire. Elle renvoie un tableau dont le premier élément est n, le deuxième e et le troisième d.

Exemple :

```
> cles:=generation_cle();
```

$$cles := [292078830633211,\ 93911173437539,\ 20934059]$$

```
> RSA_crypt:=proc(message,n,e,taille_blocs)
> local blocs_chiffres,blocs_cryptes,i;
> blocs_chiffres:=generation_tableau_blocs(taille_blocs,message);
> blocs_cryptes:=Array(1..ArrayNumElems(blocs_chiffres));
> for i from 1 to ArrayNumElems(blocs_chiffres) do
> blocs_cryptes[i]:=eval((convert(blocs_chiffres[i],decimal,10))&^e
> mod n);
> od;
> return blocs_cryptes;
> end:
```

La fonction RSA_crypt permet de crypter un message grâce au cryptosystème RSA. Elle commence par chiffrer le message passé en argument puis le découpe en blocs de taille taille_blocs. Pour finir, chaque bloc est crypté en utilisant la clé (n,e).

```
> RSA_decrypt:=proc(tableau,n,d,taille_blocs)
> local i,blocs_decryptes,blocs_dechiffres,recu;
> blocs_decryptes:=Array(1..ArrayNumElems(tableau));
> for i from 1 to ArrayNumElems(tableau) do
> blocs_decryptes[i]:=tableau[i]&^d mod n;
> od;
> blocs_dechiffres:=Array(1..ArrayNumElems(tableau));
> for i from 1 to ArrayNumElems(tableau) do
> blocs_dechiffres[i]:=convert(blocs_decryptes[i],string);
> od;
> recu:="";
> for i from 1 to ArrayNumElems(tableau) do
> if (length(blocs_dechiffres[i])<>2*taille_blocs) then
> blocs_dechiffres[i]:=cat("0",blocs_dechiffres[i]) fi;
> recu:=cat(recu,dechiffrement(blocs_dechiffres[i]));
> od;
> return recu;
> end:
```

La fonction RSA_decrypt permet tout simplement de décrypter un message crypté grâce à la fonction RSA_crypt.

Exemple :

```
> message_securise:=RSA_crypt("Bonjour! Ceci est un test pour mon
> TER.",cles[1],cles[2],7);
```

message_securise := [174972251668963, 173781511770635, 16851659775774, 49628687688278, 71563738873072, 41587540266767]

```
> message_recu:=RSA_decrypt(message_securise,cles[1],cles[3],7);
```

message_recu := "Bonjour ! Ceci est un test pour mon TER. "

Notons que si l'on souhaite transmettre le message crypté, il faudra transmettre (dans notre exemple) le tableau message_securise.

```
> RSA_FILE_CRYPT:=proc(fichier,fichier2,n,e,taille_blocs)
> local i,fd,fd2,str,message_securise,taille,nb;
> fd:=fopen(fichier,READ,TEXT);
> str:=readbytes(fd,infinity,TEXT);
> message_securise:=RSA_crypt(str,n,e,taille_blocs);
> fd2:=fopen(fichier2,WRITE,BINARY);
> fprintf(fd2,"%d",message_securise);
> fclose(fd);
> fclose(fd2);
> end:
```

La fonction RSA_FILE_CRYPT crypte un fichier (dont le nom est passé en argument) et enregistre le message sécurisé dans un autre fichier (dont le nom est aussi passé en argument).

Exemple :

```
> RSA_FILE_CRYPT("c:/test.txt","c:/resultat.txt",cles[1],cles[2],2);
```

```
> RSA_FILE_DECRYPT:=proc(fichier,n,d,taille_blocs)
> local i,str,fd,tab,nb,tmp;
> fd:=fopen(fichier,READ,TEXT);
> nb:=0;
> while (feof(fd)=false) do
> nb:=nb+1;
> fscanf(fd,"%d");
> od;
> tab:=Array(1..(nb));
> fclose(fd);
> fd:=fopen(fichier,READ,TEXT);
> i:=1;
> while (feof(fd)=false) do
> tmp:=fscanf(fd,"%d");
> tab[i]:=tmp[1];
> i:=i+1;
> od;
> print(RSA_decrypt(tab,n,d,taille_blocs));
> end:
```

La fonction RSA_FILE_DECRYPT décrypte un message sécurisé placé dans un fichier et affiche ce message dans la ligne de commande.

Exemple :

```
> RSA_FILE_DECRYPT("c:/resultat.txt",cles[1],cles[3],2);
```

"ABCDEFGHIJ"

Chapitre 8

Conclusion

Par manque de temps, je n'ai pas pu approfondir les cryptosystèmes à clé secrète et réaliser un exemple concret : DES. De plus, il aurait été intéressant de réaliser des comparaisons de performance entre les cryptosystèmes à clé secrète et à clé publique. En effet, généralement, les cryptosystèmes tels que DES sont beaucoup plus rapides que le système RSA (environ 400 fois).

L'impléméntation de RSA a été réalisée grâce à Maple mais il aurait été préférable, pour une utilisation réelle, de réaliser cette implémentation dans un langage plus rapide (tel que C).

Annexe A

Preuves des tests

A.1 Test de primalité de Lucas-Lehmer

En effet, l'hypothèse revient à dire que l'ordre de $a(mod\ n)$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ est $n-1$. Or, l'ordre de ce groupe est $\Phi(n)$. On en déduit que $(n-1) \mid \Phi(n)$ et en particulier, $n-1 \leq \Phi(n)$.
Si n est composé, il admettrait deux facteurs propres dans l'ensemble $\{1, 2, \ldots, n\}$ et le nombre $\Phi(n)$ des éléments de cet ensemble, qui sont premiers avec n, serait strictement inférieur à $n-2$.

Donc $\boxed{\Phi(n) = n-1}$ et **n est premier**.

A.2 Critère de primalité de Lucas-Lehmer

Soit p un facteur premier de n.
L'anneau quotient $\mathbb{Z}[X]/I$, où I est un idéal engendré par p et $X^2 - aX + 1$, peut être obtenu de deux façons :

- en quotientant par (p) puis par $(X^2 - aX + 1)$, on obtient $\mathbb{F}_p[X]/(X^2 - aX + 1)$
- en quotientant par $(X^2 - aX + 1)$ puis par (p), on obtient ainsi le schéma suivant :

$$\begin{array}{ccccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}[X] & \longrightarrow & B = \mathbb{Z}[X]/(X^2 - aX + 1) \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{F}_p & \longrightarrow & \mathbb{F}_p[X] & \longrightarrow & K = \mathbb{F}_p[X]/(X^2 - aX + 1) \end{array}$$

Soit x la classe de X dans B et α celle de x dans K.
Le polynôme $X^2 - aX + 1$ est irréductible sur $\mathbb{F}_p$ puisque son discriminant $\Delta = a^2 - 4$ est premier avec p. On en conclut que l'anneau K est un corps de degré 2 sur $\mathbb{F}_p$. Il est donc fini et son groupe multiplicatif K^* est cyclique.
Par ailleurs, l'image (v_n) de la suite de Lucas (V_n) dans $\mathbb{F}_p$ est une suite de Lucas et on a :

$$v_0 \ = \ 2 \ , \ \ v_1 \ = \ a \ (mod\ p) \ \ , \ \ v_n \ = \ \alpha^n \ + \ \alpha^{-n}.$$

L'hypothèse $V_{n+1} \equiv 2 \ (mod\ n)$ et $pgcd(V_{(n+1)/q} - 2, n) = 1$ pour tout facteur premier q de $n+1$ implique :

- $v_{n+1} \equiv 2 \ (mod\ p)$ donc $\alpha^{n+1} = 1$,
- $v_{(n+1)/q} \neq 2 \ (mod\ p)$ donc $\alpha^{(n+1)/q} \neq 1$ pour tout facteur premier q de $n+1$.

Donc l'ordre multiplicatif de α dans K^* est $n+1$.

On va maintenant démontrer la relation $\alpha^{p+1} = 1$: on utilise le discriminant Δ. Comme $\Delta \neq 0 \ (mod\ p)$, on a $\Delta^{p-1} \equiv 1 \ (mod\ p)$ et $\Delta^{(p-1)/2} \equiv \pm 1 \ (mod\ p)$.
Le nombre 2 est inversible modulo p puisque p est impair et l'image δ de Δ dans K est le discriminant de l'image du polynôme $X^2 - aX + 1$ dont une racine est α. On en déduit la relation suivante : $\frac{\delta}{4} \equiv (\alpha - \frac{a}{2})^2 \ \ (mod\ p)$.En élevant à la puissance $\frac{(p-1)}{2}$ et en multipliant par $\alpha - \frac{a}{2}$, on obtient :

$$\Delta^{(p-1)/2}(\alpha - \frac{a}{2}) \equiv (\alpha - \frac{a}{2})^p \equiv \alpha^p - \frac{a}{2} \quad (mod\ p).$$

- Si $\Delta^{(p-1)/2} \equiv 1 \ (mod\ p)$, $\alpha - \frac{a}{2} \equiv \alpha^p - \frac{a}{2}$
  donc $\boldsymbol{\alpha^{p-1} \equiv 1 \ (mod\ p)}$.

- Si $\Delta^{(p-1)/2} \equiv -1 \ (mod\ p)$, $\alpha^p + \alpha \equiv a \equiv \alpha + \alpha^{-1}$
  donc $\boldsymbol{\alpha^{p+1} \equiv 1 \ (mod\ p)}$.

L'ordre multiplicatif de α étant $n+1$, il en résulte les relations suivantes :
$n+1 \mid p+1$ ou $n+1 \mid p-1$.
L'entier p, étant un diviseur de n, la deuxième relation est impossible et la première donne : $n+1 = p+1$.

Donc $\boxed{n = p}$ et **n est premier**.

A.3 Preuve du test de Miller-Rabin

On fait une démonstration par l'absurde.
Supposons que l'algorithme réponde qu'un nombre premier est factorisable.
D'après la réponse de l'algorithme, on a :

$$a^t \not\equiv 1 \ (mod\ n).$$

Comme b est élevé au carré à chaque itération de la boucle, alors b devient successivement : $a^t, a^{2t}, a^{2^s t}, \ldots, a^{2^{s-1}t}$.
D'après la réponse de l'algorithme, on a : $a^{2^s t} \not\equiv -1$ (mod n) et ceci $\forall i = 0, \ldots, k-1$.

En utilisant l'hypothèse que n est premier, d'après le théorème de Fermat :
$a^{n-1} \equiv 1$ (mod n) $\Rightarrow a^{2^s t} \equiv 1$(mod n).

$a^{2^{s-1}t}$ est donc une racine carée de 1 modulo n. Comme n est premier, 1 n'admet que 1 et -1 commes racines carrées.

En effet : n|(x-1)(x+1)

n premier $\Rightarrow$ $n|(x-1)$ ou $n|(x+1)$

$\Rightarrow$ $x \equiv 1 \pmod{n}$ ou $x \equiv -1 \pmod{n}$

On a : $a^{2^{s-1}t} \not\equiv -1 \pmod{n}$

Donc : $a^{2^{s-1}t} \equiv 1 \pmod{n}$

$a^{2^{s-2}t}$ doit être une racine carrée de 1 autre que -1, donc $a^{2^{s-2}t} \equiv 1 \pmod{n}$.

En itérant cet argument, on obtient : $a^t \equiv 1 \pmod{n}$ ce qui contredit le fait que l'algorithme ne s'est pas arrêté à l'étape 4.

La probabilité d'erreur de cet algorithme est $\frac{1}{4}$. Sa complexité est de $O((\log n)^3)$.

Annexe B

Fonction indicatrice d'Euler

Le tableau suivant donne les valeurs de $\phi(n)$ pour n$\in [1, 199]$.
L'indice de ligne est le chiffre des dizaines, l'indice de colonne le chiffre des unités (de sorte que l'on lit $\phi(i * 10 + j)$ à l'intersection de la ligne i et de la colonne j).

	0	1	2	3	4	5	6	7	8	9
0	*	1	1	2	2	4	2	6	4	6
1	4	10	4	12	6	8	8	16	6	18
2	8	12	10	22	8	20	12	18	12	28
3	8	30	16	20	16	24	12	36	18	24
4	16	40	12	42	20	24	22	46	16	42
5	20	32	24	52	18	40	24	36	28	58
6	16	60	30	36	32	48	20	66	32	44
7	24	70	24	72	36	40	36	60	24	78
8	32	54	40	82	24	64	42	56	40	88
9	24	72	44	60	46	72	32	96	42	60
10	40	100	32	102	48	48	52	106	36	108
11	40	72	48	112	36	88	56	72	58	96
12	32	110	60	80	60	100	36	126	64	84
13	48	130	40	108	66	72	64	136	44	138
14	48	92	70	120	48	112	72	84	72	148
15	40	150	72	96	60	120	48	156	78	104
16	64	132	54	162	80	80	82	166	48	156
17	64	108	84	172	56	120	80	116	88	178
18	48	180	72	120	88	144	60	160	92	108
19	72	190	64	192	96	96	84	196	60	198

Annexe C

Quelques polynômes cyclotomiques

Voici les 55 premiers polynômes cyclotomiques dans $\mathbb{Q}[X]$:

$\Phi_1(X) = X - 1$
$\Phi_2(X) = X + 1$
$\Phi_3(X) = X^2 + X + 1$
$\Phi_4(X) = X^2 + 1$
$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$
$\Phi_6(X) = X^2 - X + 1$
$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
$\Phi_8(X) = X^4 + 1$
$\Phi_9(X) = X^6 + X^3 + 1$
$\Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1$
$\Phi_{11}(X) = X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
$\Phi_{12}(X) = X^4 - X^2 + 1$
$\Phi_{13}(X) = \sum_{i=0}^{12} X^i$
$\Phi_{14}(X) = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$
$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$
$\Phi_{16}(X) = X^8 + 1$
$\Phi_{17}(X) = \sum_{i=0}^{16} X^i$
$\Phi_{18}(X) = X^6 - X^3 + 1$
$\Phi_{19}(X) = \sum_{i=0}^{18} X^i$
$\Phi_{20}(X) = X^8 - X^6 + X^4 - X^2 + 1$
$\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$
$\Phi_{22}(X) = X^{10} - X^9 + X^8 - X^7 + X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$
$\Phi_{23}(X) = \sum_{i=0}^{22} X^i$
$\Phi_{24}(X) = X^8 - X^4 + 1$
$\Phi_{25}(X) = X^{20} + X^{15} + X^{10} + X^5 + 1$
$\Phi_{26}(X) = X^{12} - X^{11} + X^{10} - X^9 + X^8 - X^7 + X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$
$\Phi_{27}(X) = X^{18} + X^9 + 1$
$\Phi_{28}(X) = X^{12} - X^{10} + X^8 - X^6 + X^4 - X^2 + 1$
$\Phi_{29}(X) = \sum_{i=0}^{28} X^i$
$\Phi_{30}(X) = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1$

$\Phi_{31}(X) = \sum_{i=0}^{30} X^i$
$\Phi_{32}(X) = X^{16} + 1$
$\Phi_{33}(X) =$
$X^{20} - X^{19} + X^{17} - X^{16} + X^{14} - X^{13} + X^{11} - X^{10} + X^9 - X^7 + X^6 - X^4 + X^3 - X + 1$
$\Phi_{34}(X) = X^{16} - X^{15} + X^{14} - X13 + X^{12} - X^{11} + X^{10} - X^9 + X^8 - X^7 + X^6 -$
$X^5 + X^4 - X^3 + X^2 - X + 1$
$\Phi_{35}(X) = X^{24} - X^{23} + X^{19} - X^{18} + X^{17} - X^{16} + X^{14} - X^{13} + X^{12} - X^{11} + X^{10} -$
$X^8 + X^7 - X^6 + X^5 - X + 1$
$\Phi_{36}(X) = X^{12} - X^6 + 1$
$\Phi_{37}(X) = \sum_{i=0}^{36} X^i$
$\Phi_{38}(X) = X^{18} - X^{17} + X^{16} - X^{15} + X^{14} - X^{13} + X^{12} - X^{11} + X^{10} - X^9 + X^8 -$
$X^7 + X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$
$\Phi_{39}(X) = X^{24} - X^{23} + X^{21} - X^{20} + X^{18} - X^{17} + X^{15} - X^{14} + X^{12} - X^{10} + X^9 -$
$X^7 + X^6 - X^4 + X^3 - X + 1$
$\Phi_{40}(X) = X^{16} - X^{12} + X^8 - X^4 + 1$
$\Phi_{41}(X) = \sum_{i=0}^{40} X^i$
$\Phi_{42}(X) = X^{12} + X^{11} - X^9 - X^8 + X^6 - X^4 - X^3 + X + 1$
$\Phi_{43}(X) = \sum_{i=0}^{42} X^i$
$\Phi_{44}(X) = X^{20} - X^{18} + X^{16} - X^{14} + X^{12} - X^{10} + X^8 - X^6 + X^4 - X^2 + 1$
$\Phi_{45}(X) = X^{24} - X^{21} + X^{15} - X^{12} + X^9 - X^3 + 1$
$\Phi_{46}(X) = \sum_{j=0}^{22} (-X)^j$
$\Phi_{47}(X) = \sum_{i=0}^{46} X^i$
$\Phi_{48}(X) = X^{16} - X^8 + 1$
$\Phi_{49}(X) = X^{42} + X^{35} + X^{28} + X^{21} + X^{14} + X^7 + 1$
$\Phi_{50}(X) = X^{20} - X^{15} + X^{10} - X^5 + 1$
$\Phi_{51}(X) = X^{32} - X^{31} + X^{29} - X^{28} + X^{26} - X^{25} + X^{23} - X^{22} + X^{20} - X^{19} + X^{17} -$
$X^{16} + X^{15} - X^{13} + X^{12} - X^{10} + X^9 - X^7 + X^6 - X^4 + X^3 - X + 1$
$\Phi_{52}(X) = X^{24} - X^{22} + X^{20} - X^{18} + X^{16} - X^{14} + X^{12} - X^{10} + X^8 - X^6 + X^4 - X^2 + 1$
$\Phi_{53}(X) = \sum_{i=0}^{52} X^i$
$\Phi_{54}(X) = X^{18} - X^9 + 1$
$\Phi_{55}(X) = X^{40} - X^{39} + X^{35} - X^{34} + X^{30} - X^{28} + X^{25} - X^{23} + X^{20} - X^{17} + X^{15} -$
$X^{12} + X^{10} - X^6 + X^5 - X + 1$

Annexe D

Algorithme d'Euclide étendu

L'algorithme d'Euclide de calcul du PGCD de deux entiers a et b peut être modifié pour calculer un inverse modulaire.
On rappelle que cet algorithme - basé sur l'observation $(a, b) = (b, a \ mod \ b)$ - consiste à itérer cette propriété jusqu'à ce que le reste $a \ mod \ b$ soit nul. Le dernier reste non nul fournit alors le PGCD de a et b.

Soit $d = (a, b)$.
Par l'identité de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$. L'algorithme d'Euclide étendu permet d'obtenir u et v.
Pour trouver l'inverse de b *modulo* n lorsque $(b, n) = 1$, il suffit de l'appliquer avec $a = n$: l'entier v fournit alors l'inverse cherché.

Le principe de l'algorithme est le suivant :
Notons $r_0 = a$, $r_1 = b$. Soit $\{q_j\}_{1 \leq j \leq m}$ la suite de quotients obtenus par l'algorithme d'Euclide, c'est-à-dire :

$$\begin{array}{ccccc} r_0 & = & q_1 r_1 + r_2 \ , & & 0 < r_2 < r_1 \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ r_{m-2} & = & q_{m-1} r_{m-1} + r_m \ , & & 0 < r_m < r_{m-1} \\ r_{m-1} & = & q_m r_m \ , & & 0 < r_m < r_{m-1} \end{array}$$

On a donc $d = r_m$.

Soit $\{t_j\}_{1 \leq j \leq m}$ la suite définie par :

$$\begin{cases} t_0 = 0 \ \ et \ \ t_1 = 1 \\ t_j = t_{j-2} - q_{j-1} t_{j-1} \ \ mod \ r_0 \ , \ 2 \leq j \leq m \end{cases}$$

Alors, on peut montrer par récurrence que les t_j vérifient

$$r_j = t_j r_1 \ \ mod \ r_0 \ , \ 0 \leq j \leq m.$$

Ainsi, $t_m = v$.
Si $a, b \leq n$, on peut vérifier que la complexité de cet algorithme est en $\Theta((log \ n)^2)$.

Bibliographie

[1] Abdelmajid Bayad. Cours de maîtrise mathématiques, corps finis, Avril 2005.

[2] Sabah Al Fakir. *Algèbre et théorie des nombres, Cryptographie, Primalité.* Mathématiques pour le deuxième cycle, 2003.

[3] Ivan Gozard. *Théorie de Galois.* Mathématiques pour le deuxième cycle, 2000.

[4] Françoise Lévy-Dit-Véhel. Cours de cryptographie.

[5] Bruno MARTIN. *Codage, cryptologie et applications.* Presses polytechniques et universitaires normandes, 2004.

[6] Gilles Zémor. *Cours de Cryptographie.* Mathématiques pour le deuxième cycle, 2003.