DUT Informatique, modélisation mathématique, S3, M3202C

Jean-François COUCHOT
jean-francois[point]couchot[arobase]univ-fcomte[point]fr

23 novembre 2016

Chapitre 1

Cryptographie par RSA

1.1 Introduction

La *cryptographie*, où l'art d'écrire avec une clé, est apparue en même temps que l'écriture. Dès qu'une information doit être transmise de manière sure, le message doit être protégé de toute interception : il est crypté par l'émetteur et décrypté par le récepteur. Dans le cas où l'on utilise une clé de cryptage, on a le schéma présenté à la figure 1.1. Dans cette figure, rien ne précise cependant que la clé de cryptage est la même que celle de décryptage. Lorsqu'une

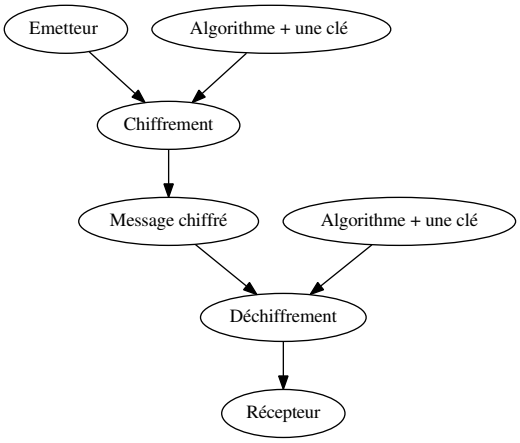

FIGURE 1.1 – Schéma général d'une méthode de cryptage/décryptage

méthode se fondent sur une clé unique pour chiffrer et déchiffrer un message on emploie le terme de cryptographie *symétrique*. Se pose immédiatement le problème de confidentialité de la clé et la mise en œuvre de celle-ci surtout lorsque le nombre de destinataires est grand : il faut une clé pour chacun d'entre eux.

Pour résoudre ce problème d'échange de clés, la cryptographie *asymétrique* a été mise au point dans les années 1970. Elle se base sur le principe d'une clé publique pour le chiffrement et d'une clé privée pour le déchiffrement. Chaque destinataire (receveur) diffuse sa clé publique à quiconque désire chiffrer un message. Le message crypté ne pourra être déchiffré qu'avec la clé privée, qui elle reste confidentielle.

RSA est un algorithme de cette famille. Son étude d'un point de vue mathématique est l'objectif de ce TD. Il s'inspire largement de [CR09]

1.2 Rappels d'arithmétique jusqu'au PGCD

Soit deux entiers a et b dans $\mathbb{Z}$. On dit que a divise b (que l'on note $a|b$) s'il existe un entier $q \in \mathbb{Z}$ tel que $b = aq$.

1.2.1 Calcul de PGCD

Le plus grand diviseur commun (PGCD) de a et b, noté $a \wedge b$ est l'entier naturel qui vérifie
— $a \wedge b | a$ et $a \wedge b | b$;
— Si $d|a$ et $d|b$, alors $d|a \wedge b$.

EXERCICE 1.1. *Déterminer* $550 \wedge 1540$.

1.2.2 Algorithme d'Euclide

Par définition, le PGCD de a non nul avec 0 est a (définition raisonnable, car 0 est divisible par tout entier non nul, donc par a, qui l'est aussi par a) et enfin le PGCD de 0 et de 0 n'est pas défini.

On se limite ici au cas de deux entiers a et b strictement positifs. Supposons par exemple $a > b$

1. La division euclidienne de a par b peut s'écrire $a = bq + r$ avec $0 \leqslant r < b$.
2. Montrons que « d est un diviseur commun à a et b » est équivalent à « d est un diviseur commun à b et r ».
   — Soit d un diviseur commun à a et b, qui peuvent alors s'écrire $a = da'$ et $b = db'$. L'égalité $a = bq + r$ devient $da' = db'q + r$ ou encore $r = d(a' - b'q)$, donc d est aussi un diviseur commun à b et r.
   — Réciproquement, soit d un diviseur commun à b et r, qui peuvent alors s'écrire $b = db'$ et $r = dr'$ et l'égalité $a = bq + r$ devient $a = d(b'q + r')$. Donc d est un diviseur commun à a et b.

   Ainsi, les ensembles des diviseurs communs à a et b d'une part et à b et r d'autre part sont identiques. En particulier $a \wedge b = b \wedge r$.
3. Si $r = 0$ on a $a \wedge b = b \wedge 0$ qui est égal à b.
4. Sinon, r est différent de 0 et on peut donc effectuer la division euclidienne de b par r, qui donne un reste r_1, tel que $0 \leq r_1 < r$ et $b \wedge r = r \wedge r_1$.
5. Cet algorithme est itéré jusqu'à l'obtention d'un reste nul, ce qui se produit obligatoirement puisqu'il s'agit d'entiers et que la suite des restes ainsi construite est strictement décroissante. Le PGCD est alors l'avant-dernier reste (le dernier non nul).

EXERCICE 1.2. *Déterminer* $154 \wedge 35$ *par l'algorithme d'Euclide.*

EXERCICE 1.3. *Donner le code d'un programme qui prend en entrée deux entiers naturels a et b tels que $a > b \geq 0$ et qui retourne leur PGCD*

PROPOSITION 1.1 (IDENTITE DE BÉZOUT). On considère deux nombres entiers strictement positifs a et b. Il existe un couple d'entiers x et y tels que $ax + by = d$, où d est le PGCD de a et de b.

PREUVE. *Dans la preuve de la proposition précédente, on avait successivement*

$$\begin{aligned}
a &= b \times q_1 + r_1 && (1.1)\\
b &= r_1 \times q_2 + r_2 &&\\
r_1 &= r_2 \times q_3 + r_3 &&\\
&\vdots &&\\
r_{n-4} &= r_{n-3} \times q_{n-2} + r_{n-2} && (1.2)\\
r_{n-3} &= r_{n-2} \times q_{n-1} + r_{n-1} && (1.3)\\
r_{n-2} &= r_{n-1} \times q_n + r_n && (1.4)\\
r_{n-1} &= r_n \times q_{n+1} + 0 &&
\end{aligned}$$

On sait que $a \wedge b$ est r_n le dernier reste non nul. On remonte les équations une à une en démarrant de (1.4).

$$\begin{aligned}
r_n &= r_{n-2} - r_{n-1} \times q_n\\
&= r_{n-2} - (r_{n-3} - r_{n-2} \times q_{n-1}) \times q_n \text{ (on remplace } r_{n-1} \text{ par son expression tirée de (1.3))}\\
&= r_{n-2}.(1 + q_{n-1}.q_n) - r_{n-3}.q_n \text{ (factorisation)}\\
&= (r_{n-4} - r_{n-3} \times q_{n-2}).(1 + q_{n-1}.q_n) - r_{n-3}.q_n \text{ (on remplace } r_{n-2} \text{ par son expression tirée de (1.2))}\\
&\vdots\\
&= \ldots \text{ (on remplace } r_1 \text{ par son expression tirée de (1.1))}\\
&= ax + by
\end{aligned}$$

EXERCICE 1.4. *Montrer qu'il existe x et y tels que $29x + 72y = 1$ puis trouver une valeur pour x et y.*

DÉFINITION 1.1 (NOMBRES PREMIERS ENTRE EUX). Les deux entiers relatifs a et b sont premiers entre eux si leur plus grand commun diviseur est égal à 1.

EXERCICE 1.5. *Montrer que 55 et 21 sont premiers entre eux.*

1.3 L'algorithme RSA

1.3.1 Les étapes détaillées de l'algorithme

On rappelle qu'un système cryptographique à clé publique est initialisé par le receveur, c.-à-d. celui qui veut recevoir des messages de manière sure.

Première étape : choix des deux nombres p et q. Le receveur choisit deux grands nombres premiers p et q et calcule $n = pq$. Puis il calcule $\varphi(n)$, où $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est la *fonction d'Euler* L'entier $\varphi(n)$ est le nombre d'entiers dans $\{1, 2, \ldots, n-1\}$ qui sont premiers avec n.

EXERCICE 1.6. *Le receveur choisit $p = 7$, $q = 13$. Construire l'ensemble des entiers qui sont premiers avec $n = pq$ et en déduire que $\varphi(91) = 72$.*

Deuxième étape : choix de la clé publique. Le receveur choisit $e \in \{1, \ldots, \varphi(n) - 1\}$ premier avec $\varphi(n)$. La clé publique est la paire (e, n). Chaque expéditeur va s'en servir pour crypter son message à destination de ce receveur. Le cryptage est détaillé à la quatrième étape ci-dessous.

EXERCICE 1.7. *Montrer que $(29, 91)$ est un candidat acceptable de clé publique.*

Troisième étape : construction de la clé privée. Le receveur calcule l'entier $d \in \{1, \ldots, \varphi(n) - 1\}$ tel que le reste de la division de ed par $\varphi(n)$ est 1. Ceci se note aussi $ed \equiv 1[\varphi(n)]$ qui se lit ed est congru à 1 modulo $\varphi(n)$. La paire (d, n) est la clé privée de décryptage. Elle est secrète et permet au receveur de décrypter tous les messages reçus et cryptés avec (e, n).

EXERCICE 1.8. *Trouver la clé privée associée.*

Quatrième étape : cryptage du message. L'expéditeur peut crypter tout message écrit sous la forme d'un nombre m appartenant à $\{1, \ldots, n-1\}$ et qui est premier avec n. Le message codé est le reste a de la division de m^e par n. On a donc $m^e \equiv a[n]$, où $a \in \{1, \ldots, n-1\}$.

EXERCICE 1.9.
1. *Montrer que l'expéditeur a la possibilité de crypter le message $m = 59$.*
2. *Construire le message crypté a à l'aide de la clé publique.*

Cinquième étape : décryptage du message. Le receveur dispose de a et de sa clé privée (d, n). Pour décrypter a, il calcule le reste dans la division par n de a^d (c.-à-d. $a^d[n]$). Si aucune erreur de calcul n'a été effectuée, c'est le message initial m.

EXERCICE 1.10. *Décrypter le message a à l'aide de la clé privée. Il doit s'agir de m.*

1.3.2 Les points clés

L'algorithme RSA repose sur plusieurs points clés rencontrés successivement :
— la génération de deux grands nombres premiers p et q ;
— la multiplication de grands nombres : pq, ed,
— l'arithmétique modulaire ;
— l'algorithme d'Euclide de génération de PGCD et son corollaire de Bézout ;
— la factorisation, qui tant qu'elle n'est pas réalisable sur des grands nombres, garantit la sécurité du cryptage des données.

1.4 Les incontournables théorèmes de Bézout et de Gauß

PROPOSITION 1.2 (THÉORÈME DE BÉZOUT). Deux entiers strictement positifs a et b sont premiers entre eux, si et seulement s'il existe un couple (x, y) d'entiers relatifs vérifiant $ax + by = 1$.

PREUVE. ***Seulement si.*** *Supposons a et b premiers entre eux. D'après l'identité de Bézout, il existe donc un couple d'entiers x et y tels que $ax + by = 1$, car 1 est le PGCD de a et de b.*

Si. *Supposons qu'il existe un couple (x, y) d'entiers relatifs vérifiant $ax + by = 1$ et $d = a \wedge b$. L'entier d divise les produits ax et by. Donc d divise $ax + by$ et donc d est 1.*

EXERCICE 1.11. *Montrer que les propriétés $a \wedge m = 1$ et $b \wedge m = 1$ impliquent $ab \wedge m = 1$.*

PROPOSITION 1.3 (THÉORÈME DE GAUSS). Soient a, b et c trois entiers naturels. Si a divise le produit bc et s'il est premier avec b, alors il divise c.

EXERCICE 1.12. *L'objectif est de résoudre l'équation (E) $405x - 120y = 15$ d'inconnues x et y.*

1. *Trouver le PGCD de 405 et 120 à l'aide de l'algorithme d'Euclide.*
2. *En déduire une solution particulière de cette équation.*
3. *En utilisant la solution particulière, montrer que (E) est équivalente à $27(x - 3) = 8(y - 10)$.*
4. *Utiliser le théorème de Gauß pour montrer que l'ensemble des solutions de (E) est $\{(8k+3; 27k+10) | k \in \mathbb{Z}\}$.*

EXERCICE 1.13. *Faire la preuve du théorème de Gauß.*

PROPOSITION 1.4 (FONCTION D'EULER). Si p et q sont deux nombres premiers distincts alors l'égalité suivante permet de trouver le valeur de la fonction d'Euler en un seul produit :

$$\varphi(pq) = (p - 1)(q - 1). \tag{1.5}$$

EXERCICE 1.14 (PREUVE DE L'EXPRESSION D'EULER). *On doit compter le cardinal des nombres de $\{1, 2, ..., pq-1\}$ qui sont premiers avec pq.*

1. *Construire l'ensemble P des entiers naturels multiples de p inférieurs à $pq - 1$. Combien en a-t-on ?*
2. *Construire l'ensemble Q des entiers naturels multiples de q inférieurs à $pq - 1$. Combien en a-t-on ?*
3. *Supposons qu'un élément k appartienne à la fois à P et à Q. Montrer que cela implique qu'il existe deux entiers naturels m_1, $1 \leq m_1 \leq q - 1$, et m_2, $1 \leq m_2 \leq p - 1$ tels que $m_1.p = m_2.q$.*
4. *En utilisant le théorème de Gauß, montrer que cela est absurde.*
5. *En déduire l'équation (1.5).*

EXERCICE 1.15. *Soit p un nombre premier.*

1. *Calculer $\varphi(p^2)$.*
2. *Est-ce que RSA fonctionnerait aussi avec l'entier $n = p^2$ à la place de $n = pq$?*

1.5 Congruence modulo

DÉFINITION 1.2 (CONGRUENCE MODULO). Soit a et b deux entiers relatifs. On dit que a est congru b modulo n si n divise $a-b$, c'est-à-dire s'il existe $x \in \mathbb{Z}$ tel que $(a-b) = nx$. On note $a \equiv b[n]$. La relation « $\equiv [n]$ » est une relation d'équivalence appelée congruence modulo n.

PROPOSITION 1.5. Soit a, b, c, d, x et y dans $\mathbb{Z}$. Si $a \equiv c[n]$ et $b \equiv d[n]$, alors

1. $a+b \equiv c+d[n]$;
2. $ab \equiv cd[n]$;
3. $ax+by \equiv cx+dy[n]$.

EXERCICE 1.16. *Démontrer la proposition précédente.*

PROPOSITION 1.6. Soit deux entiers naturels a et n tels que $1 < a < n$. Si a et n sont premier entre eux, alors il existe un unique $x \in \{1, \ldots, n-1\}$ tel que $ax \equiv 1[n]$.

PREUVE. ***Existence.*** *Comme a et n sont premiers entre eux, d'après le théorème de Bézout, il existe x et y entiers tels que $ax+ny=1$, soit encore $ax \equiv 1[n]$.*

Unicité. *Supposons qu'il existe une seconde solution $x' \in \{1, \ldots, n-1\}$ telle que $ax' \equiv 1[n]$. Donc $a(x-x') \equiv 0[n]$. Or n est premier avec a. D'après le théorème de Gauß, n divise donc $x-x'$. Or $x-x' \in \{-n+2, -n+3, \ldots, -1, 0, 1, \ldots, n-2\}$. Le seul nombre divisible par n est 0 et donc $x = x'$.*

EXEMPLE 1.1. *Trouvons les nombres x tels que $7x+11$ soit multiple de 36. Dit autrement, résoudre l'équation $7x \equiv -11[36]$.*

On cherche un « inverse » de 7 c.-à-d. un nombre t, $1 < t < 35$ tel que $7t \equiv 1[36]$. Soit à résoudre $7t \equiv 1[36]$ qui revient à trouver t et u tels que $7t - 36u = 1$, soit encore les coefficient de Bézout relatifs à (7 et 36). On trouve successivement

$$\begin{aligned} 36 &= 7 \times 5 + 1 \\ 7 &= 7 \times 1 + 0 \\ &\textit{et donc} \\ 1 &= 36 - 7 \times 5 \end{aligned}$$

et donc $t = -5$ (et $u = -1$). On en déduit $7x \equiv -11[36]$ est équivalent à $(-5).7x \equiv (-5).-11[36]$ soit encore $x \equiv 55[36] \equiv 19[36]$.

EXERCICE 1.17. *Trouver les entiers relatif x tels que $261x+2$ soit multiple de 305.*

EXERCICE 1.18.

1. *Démonter que $3^5 \equiv 1[11]$*
2. *En déduire que pour tous entiers naturels k et r on a $3^{5k+r} \equiv 3^r[11]$.*
3. *n étant un entier naturel, quels sont les restes possibles dans la division de 3^n par 11 ?*
4. *Trouvez pour quelles valeurs de n, 3^n+7 est divisible par 11.*

EXERCICE 1.19. *On se place dans le contexte de cryptographie par RSA. Démontrer que si la clé d'encryptage est $e < \varphi(n)$, alors il existe une unique clé de décodage entre 1 et $\varphi(n)$.*

PROPOSITION 1.7 (THÉORÈME D'EULER). Soit $n \in \mathbb{N}^*$ et m, $m < n$ un entier relativement premier avec n. Alors

$$m^{\varphi(n)} \equiv 1[n]. \tag{1.6}$$

On laisse de côté la démonstration.

PROPOSITION 1.8 (CORRECTION DE RSA). Le cryptage-décryptage du code RSA est correct : on crypte un message m tel que $m \wedge n = 1$ en a avec $m^e \equiv a[n]$ selon la clé (e, n). Alors le décryptage selon la clé (d, n) redonne le message initial : $a^d \equiv m[n]$.

PREUVE.

$$\begin{aligned} a^d &\equiv (m^e)^d[n] \\ &\equiv m^{ed}[n] \text{ (réécriture)} \\ &\equiv m^{k.\varphi(n)+1}[n] \text{ (définition de } d\text{)} \\ &\equiv m^{k.\varphi(n)}m[n] \text{ (réécriture)} \\ &\equiv (m^{\varphi(n)})^k m[n] \text{ (réécriture)} \\ &\equiv (1)^k m[n] \text{ (théorème d'Euler)} \\ &\equiv m[n] \text{ (réécriture)} \end{aligned}$$

EXERCICE 1.20. *On considère l'algorithme suivant : on choisit deux nombres premiers p et q distincts tels que $p \equiv 2[3]$ et $q \equiv 2[3]$. Soit $n = pq$. Alice veut envoyer un message à Bob. Comme dans RSA, son message est un nombre $m \in \{1, ..., n-1\}$ tel que $m \wedge n = 1$ Le message codé d'Alice est le résultat $a = m^3[n]$. Bob décode a en calculant*

$$m' \equiv a^d[n] \text{ où } d = \frac{2(p-1)(q-1)+1}{3}$$

Normalement m doit être égal à m'.

1. *Choisir $p = 11$, $q = 5$, $m = 4$ puis construire le message codé ainsi que le message décodé.*
2. *Montrer que d est toujours un entier.*
3. *Expliquer pourquoi a et m' ne sont pas divisibles par n.*
4. *Montrer que Bob a bien décodé le message d'Alice.*

PROPOSITION 1.9 (PETIT THÉORÈME DE FERMAT). Si p est un nombre premier et a un entier alors $a^p \equiv a[p]$.

PREUVE. *La preuve se fait par récurrence sur a.*

— *Pour $a = 0$, c'est trivial.*

— *Supposons la formule établie pour $k = a$ et montrons qu'elle l'est aussi pour $k = a + 1$. On remarque tout d'abord que pour chaque k, $0 < k < p$, le coefficient binomial $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ est divisible par p, c.-à-d. $\binom{p}{k} \equiv 0[p]$. On a alors successivement :*

$$\begin{aligned} (k+1)^p &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a^1 + 1 \\ &\equiv a^p + 1[p] \text{ (d'après la remarque sur les coeff. binomiaux)} \\ &\equiv a + 1[p] \text{ (par hypothèse de récurrence).} \end{aligned}$$

EXERCICE 1.21. *Soit p un nombre premier tel que $p \equiv 3[4]$. Soit a un entier qui est un carré, modulo p : il existe b tel que $a \equiv b^2[p]$. Montrer que $a^{(p+1)/4}$ est une racine carré de a, modulo p.*

PROPOSITION 1.10 (AUTRE FORMULATION DU PETIT THÉORÈME DE FERMAT). Si p est un nombre premier et a un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p.

PREUVE. *Supposons établi le petit théorème de Fermat c'est-à-dire* $a^p \equiv a[p]$. *Ainsi* p *divise* $a^p - a = a(a^{p-1} - 1)$. *Si* p *ne divise pas* a, *d'après le théorème de Gauß,* p *divise* $a^{p-1} - 1$.

Réciproquement, écrivons $a^p - a = a(a^{p-1} - 1)$. *Si* p *divise* a, *alors* p *divise* $a^p - a$. *Sinon,* p *ne divise pas* a *et d'après cette autre formulation,* p *divise* $a^{p-1} - 1$. *Finalement,* p *divise encore* $a^p - a$.

EXERCICE 1.22 (SUJET DU BAC S LIBAN 2005).

1. *On considère l'équation* (E) *:* $109x - 226y = 1$ *où* x *et* y *sont des entiers relatifs.*
   (a) *Déterminer* $109 \wedge 226$. *Que peut-on en conclure pour l'équation* (E) *?*
   (b) *Montrer que l'ensemble des solutions de* (E) *est l'ensemble des couples de la forme* $(141 + 226k; 68 + 109k)$, *où* k *appartient à* $\mathbb{Z}$. *En déduire qu'il existe un unique entier naturel non nul* d *inférieur ou égal à 226 et un unique entier naturel non nul* e *tels que* $109d = 1 + 226e$ *(on précisera les valeurs des entiers* d *et* e*).*
2. *Démontrer que 227 est un nombre premier.*
3. *On note* $A = \{0, 1, 2, \ldots, 226\}$. *On considère les deux fonctions* f *et* g *de* A *dans* A *définies de la manière suivante :*
   — *A tout entier* $a \in A$, f *associe le reste de la division euclidienne de* a^{109} *par 227.*
   — *A tout entier* $a \in A$, g *associe le reste de la division euclidienne de* a^{141} *par 227.*
   (a) *Vérifier que* $g(f(0)) = 0$.
   (b) *Montrer que, quel que soit l'entier non nul* a *de* A , $a^{226} - 1$ *est multiple de 227.*
   (c) *En déduire que, quel que soit l'entier non nul* a *de* A, $g(f(a)) = a$. *Que peut-on dire de* $f(g(a)) = a$ *?*

1.5.1 Puissance de grands nombres

EXEMPLE 1.2. *Calculons* $666^{999}[13]$. *On a successivement :*

$$\begin{aligned} 666^{999} &\equiv (13 \times 51 + 3)^{999}[13] \\ &\equiv 3^{999}[13] \\ &\equiv 3^{12\times 83+3}[13] \\ &\equiv 3^3 \times (3^{12})^{83}[13] \\ &\equiv 3^3 \times (1)^{83}[13] \text{(car } 3^{12} \equiv 1[13] \text{ d'après le petit théorème de Fermat)} \\ &\equiv 27[13] \\ &\equiv 1[13] \end{aligned}$$

EXERCICE 1.23. *Calculer* $2^{500}[13]$ *et* $26^{1000}[17]$.

1.6 Génération de grands nombres premiers

Dans ce qui suit, on nomme $\mathbb{P}$ l'ensemble des nombres premiers. Depuis Euclide, on sait que $\mathbb{P}$ est de taille infinie. Fermat avait cru donner une formule ne générant que des nombres premiers. Il affirmait que pour tout $n \in \mathbb{N}$, le nombre

$$F_n = 2^{2^n} + 1 \tag{1.7}$$

était premier. Or 641 divise F_5. Aujourd'hui, on pense que seuls les nombres de F_0 à F_4 sont premiers.

1.6.1 Distribution des nombres premiers parmi les entiers

Même si on ne connaît pas de formule permettant de construire tous les nombres premiers, tout n'est pas perdu puisque les nombres premiers ne sont pas si rares que cela. Le théorème suivant donne même la proportion approximative des entiers inférieurs ou égaux à N qui sont premiers.

PROPOSITION 1.11 (THÉORÈME DES NOMBRES PREMIERS). La fonction $\pi : \mathbb{N} \to \mathbb{N}$ associe à chaque nombre N le nombre d'entiers inférieurs ou égaux à N qui sont premiers, soit $\pi(N) = |\{p \leq N | p \text{ premier}\}|$. Lorsque N est grand, on a :

$$\pi(N) \approx \frac{N}{\ln(N)} \tag{1.8}$$

La preuve de ce théorème est d'un niveau très avancé et n'est pas reproduite ici.

Pour obtenir un entier de 100 chiffres, il suffit de considérer $N = 10^{100}$. Si on choisit au hasard un nombre dans $\mathbb{N}_N^*$, la probabilité qu'il soit premier est :

$$\begin{aligned} \text{Prob}(n \text{ premier}) &\approx \frac{\frac{N}{\ln(N)}}{N} \\ &\approx \frac{1}{\ln(N)} \end{aligned}$$

Le tableau 1.1 donne une valeur approchée de cette probabilité pour quelques nombres de chiffres. Dans celui-ci :

— la seconde ligne n'impose aucune restriction sur le dernier chiffre ;

— la troisième ligne impose que le dernier chiffre soit dans $\{1, 3, 5, 7, 9\}$: il est inutile de vérifier que les multiples de 2 sont premiers !

— la quatrième ligne impose que le dernier chiffre soit dans $\{1, 3, 7, 9\}$: les multiples de 5 ne sont pas premiers !

On constate que si l'on tire au hasard un nombre (même de 100 chiffres), parmi ceux qui se terminent par $\{1, 3, 7, 9\}$ (ensemble noté B par la suite) la probabilité qu'il soit premier n'est pas infime. La solution au problème de génération de nombres premiers repose sur la capacité ou non a disposer d'un test efficace de primalité pour des grands nombres.

Nombre de chiffres	**75**	**100**	**125**	**150**	**175**	**200**	**225**	**250**	**275**	**300**
Dernier chiffre quelconque	172	230	287	345	402	460	518	575	633	690
Dernier chiffre impair	86	115	143	172	201	230	259	287	316	345
Dernier chiffre dans $\{1, 3, 7, 9\}$	69	92	115	138	161	184	207	230	253	276

TABLE 1.1 – Probabilités inverse d'obtenir un nombre premier

On considère comme expérience aléatoire le fait de tirer un nombre au hasard dans B. On a une probabilité p que le nombre soit premier. Soit X la variable aléatoire qui compte le nombre de fois où l'on a réalisé cette expérience avant d'obtenir un nombre premier. X suit une loi géométrique de paramètre p :

$$P(X = k) = (1 - p)^{k-1} p.$$

Or l'espérance d'une variable aléatoire suivant une loi géométrique de paramètre p est $\frac{1}{p}$. Pour 100 chiffres, il faudra en moyenne 92 tirages pour générer un nombre premier.

Il « reste » à fournir une méthode efficace pour décider de la primalité d'un entier, ce que présente la section suivante.

1.6.2 Tests de primalité

Chaque section donne un algorithme permettant de décider si un entier p fourni en entrée est premier ou non.

1.6.2.1 Méthode naïve

On vérifie s'il est divisible par l'un des entiers pairs compris entre 2 et $\sqrt{p}$. Si la réponse est négative, alors p est premier, sinon il est composé. Pour améliorer la performance de cette méthode, on peut calculer à l'avance une liste des nombres premiers inférieurs à $\sqrt{p}$ (avec un crible d'Ératosthène), pour ne tester que ceux-ci.

Par exemple, pour tester un nombre inférieur à 39 000, il suffit de vérifier qu'il n'est pas multiple d'un nombre premiers inférieur à 198 (car $198^2 = 39204$) ; on doit faire au maximum 45 divisions.

1.6.2.2 Tests probabilistes

Test de Fermat. Le petit théorème de Fermat est une implication et non pas une équivalence :

— si on prend un $p \in \mathbb{N}$ et un $a \in \mathbb{N}$ quelconque, alors si p est premier et a non divisible par p, alors on peut en déduire que $a^{p-1} \equiv 1[p]$;

— rien ne dit que si on a $a^{p-1} \equiv 1[p]$, alors p est premier et a non divisible par p.

— rien ne dit non plus que que si on a $a^{p-1} \equiv 1[p]$ et que a non divisible par p, alors p est premier.

Cependant si on effectue un grand nombre de fois l'expérience de choisir $a \in \mathbb{N}^*_{n-1}$ et qu'à chaque fois on établit $a^{p-1} \equiv 1[p]$, alors p est probablement premier. Cependant ce n'est pas toujours le cas : par exemple $2^{340} \equiv 1[341]$ et pourtant $341 = 11 \times 31$.

EXERCICE 1.24. *Donner le code de la fonction* `testPrimaliteFermat(n,t)` *qui retourne* `True` *si* `t` *evaluations de* a^{n-1} *ont retourné* $1[n]$ *pour un* $a \in \mathbb{N}^*_{n-1}$ *et* `False` *sinon.*

Test de Miller-Rabin Soit n un nombre premier impair, alors nous pouvons écrire $n-1$ comme $2^s \times d$, où s est un entier et d est impair. Alors, pour tout entier naturel $a \in \mathbb{N}^*_{n-1}$ tel que a est premier avec n, une des conditions suivantes doit être vérifiée :

1. $a^d \equiv 1[n]$, ou bien
2. $a^{2^r \cdot d} \equiv -1[n]$ pour un certain $0 \leq r \leq s-1$.

La preuve de cette propriété est admise

Le test de primalité de Miller-Rabin est basé sur les équations précédentes. Si on choisit un grand nombre t de fois $a \in \mathbb{N}^*_{n-1}$ et qu'on obtienne à chaque fois

— $a^d \equiv 1[n]$ ou

— $a^{2^r \cdot d} \equiv -1[n]$ pour un certain $0 \leq r \leq s-1$,

alors le nombre n est probablement premier. Dans le cas contraire ($a^d \not\equiv 1[n]$ et $a^{2^r \cdot d} \not\equiv -1[n]$ pour tous les $0 \leq r \leq s-1$), n n'est pas premier.

EXERCICE 1.25. *Donner le code de la fonction* `testPrimaliteMillerRabin(n,t)`.

1.7 Factorisation

L'objectif de cette partie est de montrer qu'on peut factoriser n sous la forme de $p \times q$ si ces deux derniers nombres ont été mal choisis.

EXERCICE 1.26. *On considère que l'étape 1 de l'algorithme RSA a généré deux nombre premiers p et q proches tels que $p > q$. On définit $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$. Montrer que*

1. *le produit $n = pq = t^2 - s^2$;*
2. *l'entier t est légèrement supérieur à la racine carrée de n et que s est petit ;*
3. *l'on peut utiliser ces informations pour factoriser n c.-à-d. retrouver p et q ;*
4. *Factoriser 896861 et 318040531.*
5. *Factoriser 9623827 et 343570291.*

TRAVAUX PRATIQUES 1.1. *L'objectif de ce TP est d'implanter toute la démarche RSA avec les éléments vus en TD. Tout ceci est à synthétiser dans un document libreoffice à renvoyer à l'adresse* `couchot@femto-st.fr` *avec pour sujet* `RSA-NOM1-NOM2-TDX`.

1. *Quel est le plus petit nombre à trois chiffres ? Quel est le plus grand nombre à trois chiffres ? Comment générer aléatoirement un nombre qui a trois chiffres en utilisant* `randint` *?*
2. *Même question que la question précédente, en remplaçant « trois » par M.*
3. *On a vu qu'un nombre se terminant par 0,2,4,5,6,8 n'est jamais premier. Comment générer un nombre qui a N chiffres, dont le dernier chiffre n'est pas dans la liste précédente.*
4. *Pour affirmer qu'un nombre de 100 chiffres est premier, on invoquera le test de Miller-Rabin avec 50 valeurs testées différentes a. Si toutes retournent qu'il est probablement premier, on considérera qu'il l'est. Construire la fonction* `genereUnNombrePremier(N)` *qui retourne un nombre probablement premier selon cette méthode.*

5. *A l'aide de l'agorithme précédent, générer deux nombres premiers p et q de 100 chiffres. Calculer $n = pq$ puis* `phi` *telle que* `phi=(p-1)*(q-1)`.
6. *Contruire la partie e de la clé publique (e, n) comme un nombre premier de trente chiffres par exemple. Si elle est première avec* `phi`*, c'est une bonne clé, sinon on regénere un nombre premier de trente chiffres.*
7. *Donner le code la fonction* `bezout(a,b)` *qui retourne x et y tels que $x.a + y.b = a \wedge b$.*
   Se servir de cette fonction pour générer la partie d de la clé privée (d, n). Attention, faire en sorte que $0 \leq d \leq$`phi`.
8. *Chiffrer à l'aide de la clé publique (e, n) le message $m = 3402752281514000316845$ qui est un numéro de carte bancaire comprenant les 16 chiffres, la date de validité et le code de sécurité. Le mesage chiffré est a.*
9. *Déchiffrer a à l'aide de la clé privée. Vérifier que vous obtenez bien m à nouveau.*

Bibliographie

[CR09] Yvan Saint-Aubin Christiane Rousseau. La cryptographie à cle publique : le code rsa (1978). In *Mathématiques et Technologie*, Springer Undergraduate Texts in Mathematics and Technology, pages 213–244. Springer New York, 2009.