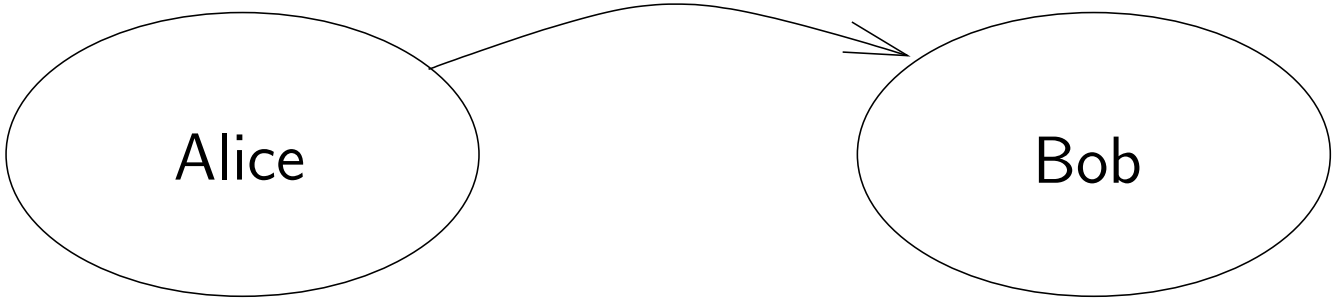
Code de Turing (version 1)



Principes :

- Soit m le message qu'Alice doit envoyer à Bob. Le message m doit être encodé sous la forme d'un nombre premier.
  Exemple d'encodage : A=01, B=02, C=03, ...

v	i	c	t	o	r	y	
22	09	03	20	15	18	25	13

- Alice et Bob ont en commun une *clé secrète*, qui est un grand nombre premier p.
- Alice crypte le message m en calculant

$$m' = mp,$$

  et l'envoie à Bob.
- Bob décrypte m' en calculant

$$\frac{m'}{p} = \frac{mp}{p} = m.$$

Exemple : Supposons que la clé secrète soit le nombre premier 22801763489 et que le message à envoyer soit "victory". Le message crypté est

$$\begin{aligned} m' &= mp \\ &= 2209032015182513 \cdot 22801763489 \\ &= 50369825549820718594667857. \end{aligned}$$

Problème : Comment peut-on s'assurer que m et p soient des nombres premiers ?

Solution : Il existe des algorithmes permettant de tester si un nombre est premier. Notamment, un algorithme de Agrawal, Kayal et Saxena (2002) permet de tester si n est premier en approximativement $(\log n)^{12}$ étapes.

Question : Le code de Turing est-il sécurisé ?

Réponse : Si $m' = mp$ est intercepté, il faut le factoriser pour trouver m. La factorisation étant un problème difficile, il est très difficile de trouver m (et p), pour autant qu'ils soient suffisamment grands.

Problème : Il reste tout de même un défaut de conception majeur dans le code de Turing.

Cassage du code de Turing

- Si les messages m_1 et m_2 doivent être envoyés grâce à la clé secrète p, Alice calcule les messages cryptés $m'_1 = m_1 p$ et $m'_2 = m_2 p$, et les envoie à Bob.
- Si m'_1 et m'_2 sont interceptés, la clé p peut être calculée par $\text{pgcd}(m'_1, m'_2)$, et les messages m_1 et m_2 peuvent alors être retrouvés par $m_1 = \dfrac{m'_1}{p}$ et $m_2 = \dfrac{m'_2}{p}$.

Arithmétique modulaire

Définition : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}_0$. On dit que *a et b sont congrus modulo c* si $c \mid (a - b)$. On note cela $a \equiv b \pmod{c}$.

Exemples :

- $29 \equiv 15 \pmod{7}$ car $7 \mid (29 - 15)$.
-

$\#$:	$\ldots$	-4	-3	-2	-1	0	1	2	3	4	5	$\ldots$
$\#$ mod 3 :	$\ldots$	2	0	1	2	0	1	2	0	1	2	$\ldots$

- Définit une partition des entiers en n ensembles :

$$\begin{array}{lllllllll} \{ & \ldots, & -6, & -3, & 0, & 3, & 6, & 9, & \ldots \} \\ \{ & \ldots, & -5, & -2, & 1, & 4, & 7, & 10, & \ldots \} \\ \{ & \ldots, & -4, & -1, & 2, & 5, & 8, & 11, & \ldots \} \end{array}$$

Lemme : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}_0$. On a

$$a \equiv b \pmod{c} \Leftrightarrow (a \bmod c) = (b \bmod c).$$

Démonstration :

- Par le théorème de division euclidienne, il existe des uniques paires $(q_1, r_1), (q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}$ telles que
  - $a = q_1 c + r_1$ (avec $0 \leq r_1 < c$) (1)
  - $b = q_2 c + r_2$ (avec $0 \leq r_2 < c$) (2)
- En soustrayant (2) de (1), on obtient $a - b = (q_1 - q_2)c + (r_1 - r_2)$, avec $-c < r_1 - r_2 < c$.
- Comme $-c < r_1 - r_2 < c$, on a

$$\begin{aligned} a \equiv b \pmod{c} &\Leftrightarrow c \mid (a - b) \\ &\Leftrightarrow c \mid (r_1 - r_2) \\ &\Leftrightarrow r_1 = r_2. \end{aligned}$$

- On conclut grâce à $(a \bmod c) = r_1$ et $(b \bmod c) = r_2$.

□

Remarque : Plusieurs propriétés de l'arithmétique sur les entiers sont valables en arithmétique modulaire, mais ce n'est pas toujours le cas.

Exemples :

- Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}_0$.
  - $a \equiv b \pmod{n}$ implique $a + c \equiv b + c \pmod{n}$.
  - $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ implique $a \equiv c \pmod{n}$.
- En arithmétique, $ac = bc$ implique $a = b$ (si $c \neq 0$). Ce n'est pas le cas en arithmétique modulaire : $2 \cdot 3 \equiv 4 \cdot 3 \pmod{6}$ mais $2 \not\equiv 4 \pmod{6}$.

Propriétés de l'arithmétique modulaire

Soient $k, n \in \mathbb{N}_0$, et $a, a_1, b_1, a_2, b_2, \ldots, a_k, b_k \in \mathbb{Z}$.

Propriété : Si $a_1 \equiv b_1 \pmod{n}$ et si $a_2 \equiv b_2 \pmod{n}$, alors

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$,
2. $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Démonstration de 2 :
On a $n \mid (a_1 - b_1)$ et $n \mid (a_2 - b_2)$. Par la propriété du transparent 64, on obtient

$$n \mid (a_2(a_1 - b_1) + b_1(a_2 - b_2)),$$

ce qui se simplifie en $n \mid (a_1 a_2 - b_1 b_2)$. □

Propriété : Si pour tout i tel que $1 \leq i \leq k$ on a $a_i \equiv b_i \pmod{n}$, alors $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{n}$.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(k) =$ "Si pour tout i tel que $1 \leq i \leq k$ on a $a_i \equiv b_i \pmod{n}$, alors $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{n}$".
- *Cas de base :* $P(1)$ est vrai.
- *Cas inductif :*
  - Supposons que $P(k)$ soit vrai.
  - Supposons que pour tout i tel que $1 \leq i \leq k+1$ on ait $a_i \equiv b_i \pmod{n}$.
  - On a $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{n}$.
  - Comme $a_{k+1} \equiv b_{k+1} \pmod{n}$, $P(k+1)$ est vrai grâce à la propriété précédente.
- Par induction, $P(k)$ est vrai pour tout $k \in \mathbb{N}_0$. □

Propriété : $(a \bmod n) \equiv a \pmod{n}$.

Démonstration : $a \bmod n$ est égal à $a - qn$ pour un certain quotient $q \in \mathbb{Z}$. On a successivement

$$\begin{aligned} n \mid qn &\Rightarrow n \mid (a - (a - qn)) \\ &\Rightarrow n \mid (a - (a \bmod n)) \\ &\Rightarrow (a \bmod n) \equiv a \pmod{n}. \end{aligned}$$

□

Propriété : $\prod_{i=1}^{k} (a_i \bmod n) \equiv \prod_{i=1}^{k} a_i \pmod{n}$.

Démonstration : Pour tout i tel que $1 \leq i \leq k$, on a $(a_i \bmod n) \equiv a_i \pmod{n}$ grâce à la propriété précédente. La conclusion découle de la propriété du transparent 96. □

Code de Turing (version 2)

Principes :

- Alice et Bob ont en commun
  - un grand nombre premier p, qui peut être public, et
  - une clé secrète $k \in \{1, 2, \ldots, p-1\}$.
- Le message m est supposé être un nombre de l'ensemble $\{1, 2, \ldots, p-1\}$. Alice l'encrypte en calculant

$$m' = mk \bmod p, \qquad (*)$$

  et l'envoie à Bob.
- Bob décrypte m' en trouvant un message m qui respecte l'égalité $(*)$.

Problèmes : Comment effectuer l'opération de décryptage ?

Simplification modulo un nombre premier

Lemme : Supposons que p soit un nombre premier et que k ne soit pas un multiple de p. Si

$$ak \equiv bk \pmod{p},$$

alors

$$a \equiv b \pmod{p}.$$

Démonstration :

- Si $ak \equiv bk \pmod{p}$, alors $p \mid (ak - bk)$. On a donc $p \mid k(a - b)$.
- Donc, $p \mid k$ ou $p \mid (a - b)$.
- Comme k n'est pas un multiple de p, on a $p \mid (a - b)$, ce qui implique $a \equiv b \pmod{p}$. □

Messages cryptés identiques

- Soient a, b deux messages.
- Les messages encryptés sont identiques si et seulement si $(ak \bmod p) = (bk \bmod p)$, c'est-à-dire si $ak \equiv bk \pmod{p}$.
- Comme k n'est pas un multiple de p ($k \in \{1, 2, \ldots, p-1\}$), cela se produit exactement lorsque $a \equiv b \pmod{p}$.
- Comme $a, b \in \{1, 2, \ldots, p-1\}$, cela signifie $a = b$.

Conclusion : Deux messages cryptés représentent le même message non-crypté si et seulement s'ils sont identiques.

Corollaire : Supposons que p soit un nombre premier et que k ne soit pas multiple de p. La séquence

$$(0k) \bmod p,\ (1k) \bmod p,\ (2k) \bmod p,\ \ldots,\ ((p-1)k) \bmod p$$

est une permutation de la séquence

$$0,\ 1,\ 2,\ \ldots,\ p-1.$$

Démonstration :

- Chacun des p nombres de la première séquence appartient à $\{0, 1, \ldots, p-1\}$.
- Par le lemme précédent, et comme $(ak \bmod p) = (bk \bmod p) \Leftrightarrow ak \equiv bk \pmod p$, la première séquence contient tous les nombres de 0 à $p-1$ dans un ordre donné. □

Inverses multiplicatifs

Tout $x \in \mathbb{R}_0$ admet un inverse multiplicatif x^{-1} tel que $x \cdot x^{-1} = 1$.

Cependant, la plupart des nombres entiers n'admettent pas d'inverses multiplicatifs dans $\mathbb{Z}$ (seul 1 et -1 ont un inverse).

Exemple : L'inverse multiplicatif de 5 est $\frac{1}{5}$, qui n'est pas entier.

Dans une arithmétique modulo un nombre premier p, la plupart des entiers admettent un inverse multiplicatif.

Exemple : $5 \cdot 9 \equiv 1 \pmod{11}$.

Théorème : Soit p un nombre premier. Si $k \in \mathbb{Z}$ n'est pas un multiple de p, alors il existe $k^{-1} \in \{1, 2, \ldots, p-1\}$ tel que $k \cdot k^{-1} \equiv 1 \pmod{p}$.

Démonstration :

- Lorsque m varie dans $\{1, 2, \ldots, p-1\}$, l'expression ($mk \bmod p$) prend toutes les valeurs de $\{1, 2, \ldots, p-1\}$.
- En particulier, ($mk \bmod p$) $= 1$ pour un m donné, et donc $\underbrace{m}_{k^{-1}} k \equiv 1 \pmod{p}$. □

Application : Pour décoder un message crypté m' obtenu à partir d'un message m par le code Turing (version 2) en utilisant la clé secrète k, il suffit de multiplier m' par k^{-1}. En effet,

$$\begin{aligned} m'k^{-1} \bmod p &\equiv m'k^{-1} \pmod{p} \\ &\equiv (mk \bmod p)k^{-1} \pmod{p} \\ &\equiv mkk^{-1} \pmod{p} \\ &\equiv m \pmod{p}. \end{aligned}$$

Calcul d'inverses

Autre démonstration du théorème du transparent 103 :

- Puisque p est premier, il a seulement deux diviseurs : 1 et p. Puisque k n'est pas un multiple de p, on doit avoir $\text{pgcd}(k, p) = 1$.
- Par la caractérisation du pgcd, on sait qu'il existe s, t tels que $\text{pgcd}(k, p) = 1 = sk + tp$.
- Dès lors, on a $tp = 1 - sk$, ce qui implique $p|(1 - sk)$.
- Par la définition de la congruence, on en déduit $\underbrace{s}_{k^{-1}} k \equiv 1 \pmod{p}$. □

Calcul d'inverses avec le pulvérisateur

Par la démonstration précédente, on peut donc obtenir un inverse multiplicatif s de $k \pmod p$ en utilisant le pulvérisateur pour calculer une décomposition $\text{pgcd}(k, p) = sk + tp$. L'algorithme demande $O(\log(p))$ opérations.

Exemple : $p = 17$ et $k = 6$

a	b	$a \bmod b$	$=$	$a - q \cdot b$
17	6	5	$=$	$17 - 2 \cdot 6$
6	5	1	$=$	$6 - 1 \cdot 5$
			$=$	$6 - 1 \cdot (17 - 2 \cdot 6)$
			$=$	$-1 \cdot 17 + \boxed{3} \cdot 6$

$\Rightarrow$ l'inverse multiplicatif de $6 \pmod{17}$ est 3 :

$$3.6 \equiv 1 \pmod{17}.$$

Théorème de Fermat

(Petit) Théorème de Fermat : Supposons que p soit un nombre premier et que k ne soit pas un multiple de p. Alors, $k^{p-1} \equiv 1 \pmod{p}$.

Démonstration :

$$\begin{aligned} & 1 \cdot 2 \cdots (p-1) \\ \equiv\ & (k \bmod p) \cdot (2k \bmod p) \cdots ((p-1)k \bmod p) \pmod{p} \\ \equiv\ & k \cdot 2k \cdots ((p-1)k) \pmod{p} \\ \equiv\ & (p-1)! \cdot k^{p-1} \pmod{p}. \end{aligned}$$

$(p-1)!$ n'est pas un multiple de p car p est premier et ne divise ni 1, ni 2, ..., ni $p-1$. Donc, on peut simplifier par $(p-1)!$. □

Calcul d'inverses avec le théorème de Fermat

Supposons que p soit un nombre premier et que k ne soit pas un multiple de p.

Par le théorème de Fermat, on a $k^{p-2}k \equiv 1 \pmod{p}$. Le nombre k^{p-2} est donc un inverse multiplicatif de k.

Exemple de calcul (logarithmique en temps) : Si l'on veut calculer l'inverse multiplicatif de 6 modulo 17, il suffit de calculer $6^{15} \pmod{17}$: (toutes les congruences qui suivent sont modulo 17)

$$6^2 \equiv 36 \equiv 2$$

$$6^4 \equiv (6^2)^2 \equiv 2^2 \equiv 4$$

$$6^8 \equiv (6^4)^2 \equiv 4^2 \equiv 16$$

$$6^{15} \equiv 6^8 \cdot 6^4 \cdot 6^2 \cdot 6 \equiv 16 \cdot 4 \cdot 2 \cdot 6 \equiv 3$$

Vérification : $3 \cdot 6 \equiv 1 \pmod{17}$.

Cassage du code de Turing

A l'aide d'une paire (message, message encrypté), et du nombre p, il est possible de retrouver la clé k.

Supposons que l'on connaisse m et m', qui satisfont l'égalité $m' = (mk \bmod p)$.

On a

$$\begin{aligned} m^{p-2}m' &\equiv m^{p-2}mk \pmod{p} \\ &\equiv m^{p-1}k \pmod{p} \\ &\equiv k \pmod{p}. \end{aligned}$$

Arithmétique avec des modulo arbitraires

Le code de Turing (version 2) est basé sur une arithmétique modulo un nombre *premier* p.

Le RSA (algorithme de cryptographie à *clé publique*) fonctionne en arithmétique modulo le produit de *deux* grands nombres premiers.

Définition : Les nombres $a, b \in \mathbb{Z}_0$ sont *premiers entre eux* si $\text{pgcd}(a, b) = 1$.

Exemple : 8 et 15 sont premiers entre eux.

Inverses multiplicatifs et modulo arbitraires

Lemme : Soit $n \in \mathbb{N}_0$. Si $k \in \mathbb{Z}_0$ est premier avec n, alors il existe $k^{-1} \in \mathbb{Z}$ tel que $k \cdot k^{-1} \equiv 1 \pmod{n}$.

Démonstration :

- Il existe $s, t \in \mathbb{Z}$ tels que $sk + tn = \text{pgcd}(k, n) = 1$.
- Dès lors on a $tn = 1 - sk$, ce qui implique $n \mid (1 - sk)$.
- On en déduit $\underbrace{s}_{k^{-1}} k \equiv 1 \pmod{n}$. □

Corollaire : Soit $n \in \mathbb{N}_0$, et soit $k \in \mathbb{Z}$ premier avec n. Si $ak \equiv bk \pmod{n}$, alors $a \equiv b \pmod{n}$.

Démonstration : Il suffit de multiplier à droite et à gauche par k^{-1}. □

Lemme

Lemme : Soient $n \in \mathbb{N}_0$ et $k \in \mathbb{Z}_0$ premier avec n. Soit $\{k_1, k_2, \ldots, k_r\}$ l'ensemble des entiers (distincts) de l'intervalle $\{0, 1, \ldots, n-1\}$ qui sont premiers avec n. La séquence

$$(k_1 k) \bmod n,\ (k_2 k) \bmod n,\ \ldots,\ (k_r k) \bmod n$$

est une permutation de la séquence

$$k_1,\ k_2,\ \ldots,\ k_r.$$

Démonstration :

Les nombres de la première séquence sont tous distincts

- Soient $i, j \in \{1, 2, \ldots, r\}$ tels que $((k_i k) \bmod n) = ((k_j k) \bmod n)$.
- On a $k_i k \equiv k_j k \pmod{n}$, ce qui implique $k_i \equiv k_j \pmod{n}$ car k est premier avec n.
- On en déduit $k_i = k_j$ car $k_i, k_j \in \{0, 1, \ldots, n-1\}$.

Tout nombre de la première séquence apparaît dans la deuxième

- Soit $i \in \{1, 2, \ldots, r\}$.
- On a $\text{pgcd}(k_i, n) = 1$ et $\text{pgcd}(k, n) = 1$.
- Par la propriété du transparent 83, on a $\text{pgcd}(k_i k, n) = 1$.
- Par la propriété du transparent 73, on obtient $\text{pgcd}(k_i k \bmod n, n) = 1$.
- Donc, $k_i k \bmod n \in \{0, 1, \ldots, n-1\}$ est premier avec n.
- On en déduit que $k_i k \bmod n$ apparaît dans la deuxième séquence. □

Fonction indicatrice d'Euler

Définition : Soit $n \in \mathbb{N}_0$. La *fonction indicatrice d'Euler* $\phi(n)$ désigne le nombre d'entiers de $\{1, 2, \ldots, n-1\}$ qui sont premiers avec n.

Exemples :

- $\phi(7) = 6$ car 1, 2, 3, 4, 5, et 6 sont premiers avec 7.
- $\phi(12) = 4$, car seuls 1, 5, 7 et 11 sont premiers avec 12.

Théorème d'Euler : Soient $n \in \mathbb{N}_0$ et $k \in \mathbb{Z}_0$ premier avec n. On a $k^{\phi(n)} \equiv 1 \pmod{n}$.

Démonstration :

- Soit $\{k_1, k_2, \ldots, k_r\}$ l'ensemble des entiers (distincts) de l'intervalle $\{0, 1, \ldots, n-1\}$ qui sont premiers avec n.
- Par définition de $\phi(n)$, on a $r = \phi(n)$.
- On a successivement

$$\begin{aligned} & k_1 k_2 \ldots k_r \\ \equiv\ & (k_1 k \bmod n)(k_2 k \bmod n) \ldots (k_r k \bmod n) \pmod{n} \\ \equiv\ & (k_1 k)(k_2 k) \ldots (k_r k) \pmod{n} \\ \equiv\ & (k_1 k_2 \ldots k_r) k^r \pmod{n}. \end{aligned}$$

- $k_1 k_2 \ldots k_r$ est premier avec n grâce à la propriété du transparent 83. On peut donc simplifier par $k_1 k_2 \ldots k_r$.
- On obtient $k^{\phi(n)} \equiv 1 \pmod{n}$. □

Calcul d'inverse

- Le théorème d'Euler permet de calculer l'inverse d'un entier k premier avec n :

$$k^{-1} = k^{\phi(n)-1}.$$

- Le calcul demande cependant de calculer d'abord $\phi(n)$, ce qui n'est pas trivial

.

Propriétés de la fonction d'Euler

Théorème :

$$\phi(pq) = (p-1)(q-1)$$

pour des premiers $p \neq q$.

Démonstration :

- Puisque p et q sont premiers, tout nombre qui n'est pas premier avec pq est soit un multiple de p, soit un multiple de q.
- Dans $\{0, 1, \ldots, pq-1\}$, il y a q multiples de p et p multiple de q et seul 0 est un multiple de p et de q.
- Il y a donc $p+q-1$ nombres dans $\{0, 1, \ldots, pq-1\}$ qui ne sont pas premiers avec pq et on a :

$$\begin{aligned} \phi(pq) &= pq - (p+q-1) \\ &= (p-1)(q-1). \end{aligned}$$

□

Propriétés de la fonction d'Euler

Théorème :

1. Si $a, b \in \mathbb{N}_0$ sont premiers entre eux, alors $\phi(ab) = \phi(a)\phi(b)$. (admis)
2. Si p est un nombre premier, alors $\phi(p^k) = p^k - p^{k-1}$ pour tout $k \in \mathbb{N}_0$.

Démonstration de 1 :

- Chaque p-ème nombre parmi les p^k nombres dans $\{0, 1, \ldots, p^k - 1\}$ est divisible par p et ce sont les seuls.
- On a donc $1/p$ des nombres entre 0 et p^k qui sont divisibles par p, les autres ne l'étant pas :

$$\phi(p^k) = p^k - \frac{1}{p}p^k = p^k - p^{k-1}.$$

En connaissant la factorisation de $n \in \mathbb{N}_0$, la nombre $\phi(n)$ se calcule aisément grâce au théorème précédent.

Exemple : $300 = 2^2 \cdot 3 \cdot 5^2$ et

$$\begin{aligned}
\phi(300) &= \phi(2^2 \cdot 3 \cdot 5^2) \\
&= \phi(2^2) \cdot \phi(3) \cdot \phi(5^2) \\
&= \underbrace{(2^2 - 2^1)}_{2}\underbrace{(3^1 - 3^0)}_{2}\underbrace{(5^2 - 5^1)}_{20} \\
&= 80
\end{aligned}$$

Note :

- Factoriser n n'est pas un problème facile
- Par le théorème du transparent 112, le pulvérisateur permet aussi de calculer k^{-1} comme le coefficient de k dans le calcul de $\text{pgcd}(k, n)$.

RSA (Rivest Shamir Adleman)

Préparation (au niveau du récepteur) :

- Générer des entiers premiers p,q et définir $n = p \cdot q$.
- Choisir e tel que $\text{pgcd}(e, (p-1)(q-1)) = 1$. La *clé publique* est la paire (e, n) qui doit être distribuée.
- Calculer d tel que $de \equiv 1 \pmod{(p-1)(q-1)}$. La *clé secrète* est la paire (d, n).

Encodage d'un message m $(0 \leq m < n)$:

- Encoder le message avec un entier m tel que $\text{pgcd}(m, n) = 1$.
- Le destinateur code alors son message comme suit :

$$m' = m^e \bmod n.$$

Décodage de m' :

- Le récepteur décode le message en calculant :

$$m = m'^d \bmod n.$$

Exemple

Soient $p = 13$, $q = 7$ ($n = pq = 91$) et $e = 5$ ($\text{pgcd}((13-1)(7-1), 5) = 1$).

Décoder le message $m' = 2$.

Mise en œuvre pratique

- Trouver deux (grands) premiers p et q
  - Il existe beaucoup de premiers
  - Il existe des tests rapide de primalité
- Trouver e tel que $\text{pgcd}(e, (p-1)(q-1)) = 1$
  - Il est existe beaucoup de premiers avec $(p-1)(q-1)$
  - Le pgcd est facile à calculer (algorithme d'Euclide par exemple)
- Trouver l'inverse de e modulo $(p-1)(q-1)$
  - Facile avec le pulvérisateur ou Euler
- Encodage/décodage
  - Facile en utilisant l'exponentiation rapide

Pourquoi ça marche ?

Lemme : Soient p et q tels que $\text{pgcd}(p, q) = 1$. Si $a \equiv b \pmod{p}$ et $a \equiv b \pmod{q}$, alors $a \equiv b \pmod{pq}$.

Démonstration :

- Si $a \equiv b \pmod{p}$ et $a \equiv b \pmod{q}$, on a par définition $p|(a - b)$ et $q|(a - b)$.
- p et q étant premiers entre eux, on a donc $pq|(a - b)$ et donc $a \equiv b \pmod{pq}$.

Pourquoi ça marche ?

Nous devons montrer que

$$m = (m')^d \bmod n = (m^e \bmod n)^d \bmod n.$$

Démonstration :

- Par la deuxième propriété du transparent 97, il suffit de démontrer que

$$m = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n.$$

- On va démontrer que $m \equiv m^{ed} \pmod{p}$. Par symétrie, on aura $m \equiv m^{ed} \pmod{q}$ et par le lemme précédent $m \equiv m^{ed} \pmod{n}$.
- Comme $m \in \{0, 1, \ldots, n-1\}$, on aura démontré que :

$$m = m^{ed} \bmod n.$$

Montrons que $m \equiv m^{ed} \pmod{p}$

- Puisque $ed \equiv 1 \pmod{(p-1)(q-1)}$, on a $(p-1)(q-1) | (ed-1)$ et donc il existe un entier k tel que $(ed-1) = k(p-1)$.
- On a

$$\begin{aligned} m^{ed} &\equiv m^{ed-1+1} \pmod{p} \\ &\equiv (m^{ed-1}).m \pmod{p} \\ &\equiv (m^{k(p-1)}).m \pmod{p}. \end{aligned}$$

- Comme p est premier, soit $\text{pgcd}(m, p) = 1$, soit $\text{pgcd}(m, p) = p$.

- Si $\text{pgcd}(m, p) = 1$:
  - Par le petit théorème de Fermat, on a $m^{p-1} \equiv 1 \pmod{p}$ et donc $m^{k(p-1)} \equiv 1^k \equiv 1 \pmod{p}$
  - Finalement, on a

$$m^{ed} \equiv 1 \cdot m \equiv m \pmod{p}.$$

- Si $\text{pgcd}(m, p) = p$:
  - $m = kp$ et donc $m^{ed} = k'p$ et $m^{ed} \equiv 0 \pmod{p}$
  - Or $m \equiv 0 \pmod{p}$
  - D'où $m^{ed} \equiv m \pmod{p}$.

□

Sécurité

- Casser ce code est facile si on peut factoriser n en un produit pq où p et q sont premiers.
- On peut alors trouver d à partir de e et $(p-1)(q-1)$ par le pulvérisateur.
- Il n'existe cependant pas de méthode efficace pour faire ça.
- RSA n'a toujours pas été cassé en 30 ans.