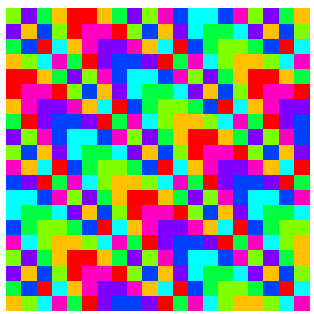
Cryptographie : Le Retour

Michel Rigo

http://www.discmath.ulg.ac.be/
http://orbi.uliege.be/

Rencontre annuelle de l'AMULg, 10 avril 2024



Il me fallait un nouvel exposé parlant de cryptographie. . .

Krypto

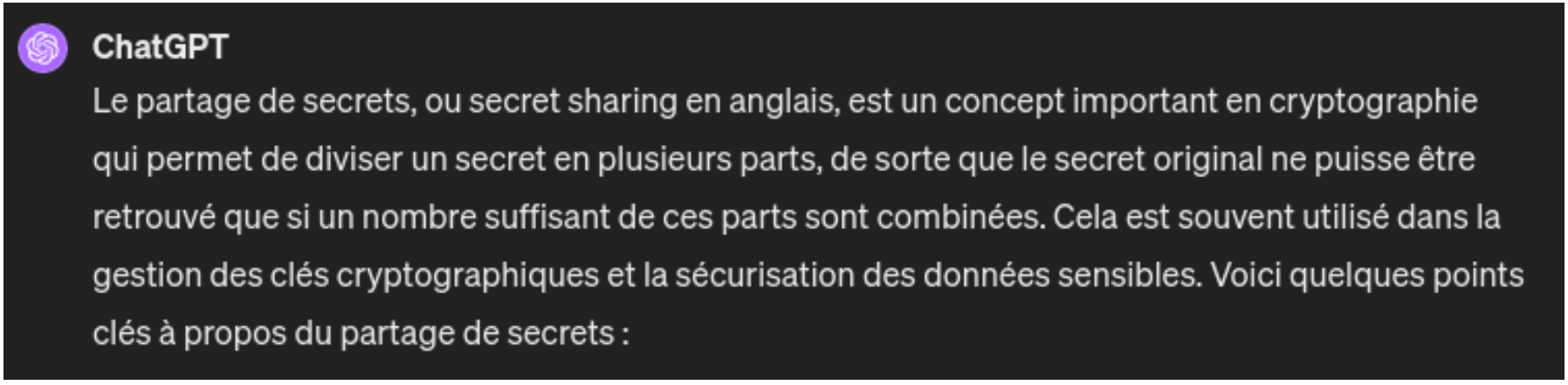
Dans cet exposé, *tout est nombre* — devise de l'école pythagoricienne, les dieux avaient ordonné l'univers par des nombres.

`tout |est n|ombre` $\longrightarrow$

26^4	26^3	26^2	26	1	
20	15	21	20	0	9417876
5	19	20	0	14	2632358
15	13	2	18	5	7084953

256^2	256	1	
$(132,$	$72,$	$243)$	8669427
$(92,$	$202,$	$23)$	6081047
$(101,$	$53,$	$131)$	6632835

Commençons avec le partage de secrets



ChatGPT

Le partage de secrets, ou secret sharing en anglais, est un concept important en cryptographie qui permet de diviser un secret en plusieurs parts, de sorte que le secret original ne puisse être retrouvé que si un nombre suffisant de ces parts sont combinées. Cela est souvent utilisé dans la gestion des clés cryptographiques et la sécurisation des données sensibles. Voici quelques points clés à propos du partage de secrets :

- Le partage de secrets est utilisé pour sécuriser les clés cryptographiques en les divisant en plusieurs parts distribuées à différents administrateurs. Ainsi, aucun administrateur individuel ne peut accéder seul à la clé.
- Il est également utilisé dans les systèmes de stockage sécurisé, les procédures de récupération de mot de passe, et pour assurer la continuité des affaires en cas de perte d'accès clé.

Le schéma de Shamir (1979) — SSS Shamir's secret sharing

Adi Shamir

J.-L. Lagrange 1736–1813

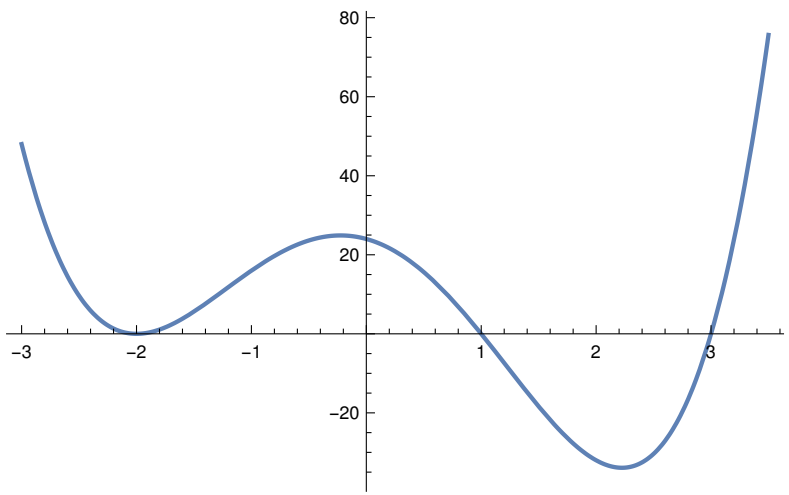
Un peu de théorie

Théorème fondamental de l'algèbre

Un polynôme $P \in \mathbb{C}[z]$ de degré $d \geq 1$ possède exactement d zéros (complexes) comptés avec leur multiplicité

$$P(z) = a(z - z_1)^{m_1} \cdots (z - z_n)^{m_n} \text{ et } m_1 + \cdots + m_n = d.$$

$$2\,x^4 - 18\,x^2 - 8\,x + 24 = 2(x+2)^2(x-1)(x-3)$$



Corollaire

Si deux polynômes P et Q de degré (au plus) d sont égaux en $d+1$ points, alors ils sont égaux.

Soient $z_1, \ldots, z_{d+1}$ des nombres complexes 2 à 2 distincts tels que $P(z_i) = Q(z_i)$ pour $i = 1, \ldots, d+1$

Le polynôme $P - Q$ est de degré au plus d

$(P - Q)(z_i) = P(z_i) - Q(z_i) = 0$ pour tout $i = 1, \ldots, d+1$

Si un polynôme de degré au plus d possède $d+1$ zéros...

Il est nul ! Donc, $P - Q = 0$

Corollaire

Si deux polynômes P et Q de degré (au plus) d sont égaux en $d+1$ points, alors ils sont égaux.

Soient $z_1, \ldots, z_{d+1}$ des nombres complexes 2 à 2 distincts tels que $P(z_i) = Q(z_i)$ pour $i = 1, \ldots, d+1$

Le polynôme $P - Q$ est de degré au plus d

$(P - Q)(z_i) = P(z_i) - Q(z_i) = 0$ pour tout $i = 1, \ldots, d+1$

Si un polynôme de degré au plus d possède $d+1$ zéros...

Il est nul ! Donc, $P - Q = 0$

Corollaire

Si deux polynômes P et Q de degré (au plus) d sont égaux en $d+1$ points, alors ils sont égaux.

Soient $z_1, \ldots, z_{d+1}$ des nombres complexes 2 à 2 distincts tels que $P(z_i) = Q(z_i)$ pour $i = 1, \ldots, d+1$

Le polynôme $P - Q$ est de degré au plus d

$(P - Q)(z_i) = P(z_i) - Q(z_i) = 0$ pour tout $i = 1, \ldots, d+1$

Si un polynôme de degré au plus d possède $d+1$ zéros...

Il est nul ! Donc, $P - Q = 0$

Corollaire

Si deux polynômes P et Q de degré (au plus) d sont égaux en $d+1$ points, alors ils sont égaux.

Soient $z_1, \ldots, z_{d+1}$ des nombres complexes 2 à 2 distincts tels que $P(z_i) = Q(z_i)$ pour $i = 1, \ldots, d+1$

Le polynôme $P - Q$ est de degré au plus d

$(P - Q)(z_i) = P(z_i) - Q(z_i) = 0$ pour tout $i = 1, \ldots, d+1$

Si un polynôme de degré au plus d possède $d+1$ zéros...

Il est nul ! Donc, $P - Q = 0$

Corollaire

Si deux polynômes P et Q de degré (au plus) d sont égaux en $d+1$ points, alors ils sont égaux.

Soient $z_1, \ldots, z_{d+1}$ des nombres complexes 2 à 2 distincts tels que $P(z_i) = Q(z_i)$ pour $i = 1, \ldots, d+1$

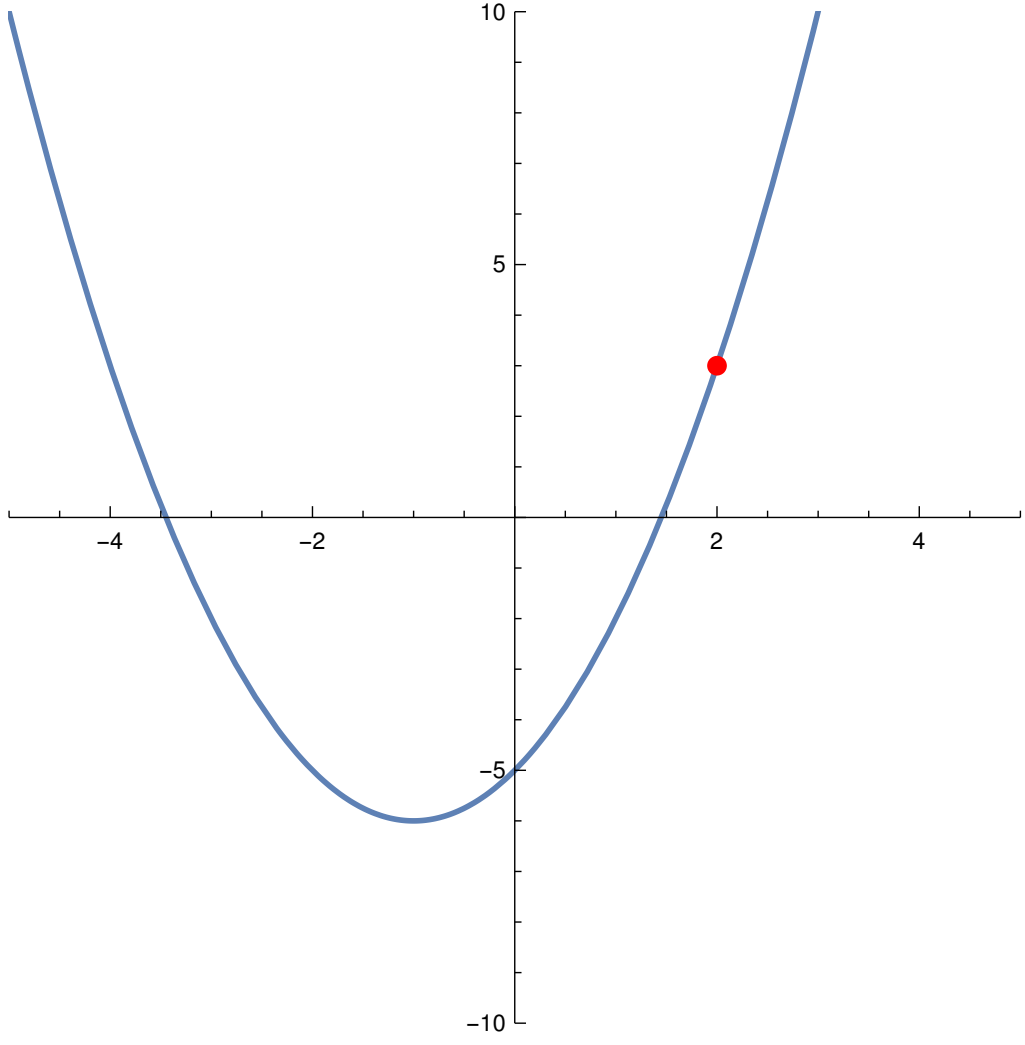
Le polynôme $P - Q$ est de degré au plus d

$(P - Q)(z_i) = P(z_i) - Q(z_i) = 0$ pour tout $i = 1, \ldots, d+1$

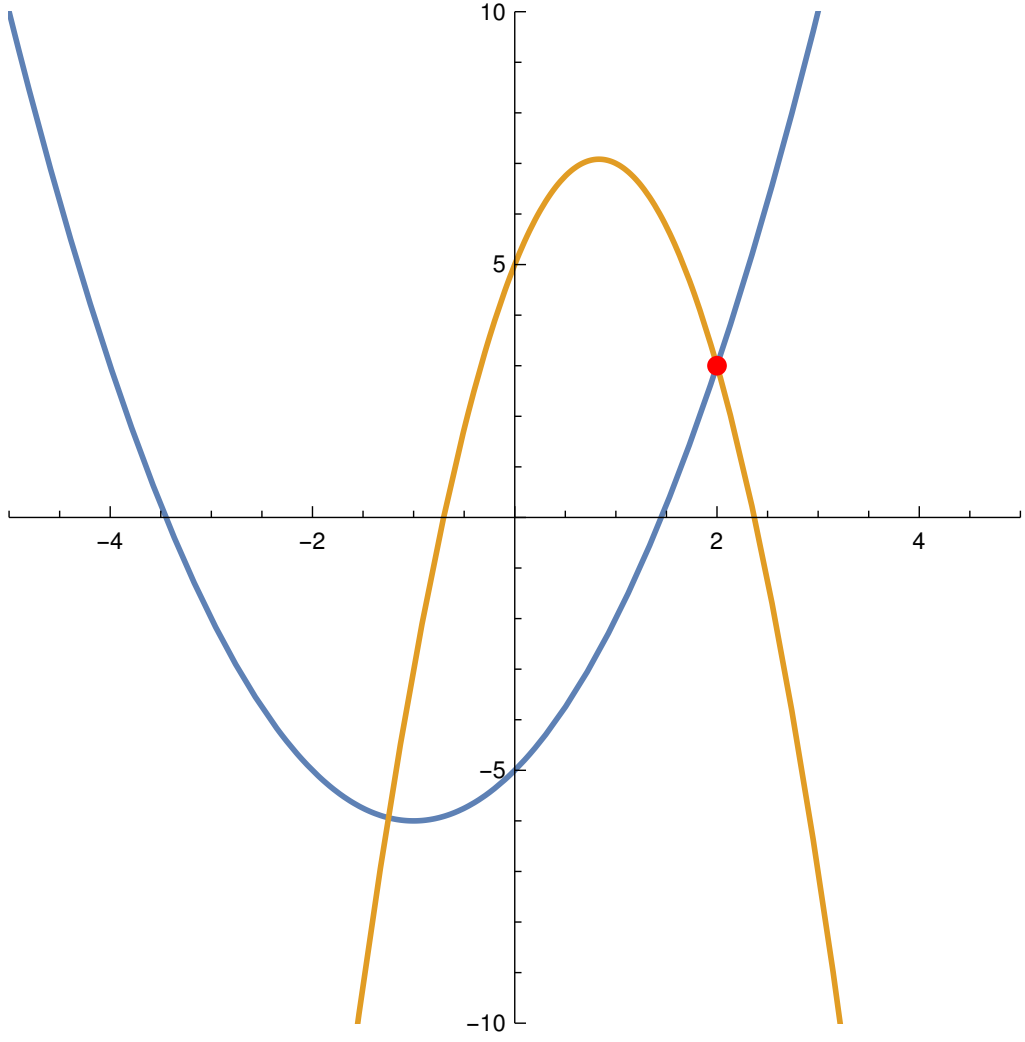
Si un polynôme de degré au plus d possède $d+1$ zéros...

Il est nul ! Donc, $P - Q = 0$

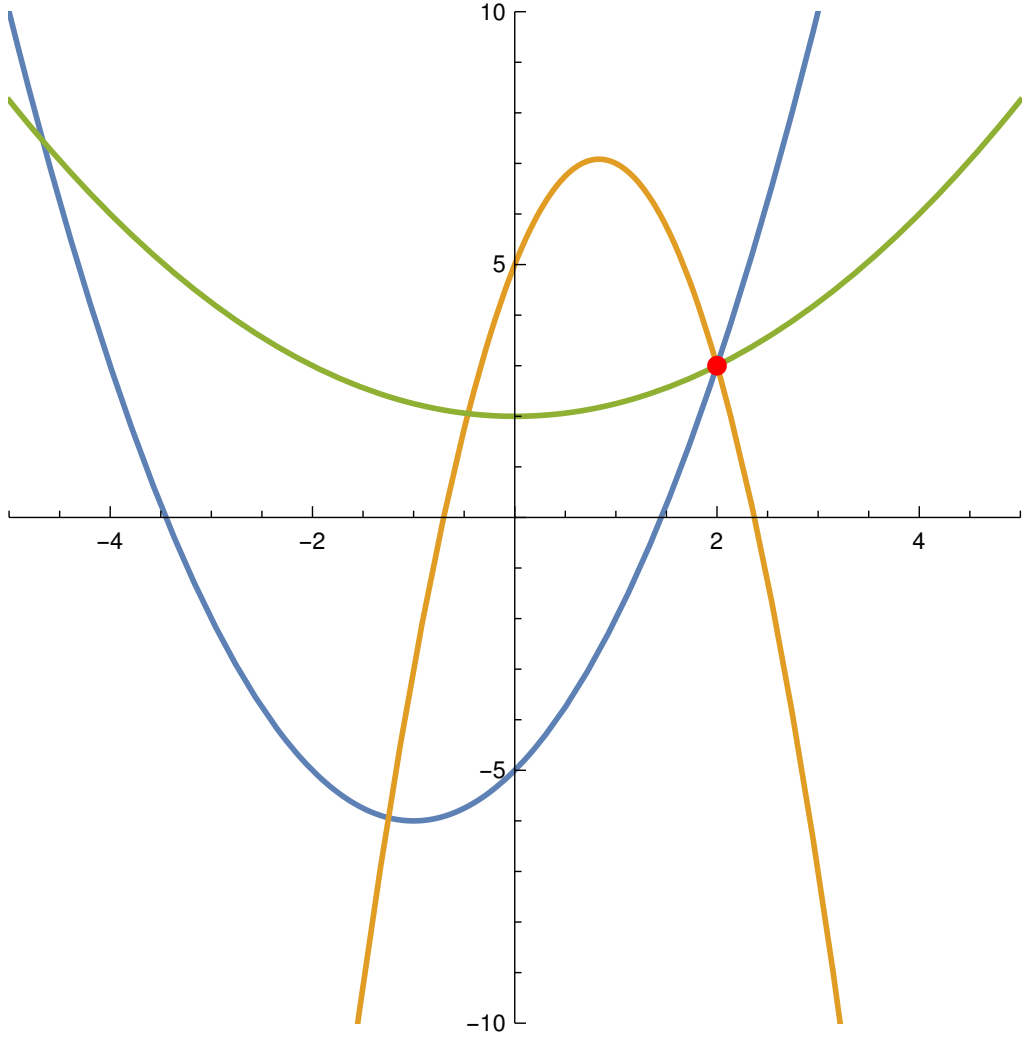
Application : étant donnés 3 points du plan, il existe une et une seule parabole (d'axe vertical) passant par ces points.



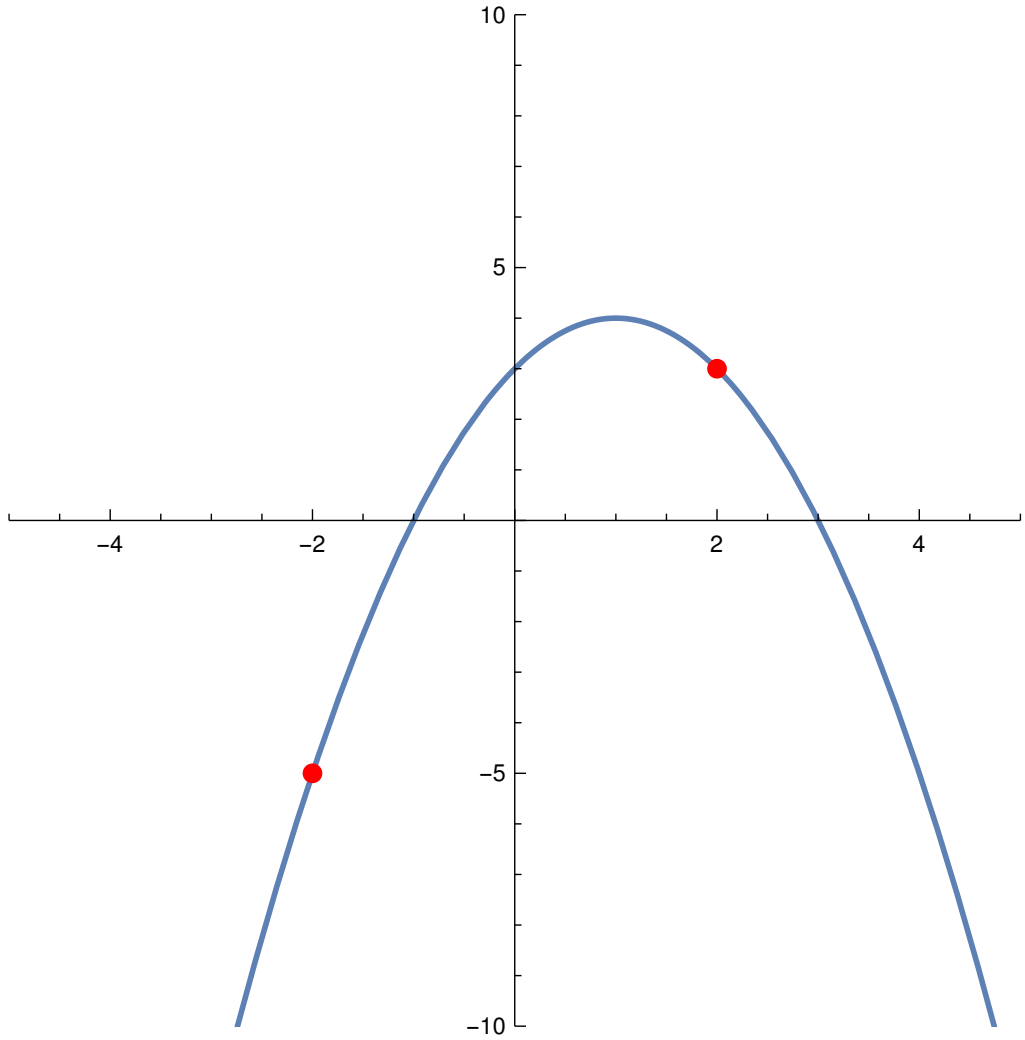
Application : étant donnés 3 points du plan, il existe une et une seule parabole (d'axe vertical) passant par ces points.



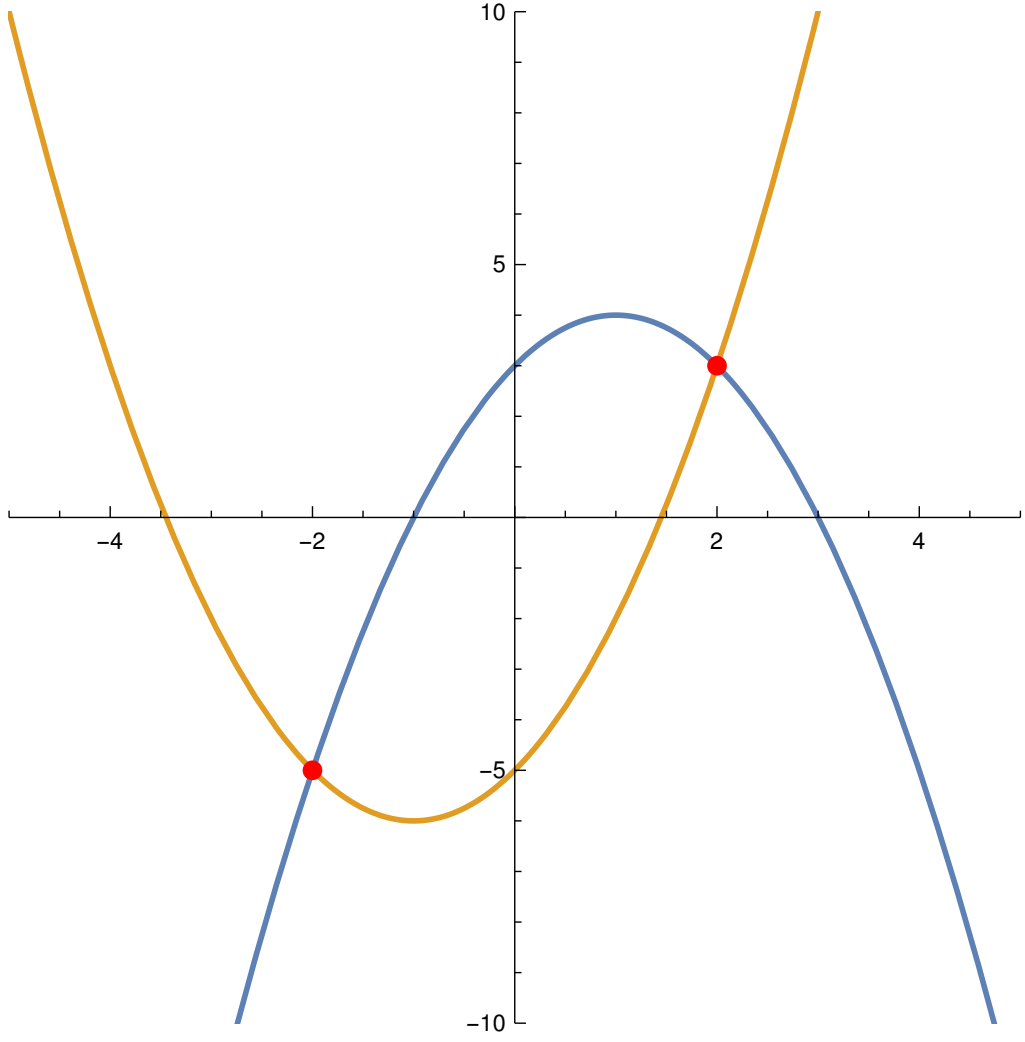
Application : étant donnés 3 points du plan, il existe une et une seule parabole (d'axe vertical) passant par ces points.



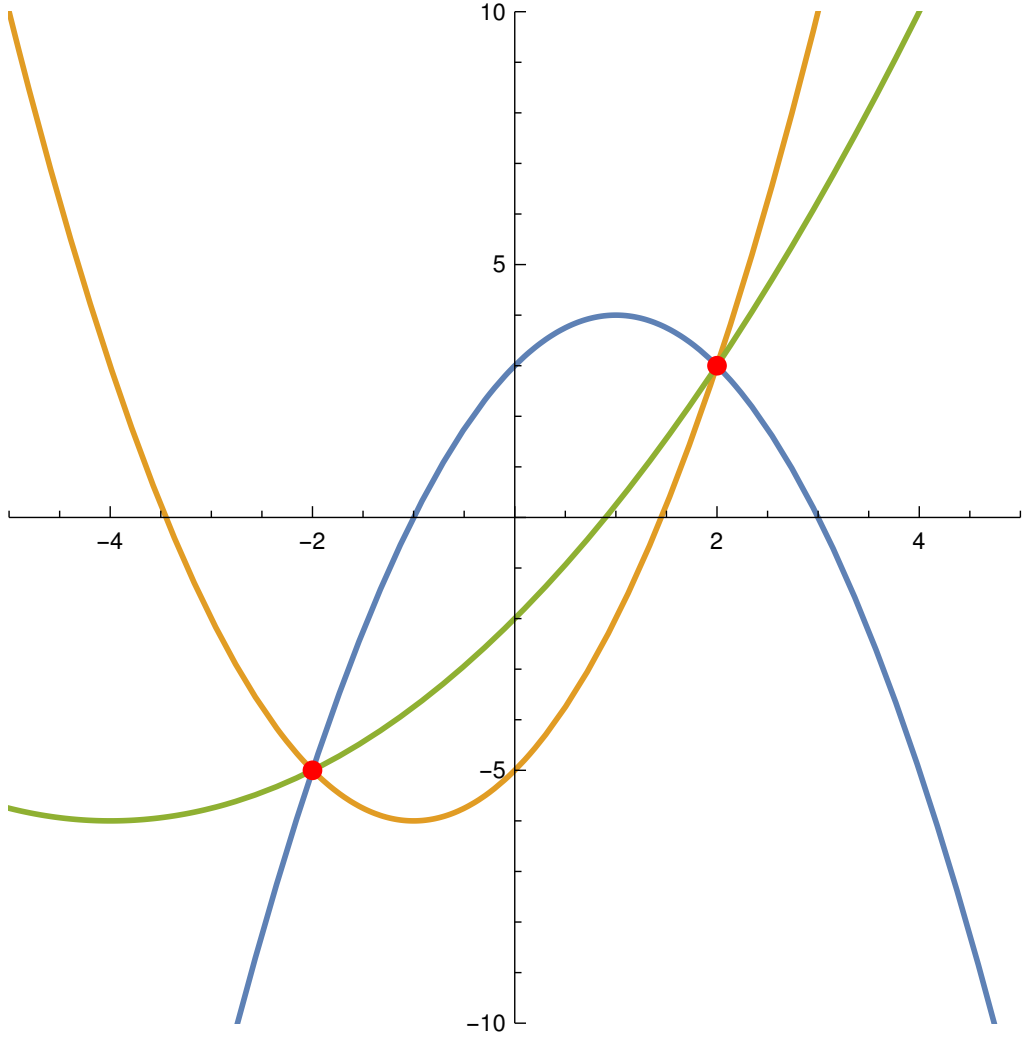
Application : étant donnés 3 points du plan, il existe une et une seule parabole (d'axe vertical) passant par ces points.



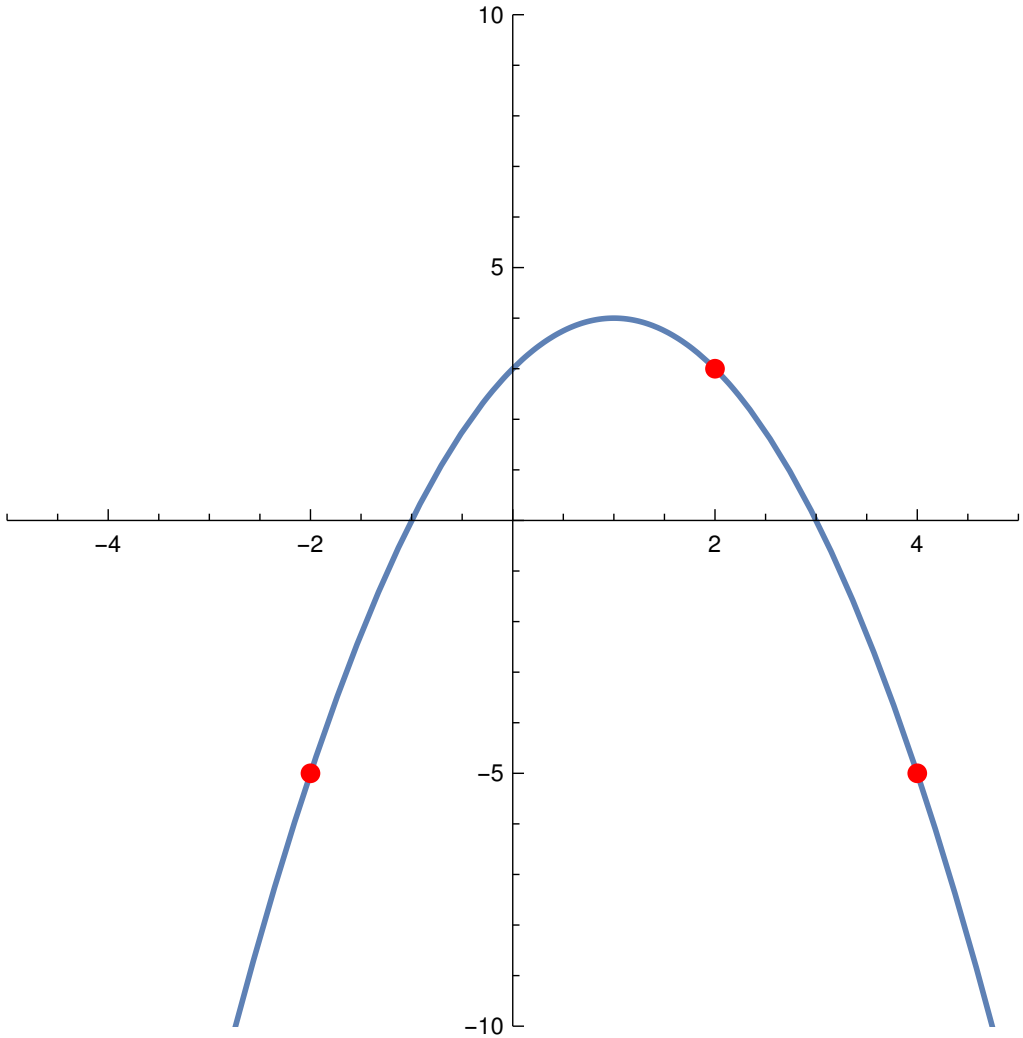
Application : étant donnés 3 points du plan, il existe une et une seule parabole (d'axe vertical) passant par ces points.



Application : étant donnés 3 points du plan, il existe une et une seule parabole (d'axe vertical) passant par ces points.

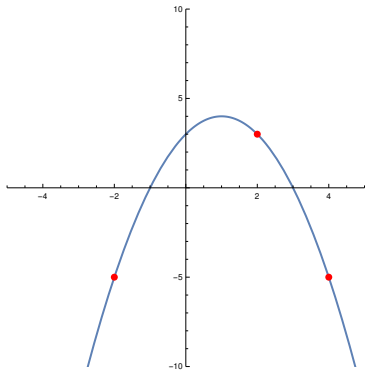


Application : étant donnés 3 points du plan, il existe une et une seule parabole (d'axe vertical) passant par ces points.



Alternative de preuve (*bien sûr généralisable*)

On a un polynôme (par exemple de degré 3) : $P(x) = ax^2 + bx + c$
On connaît x_1, x_2, x_3 et $y_1 = P(x_1), y_2 = P(x_2), y_3 = P(x_3)$ donc



$$\begin{cases} a\,x_1^2 + b\,x_1 + c = y_1 \\ a\,x_2^2 + b\,x_2 + c = y_2 \\ a\,x_3^2 + b\,x_3 + c = y_3 \end{cases}$$

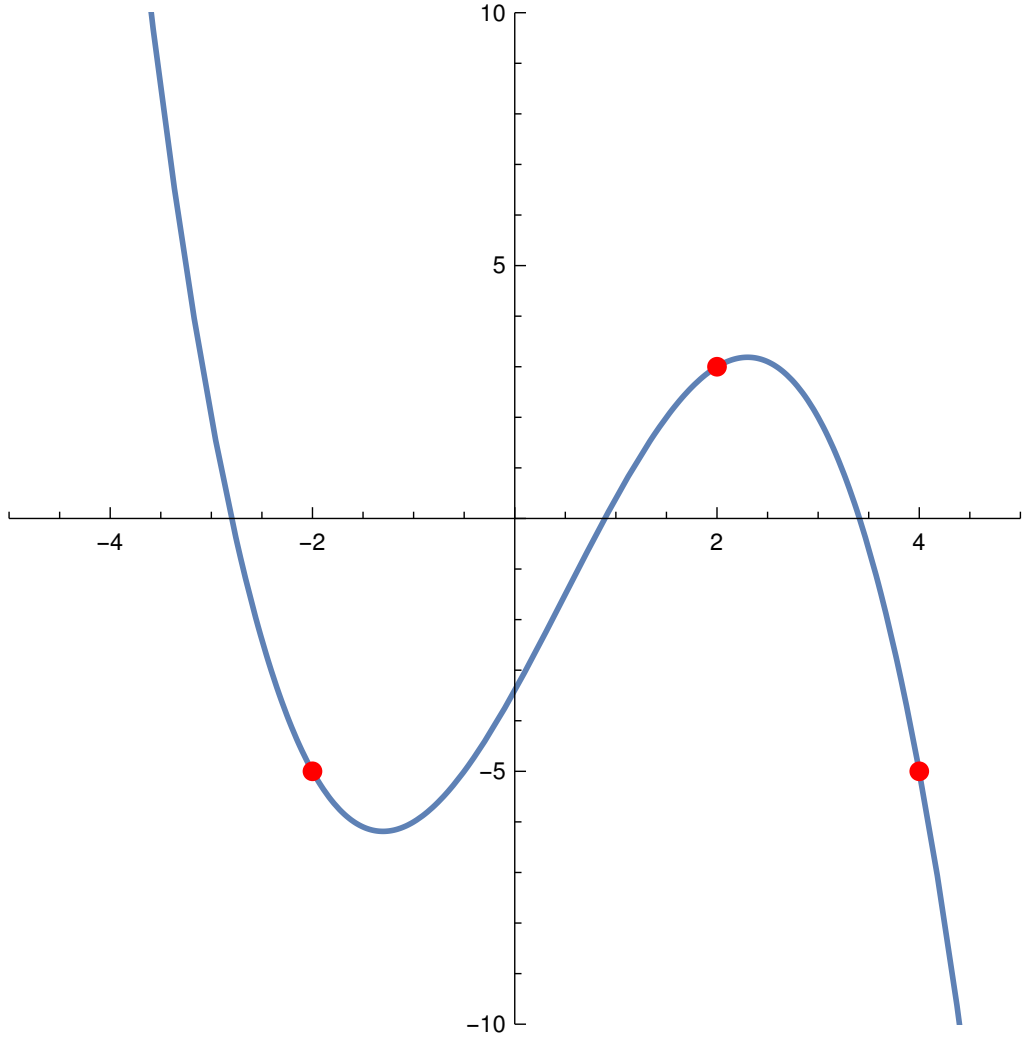
On a un système linéaire dont les inconnues sont a, b, c

$$D = \det \begin{pmatrix} x_1^2 & x_1 & 1 \\ x_2^2 & x_2 & 1 \\ x_3^2 & x_3 & 1 \end{pmatrix} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \neq 0$$

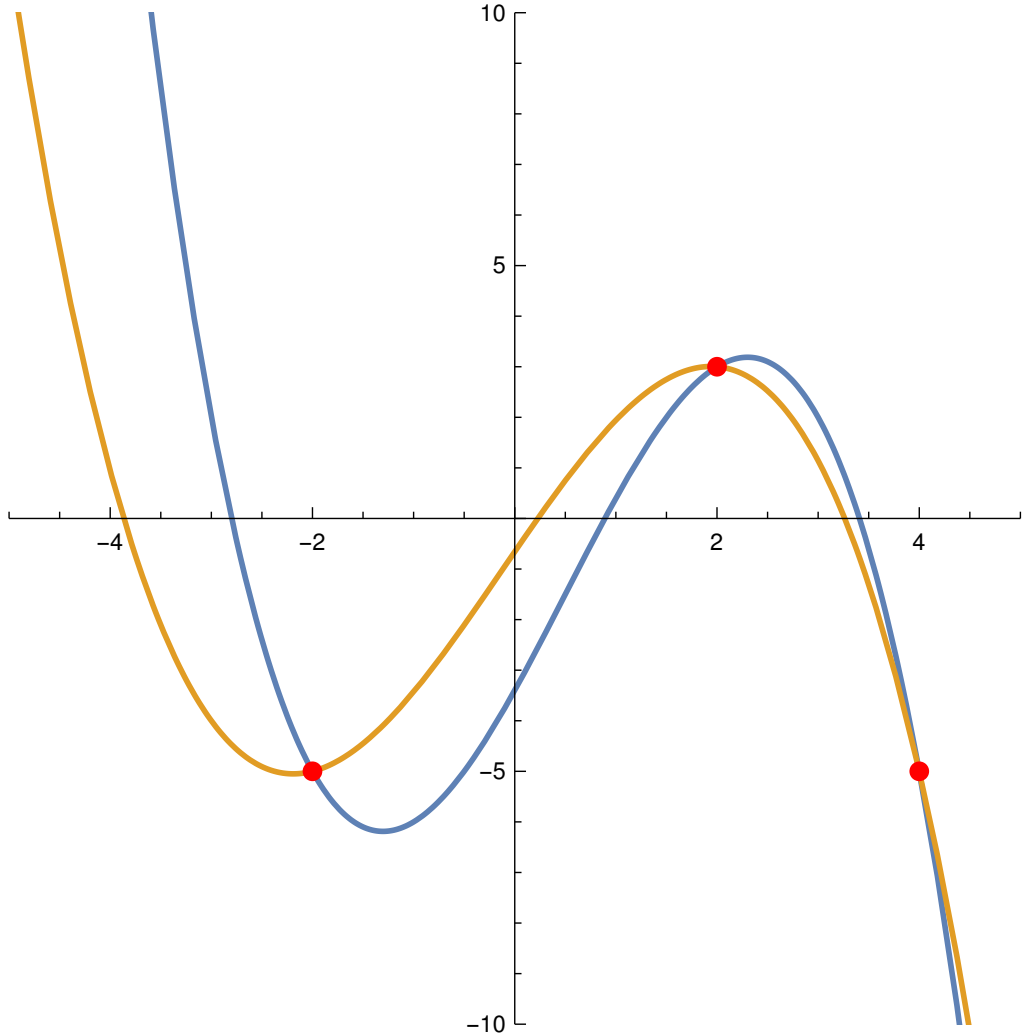
Le système possède une solution unique.

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \frac{1}{D} \begin{pmatrix} x_2 - x_3 & x_3 - x_1 & x_1 - x_2 \\ x_3^2 - x_2^2 & x_1^2 - x_3^2 & x_2^2 - x_1^2 \\ x_2^2 x_3 - x_2 x_3^2 & x_1 x_3^2 - x_1^2 x_3 & x_1^2 x_2 - x_1 x_2^2 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

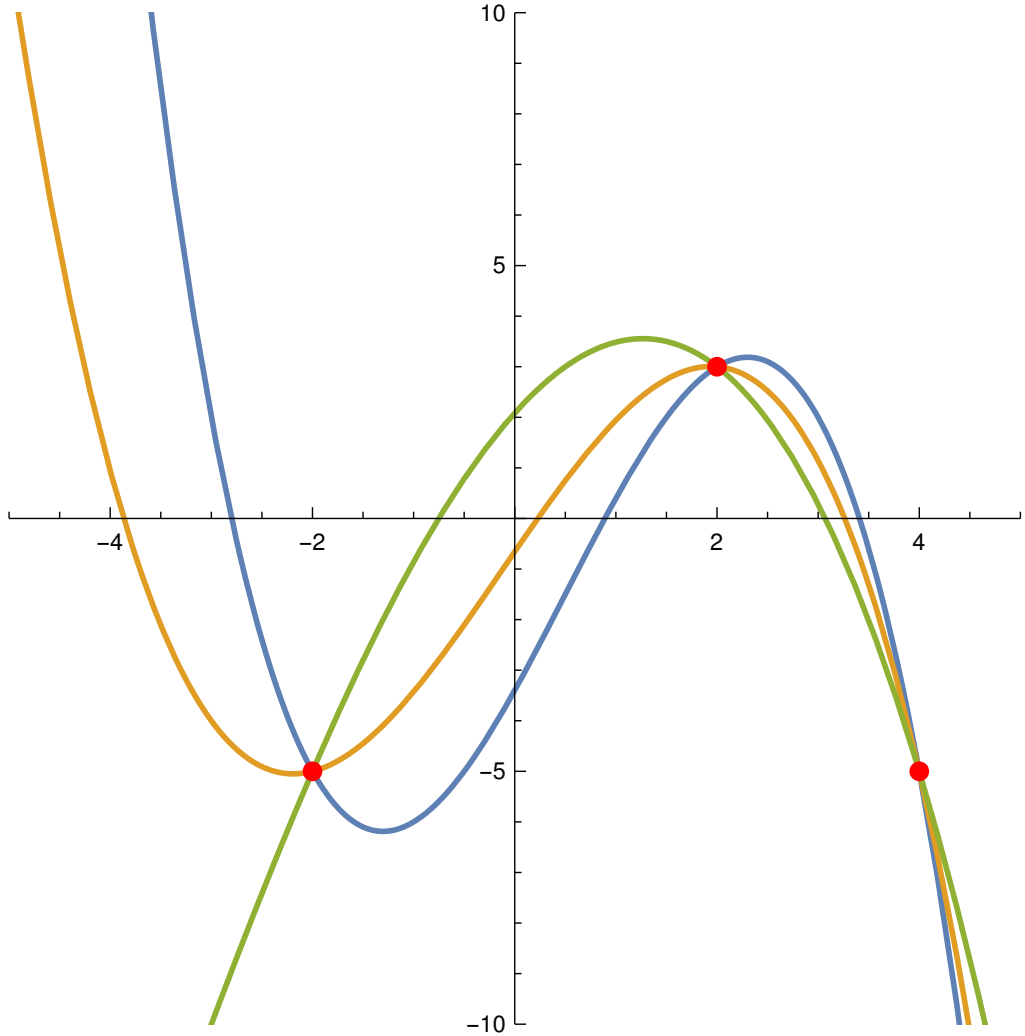
Attention : ce n'est pas vrai pour un polynôme de degré 3.
Système de 3 équations à 4 inconnues, infinité de solutions.



Attention : ce n'est pas vrai pour un polynôme de degré 3.
Système de 3 équations à 4 inconnues, infinité de solutions.



Attention : ce n'est pas vrai pour un polynôme de degré 3.
Système de 3 équations à 4 inconnues, infinité de solutions.



Passons à l'application

Dans ce groupe, 7 volontaires (dont 2 espions ennemis)

x_i	$P(x_i)$
25	7331974
26	7366456
58	10644184
66	12371776
77	15542878
85	18505774
93	22087294

Le secret (nombre à 7 chiffres) provient d'un polynôme de degré 3
On a besoin de 4 données pour retrouver le secret...

Polynôme d'interpolation de Lagrange

On connaît x_1, x_2, x_3, x_4 et les valeurs $y_i = P(x_i)$, $i = 1, 2, 3, 4$

$$\ell_1(X) = \frac{(X - x_2)}{(x_1 - x_2)} \frac{(X - x_3)}{(x_1 - x_3)} \frac{(X - x_4)}{(x_1 - x_4)}$$

$$\ell_2(X) = \frac{(X - x_1)}{(x_2 - x_1)} \frac{(X - x_3)}{(x_2 - x_3)} \frac{(X - x_4)}{(x_2 - x_4)}$$

$$\ell_3(X) = \frac{(X - x_1)}{(x_3 - x_1)} \frac{(X - x_2)}{(x_3 - x_2)} \frac{(X - x_4)}{(x_3 - x_4)}$$

$$\ell_4(X) = \frac{(X - x_1)}{(x_4 - x_1)} \frac{(X - x_2)}{(x_4 - x_2)} \frac{(X - x_3)}{(x_4 - x_3)}$$

on reconstruit le polynôme P :

$$P(X) = y_1\, \ell_1(X) + y_2\, \ell_2(X) + y_3\, \ell_3(X) + y_4\, \ell_4(X)$$

Dans ce groupe, 7 volontaires (dont 2 espions ennemis)

x_i	$P(x_i)$
25	7331974
26	7366456
58	10644184
66	12371776
77	15542878
85	18505774
93	22087294

Le secret (nombre à 7 chiffres) provient d'un polynôme de degré 3
On a besoin de 4 données pour retrouver le secret...

Le secret est le terme indépendant de $P(x)$, i.e. $P(0)$

```
a = {26, 66, 77, 85};
p = {7 366 456, 12 371 776, 15 542 878, 18 505 774};

l[i_] := Product[(x - a[[k]]) / (a[[i]] - a[[k]]),
  {k, Drop[Range[4], {i}]}]

Sum[p[[j]] × l[j], {j, 1, 4}] // Expand
```

$$7\,091\,974 - 1975\,x - 12\,x^2 + 19\,x^3$$

```
% /. x → 0
```

$$7\,091\,974$$

Cryptographie à clé publique

ChatGPT

La cryptographie à clé publique, également connue sous le nom de cryptographie asymétrique, utilise une paire de clés, une clé publique et une clé privée, pour sécuriser la communication et les données. Voici quelques exemples courants de son utilisation :

- Chiffrement des données
- Signature numérique
- Authentification
- SSL/TLS pour la sécurité web
- Échanges sécurisés de clés
- Blockchain et cryptomonnaies

Le RSA est un exemple de cryptosystème à clé publique

- Alice choisit 2 grands nombres premiers p et q.
- Elle calcule le produit $n = p.q$
- Elle calcule $\varphi(n) = (p-1).(q-1)$
- Alice choisit e et d tels que $d.e = 1 \mod \varphi(n)$. Pour ce faire, elle choisit e tel que

$$1 < e < \varphi(n) \quad \text{et} \quad \text{pgcd}(e, \varphi(n)) = 1.$$

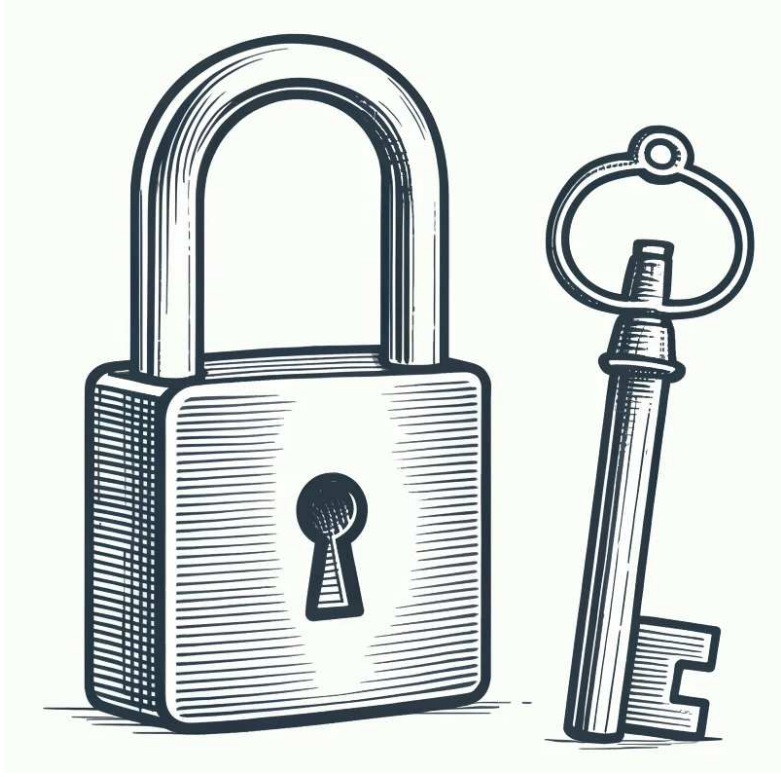
- Je ne dirai pas comment trouver de *grands* nombres premiers...
- L'adjectif *grand* est relatif à une époque donnée...
- Rappel : "calculer modulo N", reste après division par N

$$93 \bmod 15 = 3 \text{ car } 93 = 6.15 + 3$$

$$6^2 \bmod 15 = 6 \text{ car } 36 = 2.15 + 6$$

$$x^{63} = x^{2^6-1} = x^{2^5}.x^{2^4}.x^{2^3}.x^{2^2}.x^{2^1}.x$$

$$x^{25} = x^{2^4}.x^{2^3}.x^{2^2}.x^{2^1}.x$$



code–couleur :

publique	secret
n, e	$d, p, q, \varphi(n)$

$$x^{e} \mod n = y$$

$$y^{d} \mod n = x$$

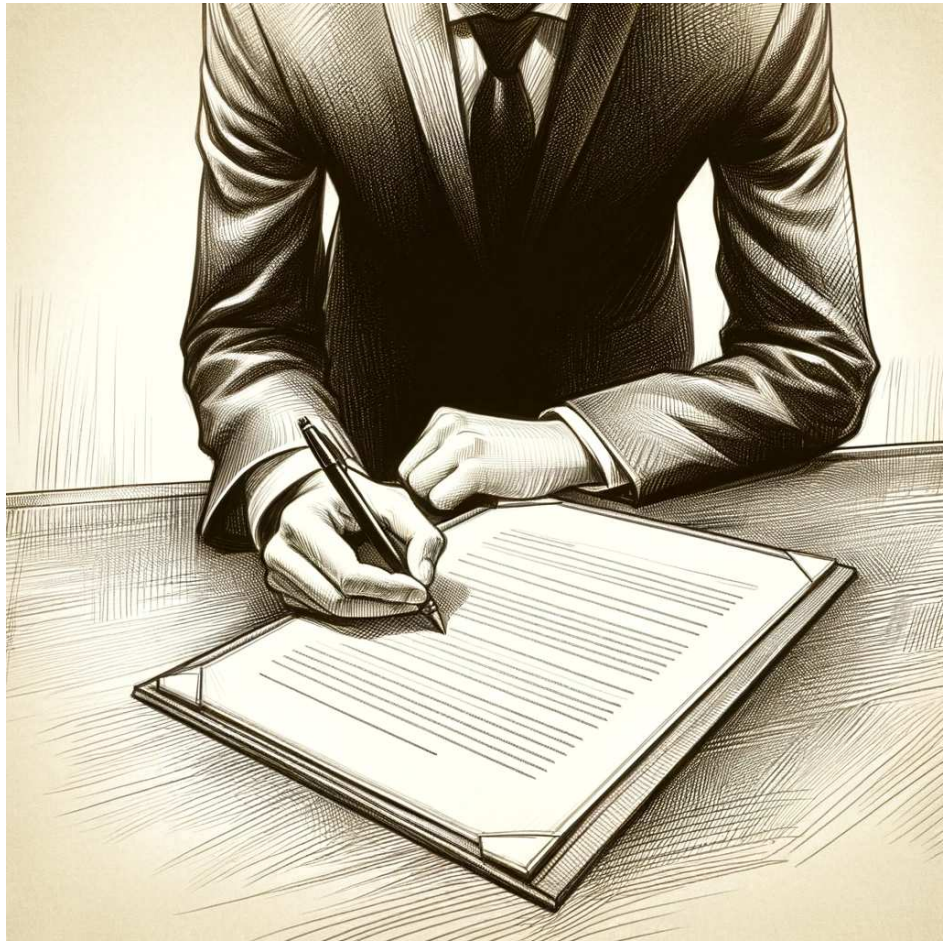
La sécurité repose sur la difficulté de factoriser $n = p\,q$.

`https://en.wikipedia.org/wiki/RSA_Factoring_Challenge`

RSA220 [b]	220	729		May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA230 [b]	230	762		August 15, 2018	Samuel S. Gross, Noblis, Inc.
RSA232 [b]	232	768		February 17, 2020[13]	N. L. Zamarashkin, D. A. Zheltkov and S. A. Matveev.
RSA768 [b]	232	768	US$50,000	December 12, 2009	Thorsten Kleinjung *et al.*[14]
RSA240 [b]	240	795		Dec 2, 2019[15]	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann
RSA250 [b]	250	829		Feb 28, 2020[16]	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann
RSA260	260	862			
RSA270	270	895			
RSA896	270	896	US$75,000[d]		
RSA280	280	928			
RSA290	290	962			
RSA300	300	995			

"RSA-2048 has 617 decimal digits (2,048 bits).
It is the largest of the RSA numbers and carried the largest cash prize for its factorization, $200,000."

```
RSA-2048 = 25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357
```



Signature (n.f.): Inscription qu'une personne fait de son nom (sous une forme particulière et constante) en vue de certifier exact ou authentique, ou d'engager sa responsabilité.
Exemple: *Apposer sa signature au bas d'un contrat*.

- Un texte est coupé en blocs (de taille convenable)
- chaque bloc correspond à un nombre $x < n$
- Bob *chiffre* chaque bloc grâce à la clé publique d'Alice

$$x^e \mod n = y$$

- Alice (et elle seule) peut *déchiffrer* les blocs reçus

$$y^d \mod n = x$$

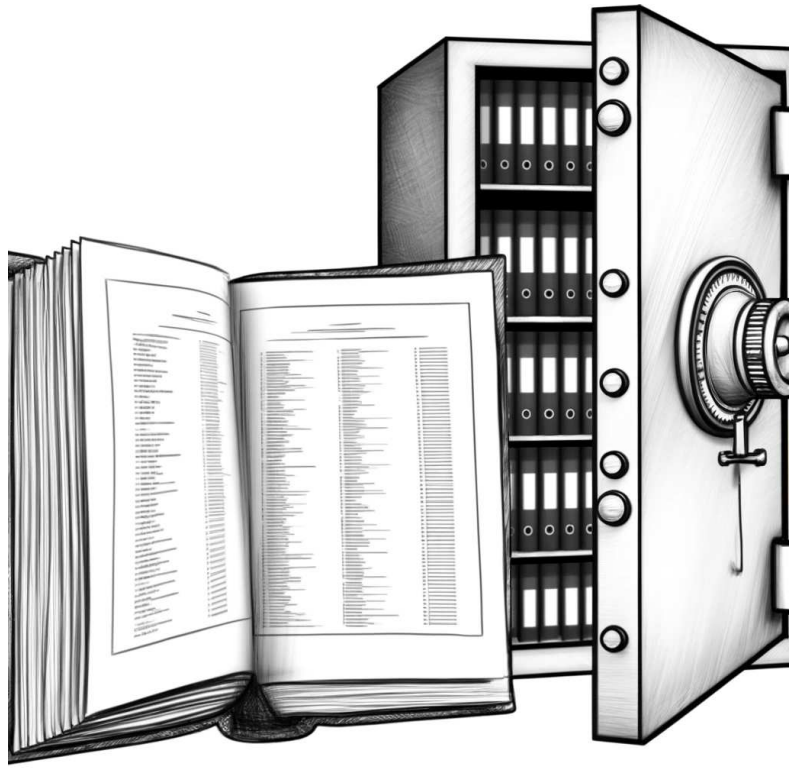
Remarque : théorie des nombres du XVIII siècle

Mais, on a évidemment

$$(x^e)^d = x^{1+\varphi(n)} = x = (x^d)^e \mod n$$

Théorème d'Euler, généralisation d'un théorème de Fermat

La clé publique d'Alice (n, e) est stockée dans un registre officiel, non falsifiable et accessible



Si Alice veut signer un document x, elle calcule $x^d \mod n$.
Authentification : Elle seule peut effectuer ce calcul.

En pratique, cela se complique : on signe et on chiffre

	publique	secret
$Alice$:	n_A, e_A	$d_A, p_A, q_A, \varphi(n_A)$
Bob :	n_B, e_B	$d_B, p_B, q_B, \varphi(n_B)$

Alice calcule et envoie à Bob

$$(x^{d_A})^{e_B} = y$$

Seul Bob peut déchiffrer, puis vérifier la signature

$$(y^{d_B})^{e_A} = x.$$

$$\text{Mais} \quad x^{d_A} \bmod n_A \in \{0, 1, 2, \ldots, n_A\}.$$

Pour assurer l'injectivité, il faut que $n_A < n_B$ ...
Sinon, on pourrait avoir $x^{d_A} = x'^{d_A}$ modulo n_B

En (pratique)^2, cela se complique encore, on fixe un seuil S et

	publique	secret
$Alice - signe :$	n_{A_s}, e_{A_s}	$d_{A_s}, p_{A_s}, q_{A_s}, \varphi(n_{A_s})$
$Alice - chiffre :$	n_{A_c}, e_{A_c}	$d_{A_c}, p_{A_c}, q_{A_c}, \varphi(n_{A_c})$
$Bob - signe :$	n_{B_s}, e_{B_s}	$d_{B_s}, p_{B_s}, q_{B_s}, \varphi(n_{B_s})$
$Bob - chiffre :$	n_{B_c}, e_{B_c}	$d_{B_c}, p_{B_c}, q_{B_c}, \varphi(n_{B_c})$

$$x < n_{A_s}, n_{B_s} < S < n_{A_c}, n_{B_c}$$

Alice calcule et envoie à Bob

$$(x^{d_{A_s}})^{e_{B_c}} = y$$

Seul Bob peut déchiffrer, puis vérifier la signature.

$$(y^{d_{B_c}})^{e_{A_s}} = x.$$

Le RSA n'est pas rapide... On veut éviter de signer tout le document mais tout de même "approuver l'ensemble"...

Concept de haché de taille fixe

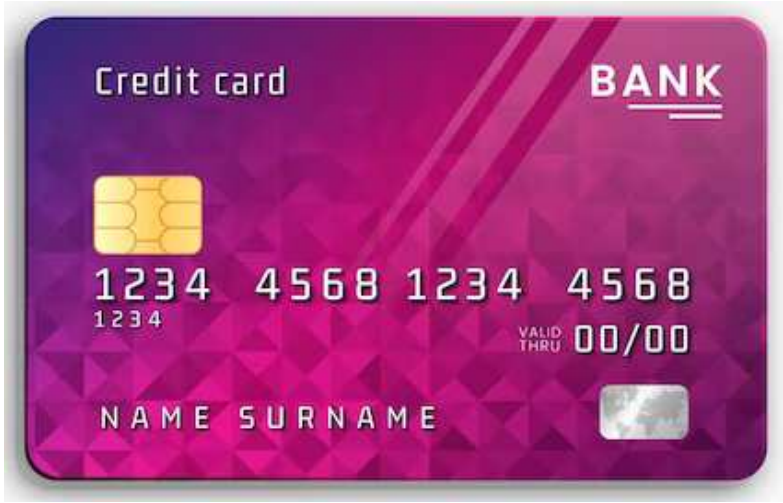
Associer à un nombre, un nombre de taille bornée (modulo 97)

$9783782711\ 28$

$97837833711\ 58$

$96837827711\ 44$

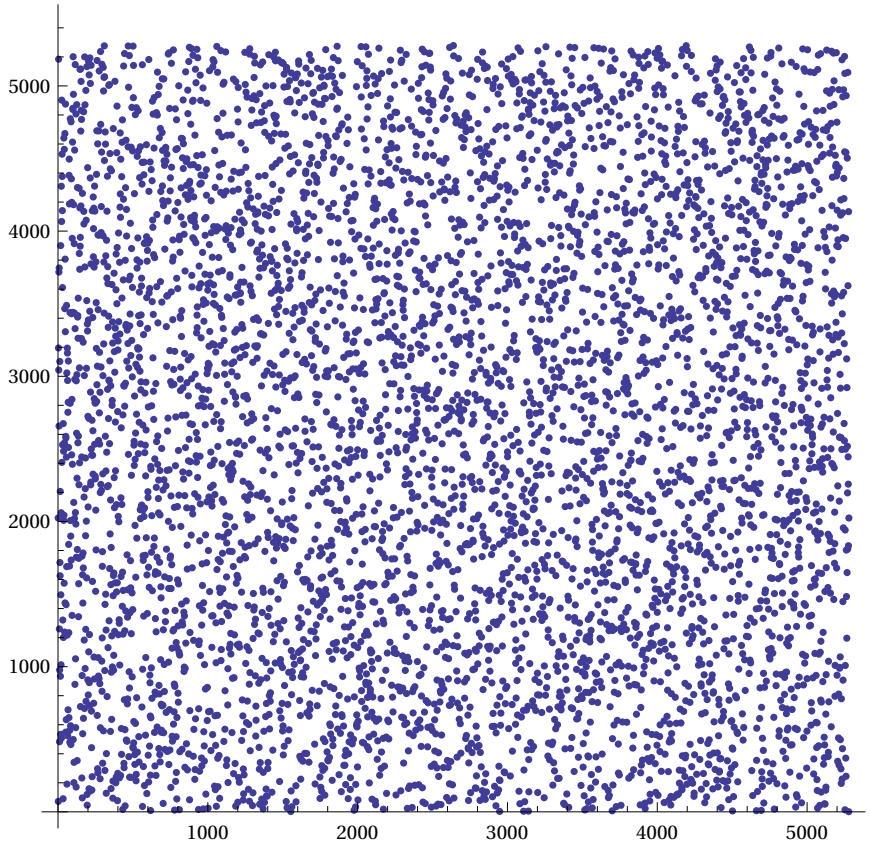
$H : x \mapsto x \bmod 97$



i	9	8	7	6	5	4	3	2	1	0
$10^i \bmod 97$	34	81	76	27	90	9	30	3	10	1
$-10^i \bmod 97$		16								

Concept de sens unique

$H : x \mapsto 2024^x \bmod 5729, \quad x = 1, 2, 3, \ldots$

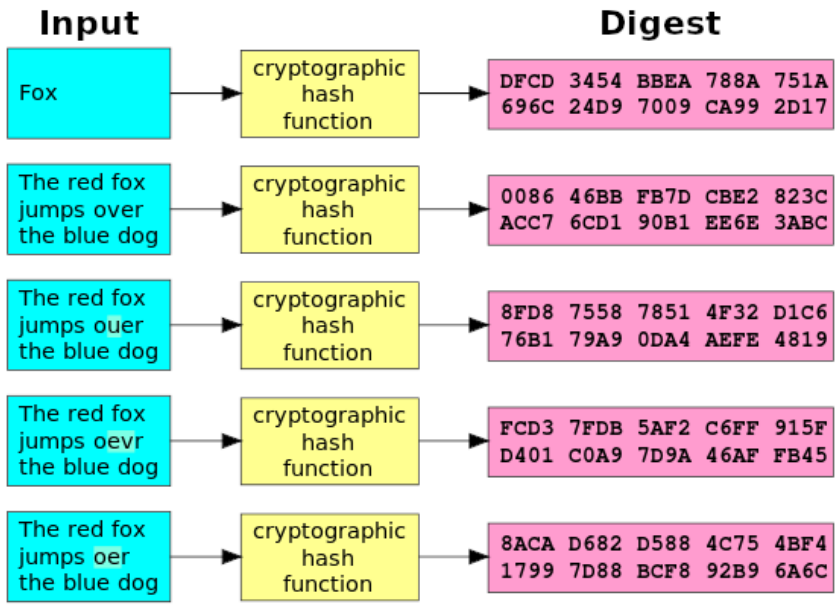


Trouver x tel que $H(x) = 1800$? Indices...

$2024^{4111} = 1798,\ 2024^{1981} = 1799,\ 2024^{3569} = 1801,\ 2024^{4523} = 1802$

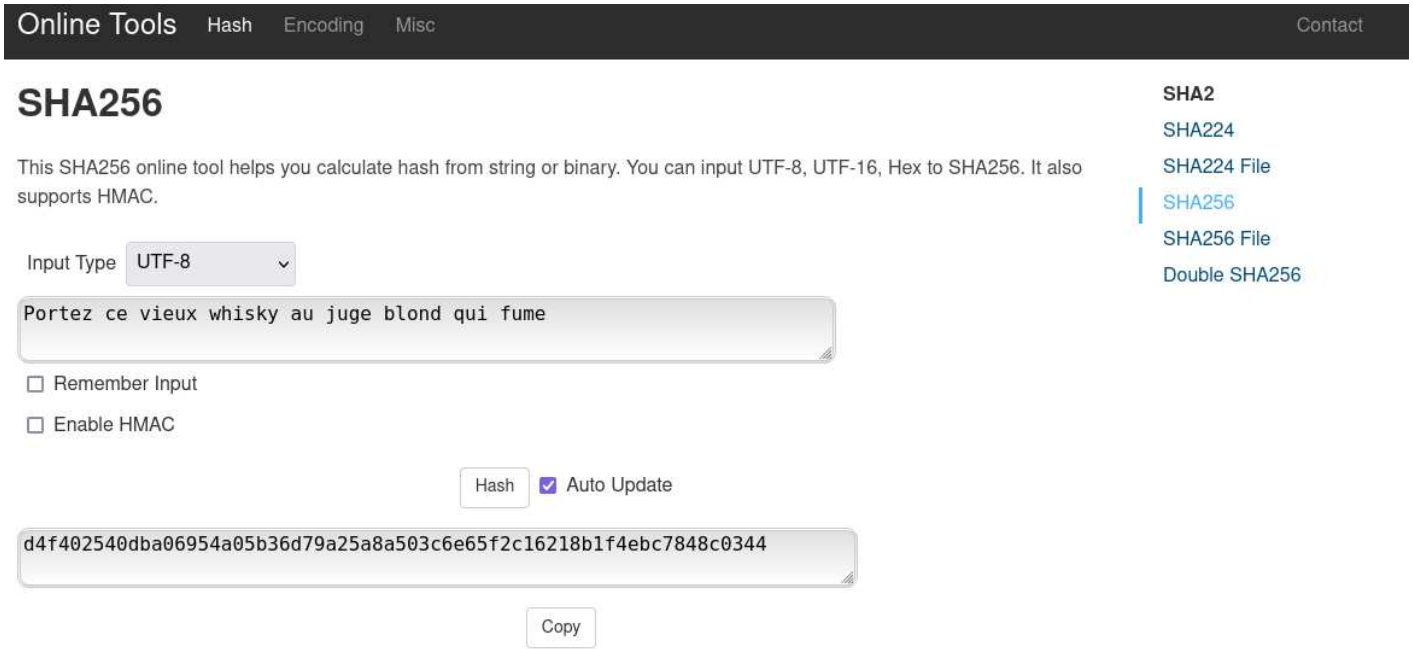
Une fonction de hachage

- associe à un texte x de taille arbitraire, une image $H(x)$ de taille fixe,
- est à sens unique : on ne peut pas "*raisonnablement*" retrouver x à partir de $y = H(x)$
- est résistante aux collisions : il est "*pratiquement impossible*" de trouver 2 textes $x \neq y$ ayant la même image $H(x) = H(y)$

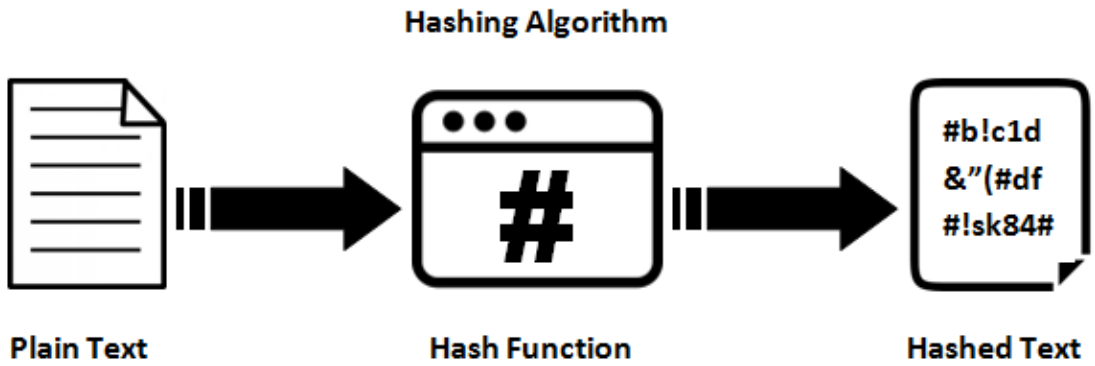


SHA-256

https://emn178.github.io/online-tools/sha256.html



- Si on change une lettre du texte x,
  le haché sera complètement différent



- Alice veut envoyer à Bob le texte x
- Alice signe le haché : $H(x)^{d_{A_s}}$
- Alice envoie à Bob les chiffrements de $x^{e_{B_c}}$ et du haché $H(x)^{e_{B_c}}$

- Jouer à pile ou face à distance
- Vérifier un vote électronique
- Téléchargements sécurisés
- Blockchain, Bitcoin, etc.

Jouer à pile ou face à distance

- Alice lance une pièce et hache le résultat avec un "nonce" (nombre aléatoire à usage unique)

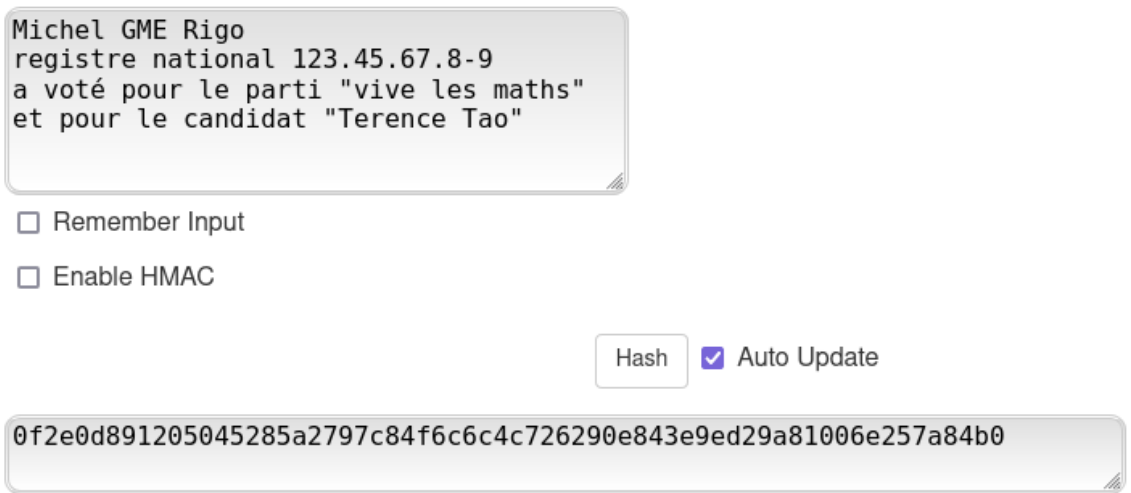
$$H(P/F, 16267366352) = y$$

- Alice envoie uniquement la valeur hachée y à Bob.
- Bob envoie son choix P/F à Alice.
- Alice révèle le résultat du jeu de pile ou face à Bob et lui révèle le nonce utilisé.
- Bob peut vérifier qu'Alice n'a pas triché.

Vérification d'un vote

Tout citoyen peut vérifier que son vote a bien été pris en compte

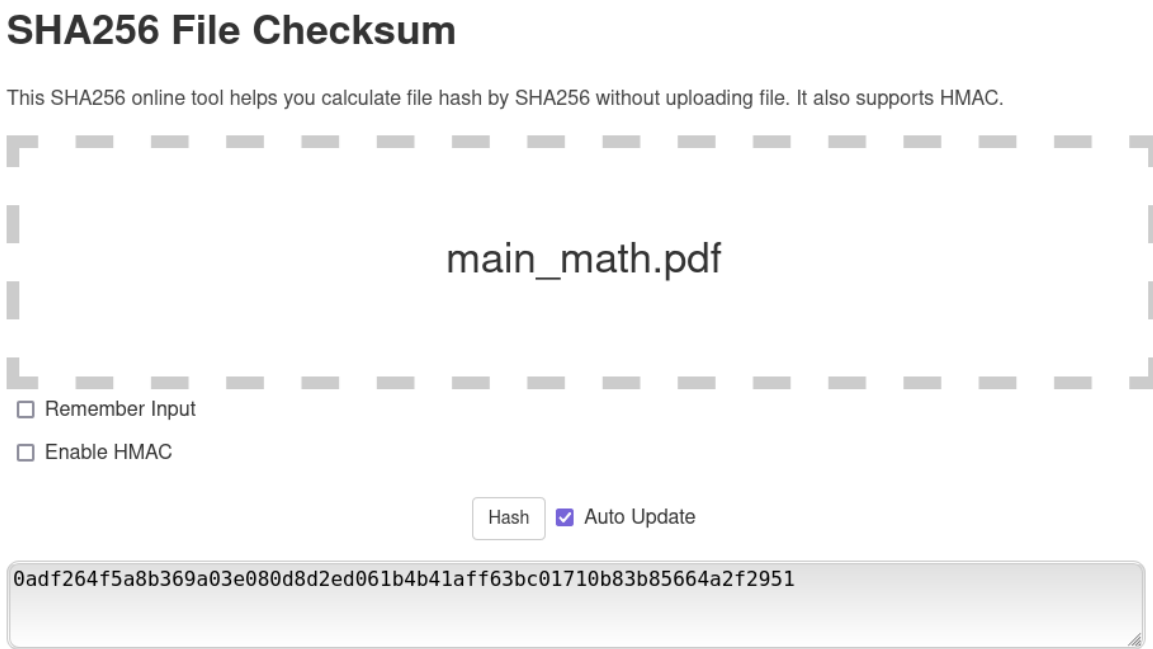
- Chaque vote produit un haché
- On publie la liste des hachés obtenus



Fichiers non altérés

- On télécharge une application (smartphone, ordinateur, . . .)
- On la compare à son haché — disponible sur un site officiel — pour savoir si elle n'a pas été altérée
- Résistance aux collisions, un pirate n'est pas en mesure de modifier raisonnablement l'application

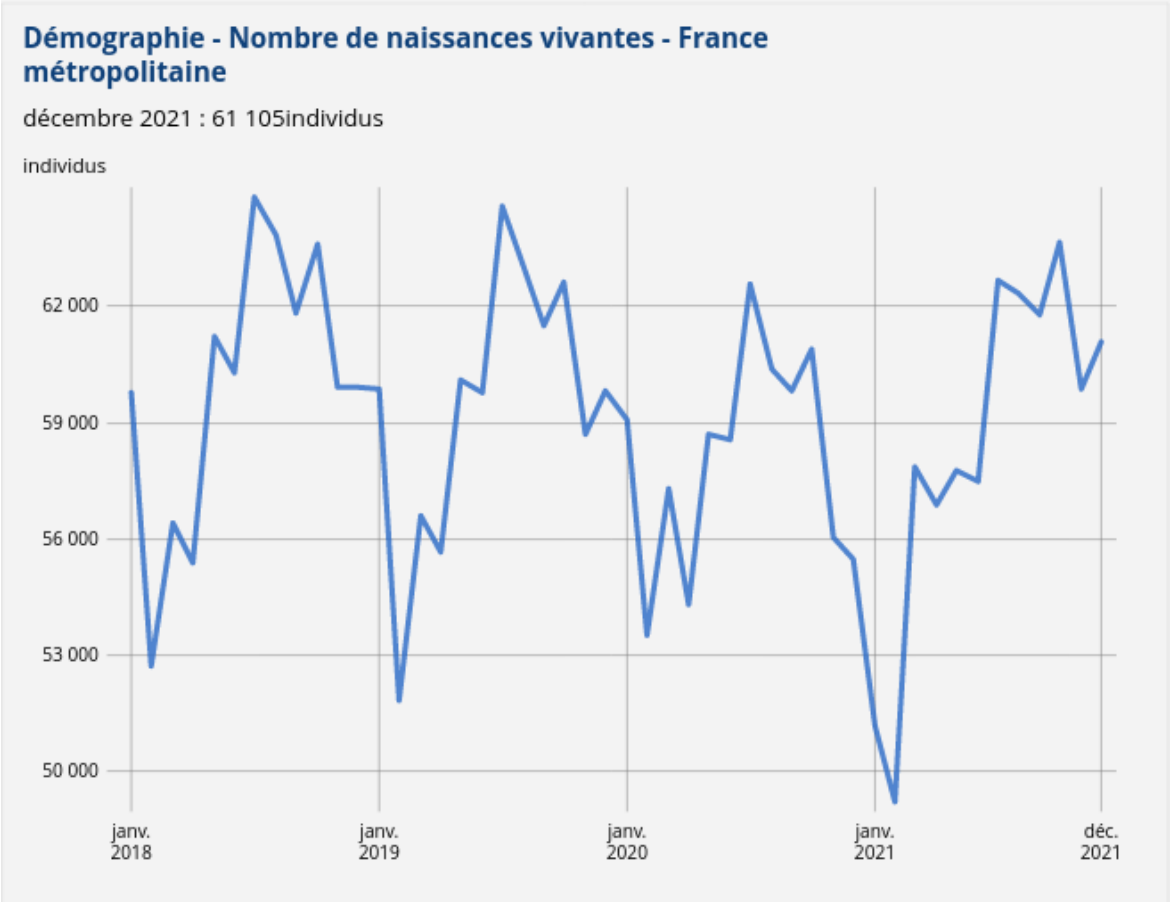
Par exemple, mes notes de cours
`http://www.discmath.ulg.ac.be/cours/main_math.pdf`



“MD5 (Message Digest 5) produces a 128-bit hash value and is no longer considered secure for cryptographic purposes due to its vulnerabilities.”

Le problème/paradoxe des anniversaires. . .

On suppose que les jours de naissance sont équiprobables tout au long de l'année



https://www.insee.fr/fr/statistiques/serie/000436391#Graphique

Supposons avoir des années de 365 jours, on s'intéresse à la date de naissance (jour / mois)

- Probabilité que, dans un groupe de 2 personnes, elles soient nées des jours (2 à 2) différents

$$\frac{364}{365}$$

- Probabilité que, dans un groupe de 2 personnes, au moins 2 soient nées le même jour

$$1 - \frac{364}{365} = \frac{1}{365}$$

Supposons avoir des années de 365 jours, on s'intéresse à la date de naissance (jour / mois)

- Probabilité que, dans un groupe de 3 personnes, elles soient nées des jours (2 à 2) différents

$$\frac{364}{365}\frac{363}{365}$$

- Probabilité que, dans un groupe de 3 personnes, au moins 2 soient nées le même jour

$$1 - \frac{364}{365}\frac{363}{365} = \frac{1093}{133225} \simeq 0,008$$

Supposons avoir des années de 365 jours, on s'intéresse à la date de naissance (jour / mois)

- Probabilité que, dans un groupe de 4 personnes, elles soient nées des jours (2 à 2) différents

$$\frac{364}{365}\frac{363}{365}\frac{362}{365}$$

- Probabilité que, dans un groupe de 4 personnes, au moins 2 soient nées le même jour

$$1 - \frac{364}{365}\frac{363}{365}\frac{362}{365} = \frac{795341}{48627125} \simeq 0,016$$

Supposons avoir des années de 365 jours, on s'intéresse à la date de naissance (jour / mois)

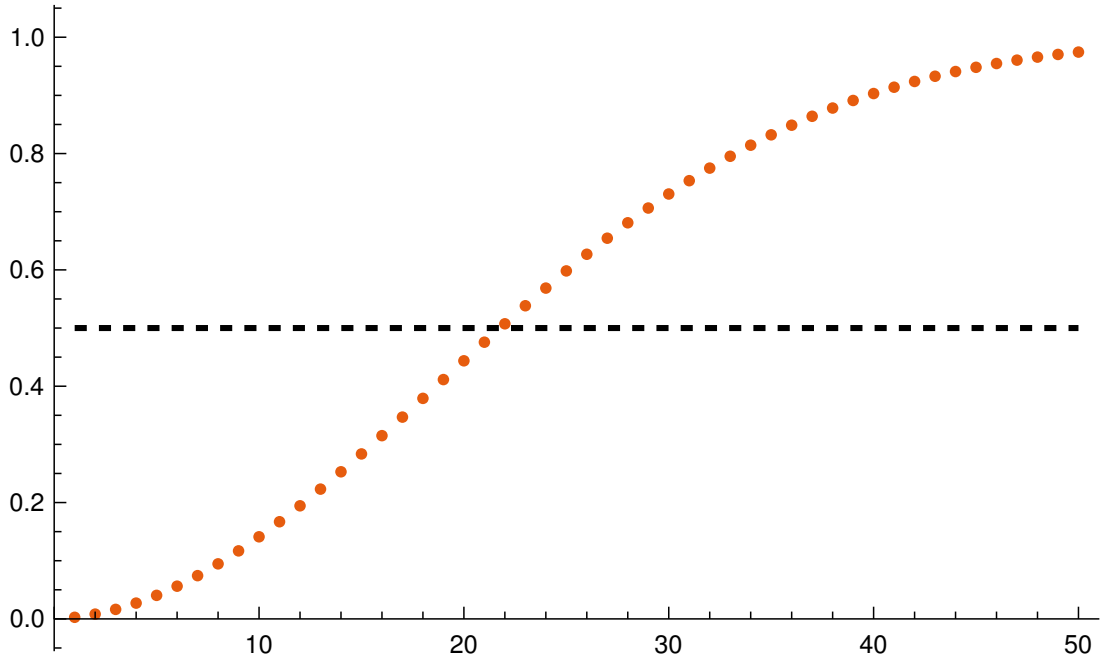
- Probabilité que, dans un groupe de $n \leq 365$ personnes, elles soient nées des jours (2 à 2) différents

$$\prod_{i=1}^{n-1} \frac{365 - i}{365}$$

- Probabilité que, dans un groupe de n personnes, au moins 2 soient nées le même jour

$$1 - \frac{1}{365^{n-1}} \prod_{i=1}^{n-1} (365 - i)$$

Probabilité que, dans un groupe de n personnes,
au moins 2 soient nées le même jour :

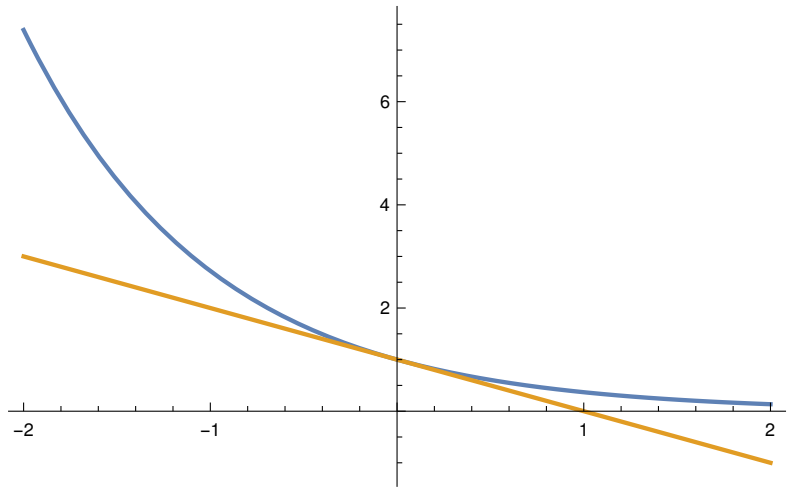


Avec 23 personnes, la probabilité dépasse les 50%

Reprenons MD5 pour lequel $H(x)$ peut prendre 2^{128} valeurs

Interlude analytique

$$\forall x \in \mathbb{R},\ 1 - x \leq e^{-x}$$



- étude “classique” de la fonction $e^{-x} + x - 1$ et vérifier ≥ 0
- ou, e^{-x} est une fonction convexe (SSI son graphique est au-dessus de chacune de ses tangentes)

Probabilité que, dans un groupe de n personnes, au moins 2 soient nées le même jour

$$1 - \frac{1}{365^{n-1}} \prod_{i=1}^{n-1} (365 - i)$$

Probabilité que, dans un groupe de n images par H, au moins 2 éléments prennent la même valeur (collision)

$$\begin{aligned}
1 - \frac{1}{(2^{128})^{n-1}} \prod_{i=1}^{n-1} (2^{128} - i) &= 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^{128}}\right) \\
&\geq 1 - \prod_{i=1}^{n-1} e^{-i/2^{128}} \\
&\geq 1 - e^{-(1+2+\cdots+(n-1))/2^{128}} \\
&\geq 1 - e^{-(n-1)n/2^{129}}
\end{aligned}$$

pour $n = 2^{64}$, $p \geq 0,39$ et pour $n = 2^{65}$, $p \geq 0,86$.

Probabilité que, dans un groupe de n personnes, au moins 2 soient nées le même jour

$$1 - \frac{1}{365^{n-1}} \prod_{i=1}^{n-1} (365 - i)$$

Probabilité que, dans un groupe de n images par H, au moins 2 éléments prennent la même valeur (collision)

$$\begin{aligned}
1 - \frac{1}{(2^{128})^{n-1}} \prod_{i=1}^{n-1} (2^{128} - i) &= 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^{128}}\right) \\
&\geq 1 - \prod_{i=1}^{n-1} e^{-i/2^{128}} \\
&\geq 1 - e^{-(1+2+\cdots+(n-1))/2^{128}} \\
&\geq 1 - e^{-(n-1)n/2^{129}}
\end{aligned}$$

pour $n = 2^{64}$, $p \geq 0,39$ et pour $n = 2^{65}$, $p \geq 0,86$.

Pour finir...

But how does bitcoin actually work?
`https://www.youtube.com/watch?v=bBC-nXj3Ng4`

- Système décentralisé
- Une liste de transactions est écrite dans un bloc, pour former une chaîne de blocs (blockchain)

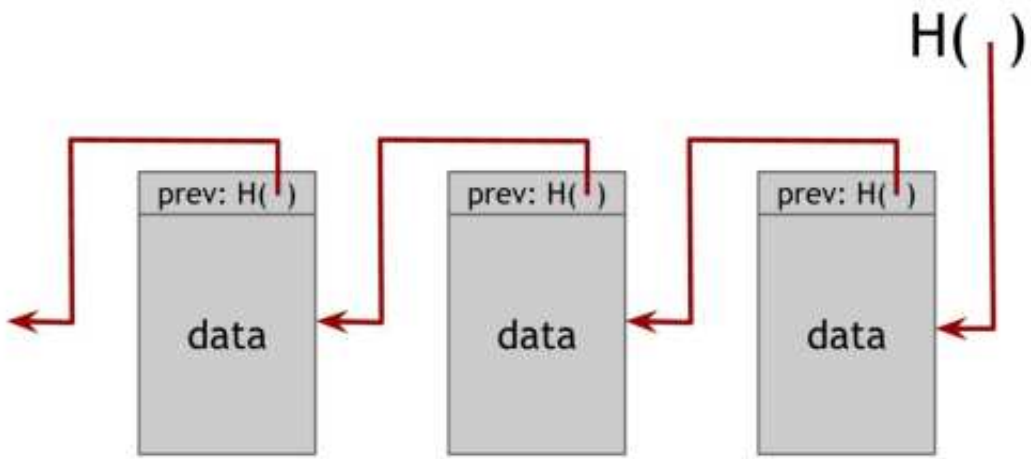
Pour de nouvelles transactions
Travail du *mineur* : trouver x (proof of work) tel que

$$\left.\begin{array}{|ll|}\hline \text{index bloc précédent} & \\ H(\text{bloc précédent}) & \\ \text{info. temporelle} & \\ Alice\ (sign.) & -20 \\ Bob\ (sign.) & +10 \\ Oscar\ (sign.) & -30 \\ Eve\ (sign.) & +40 \\ x \quad (nonce) & \\ \hline \end{array}\right\} \xrightarrow{H} \underbrace{00000\cdots000}_{\text{par ex. 60 zéros}}101010101$$

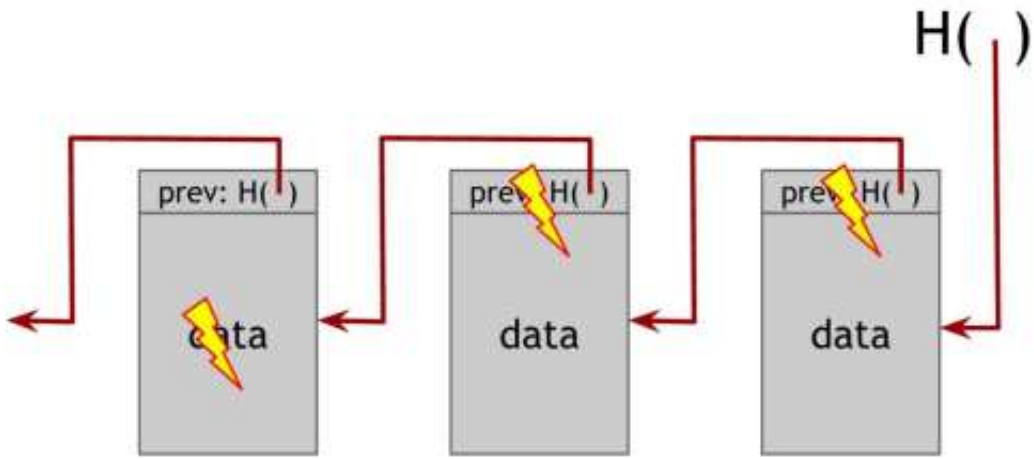
on peut ajuster le niveau de difficulté : $2^{256-60}/2^{256} = 1/2^{60} \sim 10^{-18}$

Le mineur crée un nouveau bloc qui doit être validé pour être ajouté à la chaîne ; il reçoit une récompense
Le travail doit être coûteux, ceci garantit la sécurité

Un pointeur de hachage ; indique où se trouve le bloc précédent
ET un haché de l'information pointée

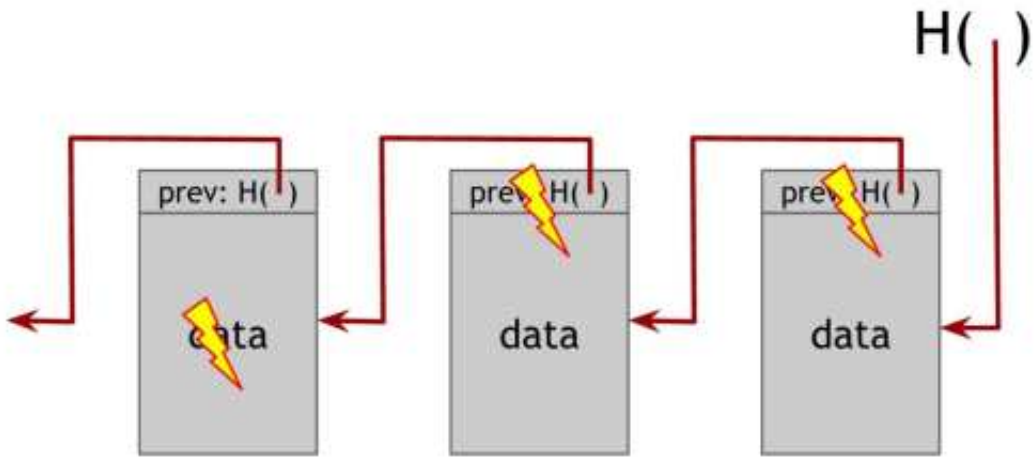


Un pointeur de hachage ; indique où se trouve le bloc précédent
ET un haché de l'information pointée



Si on falsifie la liste des transactions, cela modifie le haché du bloc et donc tout le reste de la chaîne. . .
Créer une nouvelle chaîne alternative est trop coûteux !

Un pointeur de hachage ; indique où se trouve le bloc précédent
ET un haché de l'information pointée



Si on falsifie la liste des transactions, cela modifie le haché du bloc et donc tout le reste de la chaîne...
Créer une nouvelle chaîne alternative est trop coûteux !

Je ne vous parlerai pas de spéculation, etc.

ni des aspects écologiques

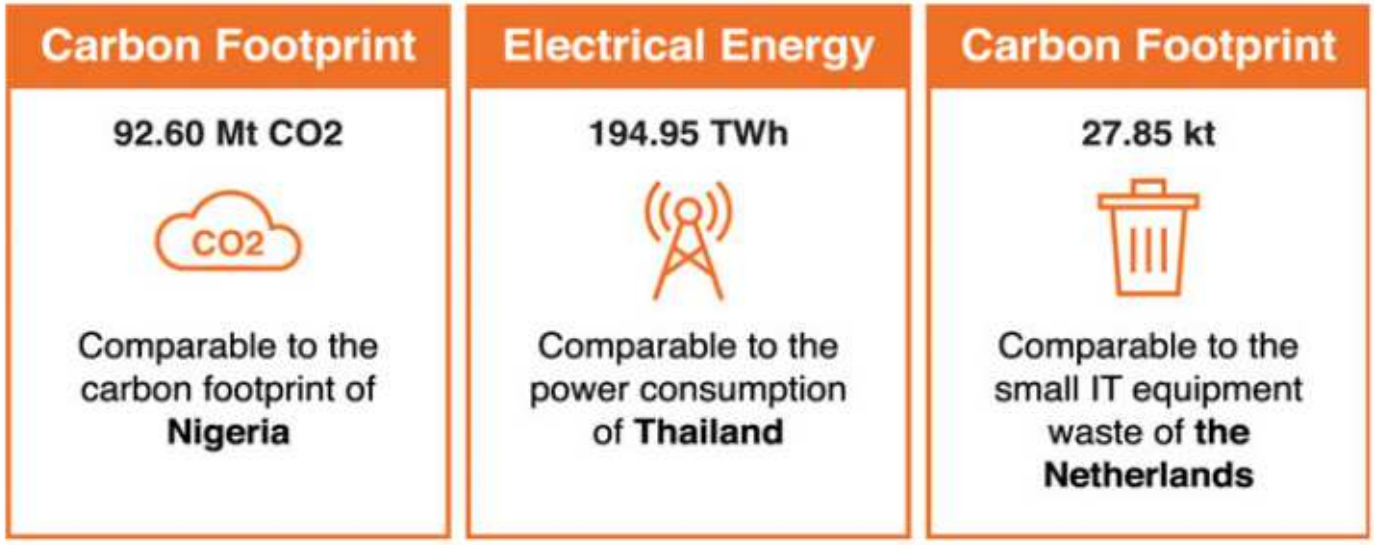
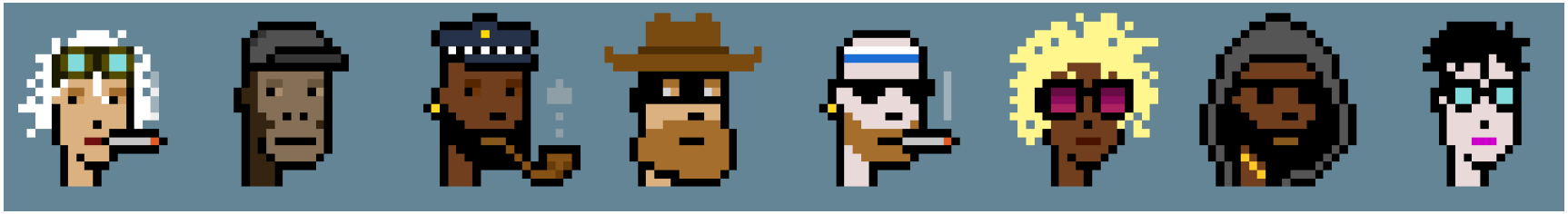


Fig. 5 Total annualized footprints (Carbon/Electricity/Waste) as of January 2022 (*Source* Digiconomist)

Une même technologie pour les NFT (non-fungible token)



`https://cryptopunks.app/`

- On crée une “oeuvre”
- On crée un bloc avec les informations sur celle-ci (un haché, son créateur, son historique,. . .) ; elle ne peut plus être altérée
- On crée une chaîne si l’oeuvre est revendue, etc.

Largest Sales

See all top sales

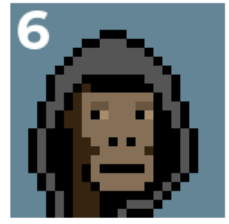
#5822
8KΞ ($23.7M)
Feb 12, 2022

#7804
4.85KΞ ($16.42M)
Mar 20, 2024

#3100
4.5KΞ ($16.03M)
Mar 04, 2024

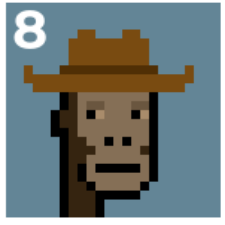
#7804
4.2KΞ ($7.57M)
Mar 11, 2021

#3100
4.2KΞ ($7.58M)
Mar 11, 2021



#2924
3.3KΞ ($4.45M)
Sep 28, 2022

#4156
2.69KΞ ($3.31M)
Jul 15, 2022



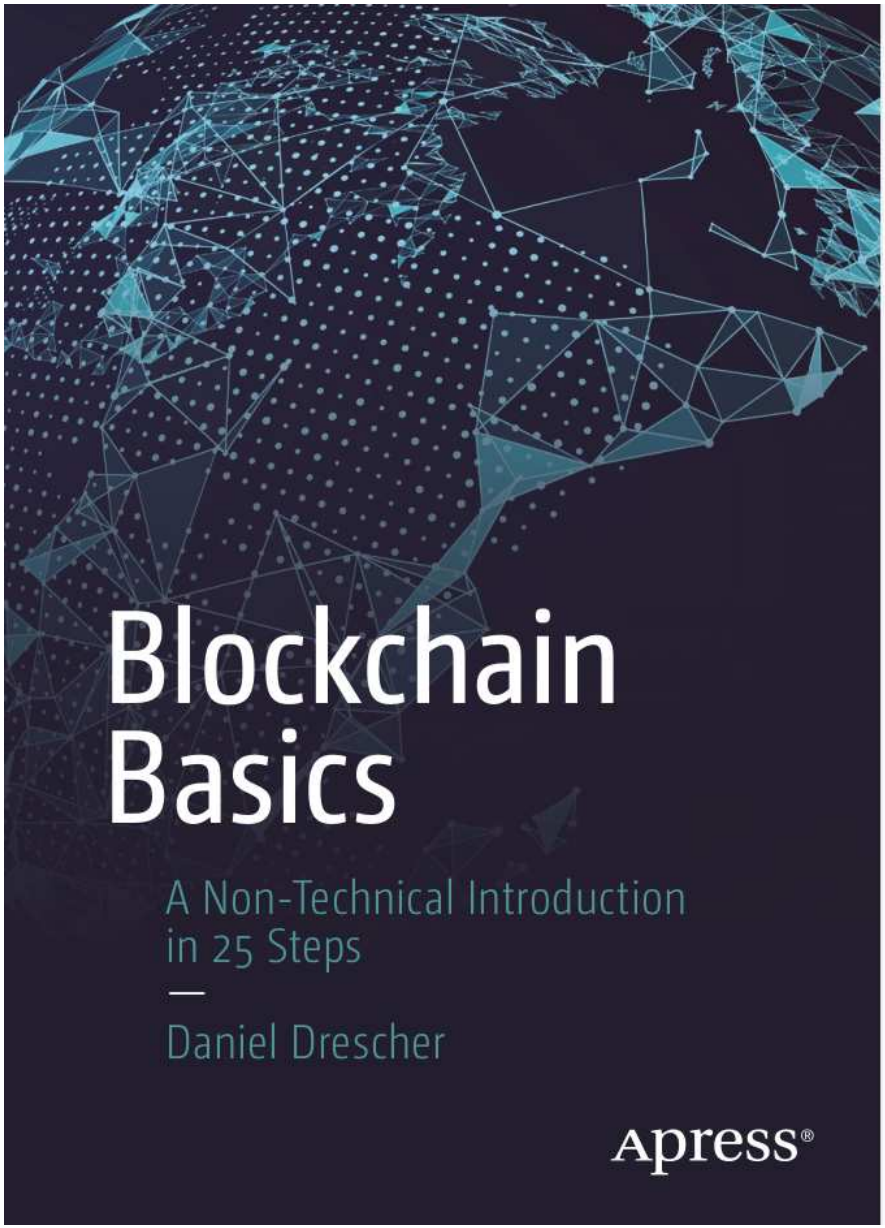
#5577
2.5KΞ ($7.7M)
Feb 09, 2022

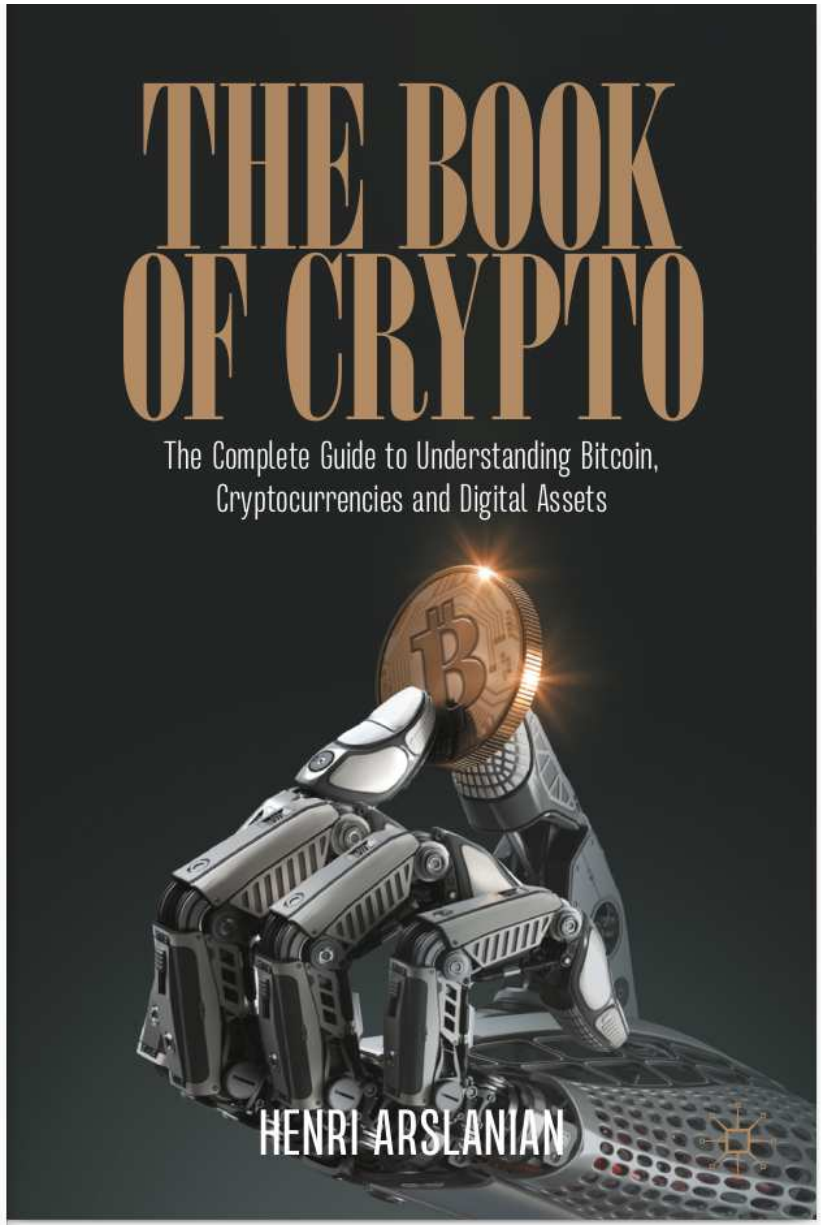
#4464
2.5KΞ ($2.62M)
Jul 12, 2022

#4156
2.5KΞ ($10.26M)
Dec 09, 2021

#5217
2.25KΞ ($5.45M)
Jul 30, 2021

#8857
2KΞ ($6.63M)
Sep 11, 2021


Blockchain
Basics
A Non-Technical Introduction
in 25 Steps
Daniel Drescher
Apress®


THE BOOK
OF CRYPTO
The Complete Guide to Understanding Bitcoin,
Cryptocurrencies and Digital Assets
HENRI ARSLANIAN