Primalité et factorisation
Les clés de RSA

Alexandra Bruasse-Bac

ESIL - 2002-2003

Primalité

Primalité

But :

rechercher des nombres premiers

Primalité

But :

rechercher des nombres premiers

Deux philosophies :

Primalité

But :

rechercher des nombres premiers

Deux philosophies :

- tests de primalité (probabiliste)

Primalité

But :

rechercher des nombres premiers

Deux philosophies :

- tests de primalité (probabiliste)
- algorithme de primalité (déterministe)

Primalité

But :

rechercher des nombres premiers

Deux philosophies :

- tests de primalité (probabiliste)
- algorithme de primalité (déterministe)

Critère :

$\longrightarrow$ complexité

Crible d'Eratosthene (algorithme)

Algorithme :

Tableau prime[1..n] initialisé à $vrai$

- Tant que $i < n$ et prime[n]
  - Si prime[i] alors pour $j > 1$
    prime[$j \cdot i$]=$faux$
  - i $\leftarrow$ i+1

Si prime[n] est faux : $i - 1$ est un facteur de n.

Crible d'Eratosthene (algorithme)

```
int prime[n+1];
int i,j;
/* Initialisation */
for(i=2;i<=n;i++)
  prime[i]=1;

i=2;
while((i<n) && prime[n])
{
  if(prime[i]) /* on vient de trouver un nouveau premier */
  {
    for(j=2*i;j<=n;j+=i)
      prime[j]=0;
  };
  i++;
};
if(prime[n])
  printf("%d est premier\n", n);
else
  printf("%d n'est pas premier - facteur : %d\n", n,i-1);
```

Crible d'Eratosthene (algorithme)

- algorithme le plus simple

Crible d'Eratosthene (algorithme)

- algorithme le plus simple
- négatif : long ...

Crible d'Eratosthene (algorithme)

- algorithme le plus simple
- négatif : long ...
- positif : fournit une factorisation

Crible d'Eratosthene (algorithme)

- algorithme le plus simple
- négatif : long ...
- positif : fournit une factorisation
- travail d'équipe :
  - chercher les premiers p tel que $p < \sqrt{n}$ (Eratosthene)
  - tester si $p|n$

Ordres de grandeur pour RSA

On peut montrer :

$$\text{il faut au moins } \frac{\sqrt{n}}{\log \sqrt{n}} \text{ divisions}$$

Ordres de grandeur pour RSA

On peut montrer :

$$\text{il faut au moins } \frac{\sqrt{n}}{\log \sqrt{n}} \text{ divisions}$$

Pour RSA :

$$n \text{ a } 256 \text{ bits} \quad : n \geqslant 10^{75}$$

Ordres de grandeur pour RSA

On peut montrer :

$$\text{il faut au moins } \frac{\sqrt{n}}{\log \sqrt{n}} \text{ divisions}$$

Pour RSA :

$$n \text{ a } 256 \text{ bits} \quad : n \geqslant 10^{75}$$

Il faut au moins :

$$0.36 \cdot 10^{36} \text{ divisions}$$

Test de Fermat

Petit théorème de Fermat :

Si a et n sont premiers entre eux ($\mathrm{pgcd}(a, n) = 1$)

$$a^{\varphi(n)} \equiv 1 \ [n]$$

Test de Fermat

Petit théorème de Fermat :

Si a et n sont premiers entre eux ($\mathrm{pgcd}(a, n) = 1$)

$$a^{\varphi(n)} \equiv 1 \ [n]$$

Fonction d'euler :

$$\varphi(n) = \mathrm{Card}\,\{p \in \{1 \ldots n\};\ \mathrm{pgcd}(p, n) = 1\}$$

Test de Fermat

Petit théorème de Fermat :

Si a et n sont premiers entre eux ($\mathrm{pgcd}(a, n) = 1$)

$$a^{\varphi(n)} \equiv 1 \ [n]$$

Fonction d'euler :

$$\varphi(n) = \mathrm{Card}\,\{p \in \{1 \ldots n\};\ \mathrm{pgcd}(p, n) = 1\}$$

Propriété :

si p est premier, $\varphi(p) = p - 1$

Test de Fermat

Algorithme :

- tirer au hasard a tel que $1 < a < n$
  - si $\mathrm{pgcd}(a, n) \neq 1$: (a facteur de n)
    $\longrightarrow$ n pas premier
  - sinon, si $a^{n-1} \not\equiv 1\ [n]$
    $\longrightarrow$ n pas premier
  - sinon,
    $\longrightarrow$ n peut-être premier ...

Test de Fermat

Si n pas premier :

finit-on toujours par le montrer ?

Test de Fermat

Si n pas premier :

finit-on toujours par le montrer ?

Il existe des n non premiers tels que pour tout a avec $\mathrm{pgcd}(a, n) = 1$:

$$a^{n-1} \equiv 1 \ [n]$$

Test de Fermat

Si n pas premier :

finit-on toujours par le montrer ?

Il existe des n non premiers tels que pour tout a avec $\mathrm{pgcd}(a, n) = 1$:

$$a^{n-1} \equiv 1 \ [n]$$

$\rightarrow$ nombres de Carmichael

Test de Fermat

Si n pas premier :

finit-on toujours par le montrer ?

Il existe des n non premiers tels que pour tout a avec $\mathrm{pgcd}(a, n) = 1$:

$$a^{n-1} \equiv 1 \ [n]$$

$\rightarrow$ nombres de Carmichael

Exemple : 561

Test de Miller-Rabin

Test de Fermat “amélioré”

On note $n - 1 = 2^s \cdot d$

Test de Miller-Rabin

Test de Fermat “amélioré”

On note $n - 1 = 2^s \cdot d$

Théorème

Si n et premier et a tel que $a^n = 1$, alors :

- soit

$$a^d \equiv 1 \ [n]$$

- soit il existe $r \in \{0, 1, \ldots, s-1\}$

$$a^{2^r s} \equiv -1 \ [n]$$

Test de Miller-Rabin

Algorithme :

Calculer d et s

- tirer au hasard a tel que $1 < a < n$
  - si $\mathrm{pgcd}(a, n) \neq 1$: (a facteur de n)
    $\rightarrow$ n pas premier
  - sinon, si $a^d \not\equiv 1\ [n]$ et $\forall r \in \{0, 1, \ldots, s-1\}$, $a^{2^r s} \not\equiv -1\ [n]$
    $\rightarrow$ n pas premier
  - sinon,
    $\rightarrow$ n peut-être premier ...

Test de Miller-Rabin

Si n n'est pas premier :

probabilité que a passe les tests quand-même :

$$\frac{1}{4}$$

Test de Miller-Rabin

Si n n'est pas premier :

probabilité que a passe les tests quand-même :

$$\frac{1}{4}$$

Tester si n est premier :

on itère jusqu'à avoir une probabilité suffisante ...

Test de Solovay-Strassen

Idée différente : symbole de Jacobi.

Test de Solovay-Strassen

Idée différente : symbole de Jacobi.

Symbole de Jacobi :

n impair

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } n \mid a \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{Z}/n\mathbb{Z} \\ -1 & \text{sinon} \end{cases}$$

Test de Solovay-Strassen

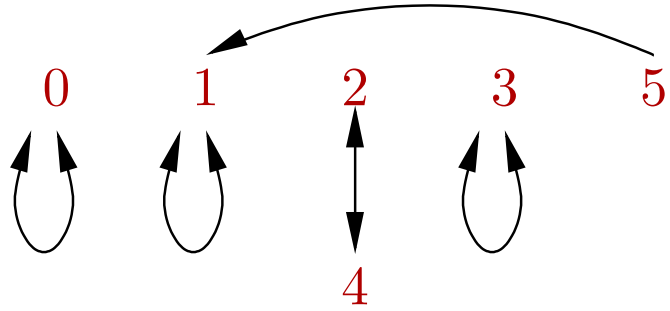
Idée différente : symbole de Jacobi.

Symbole de Jacobi :

n impair

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } n \mid a \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{Z}/n\mathbb{Z} \\ -1 & \text{sinon} \end{cases}$$

Exemple : dans $\mathbb{Z}/6\mathbb{Z}$



Test de Solovay-Strassen

Idée différente : symbole de Jacobi.

Symbole de Jacobi :

n impair

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } n \mid a \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{Z}/n\mathbb{Z} \\ -1 & \text{sinon} \end{cases}$$

Propriété :

si n premier :

$$\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \ [n]$$

Test de Solovay-Strassen

- On a :

$$\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right) \qquad \left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$$

Test de Solovay-Strassen

- On a :

$$\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right) \qquad \left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$$

- Si $a_1 \equiv a_2 \ [n]$ alors :

$$\left(\frac{a_1}{n}\right) = \left(\frac{a_2}{n}\right)$$

Test de Solovay-Strassen

- On a :

$$\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right) \qquad \left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$$

- Si $a_1 \equiv a_2\ [n]$ alors :

$$\left(\frac{a_1}{n}\right) = \left(\frac{a_2}{n}\right)$$

- Si $n \equiv \pm 1\ [8]$: Si $n \equiv \pm 3\ [8]$:

$$\left(\frac{2}{n}\right) = 1 \qquad \left(\frac{2}{n}\right) = -1$$

Test de Solovay-Strassen

- Si $a \equiv n \equiv 3\ [4]$:

$$\left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right)$$

Sinon :

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$$

Test de Solovay-Strassen

- Si $a \equiv n \equiv 3\ [4]$:

$$\left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right)$$

Sinon :

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$$

- On a :

$$\left(\frac{1}{n}\right) = 1 \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{p-1}{2}}$$

Test de Solovay-Strassen

- Si $a \equiv n \equiv 3\ [4]$:

$$\left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right)$$

Sinon :

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$$

- On a :

$$\left(\frac{1}{n}\right) = 1 \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{p-1}{2}}$$

Exemples :

$$\left(\frac{5}{6}\right)$$

Test de Solovay-Strassen

- Si $a \equiv n \equiv 3\ [4]$:

$$\left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right)$$

Sinon :

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$$

- On a :

$$\left(\frac{1}{n}\right) = 1 \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{p-1}{2}}$$

Exemples :

$$\left(\frac{12}{253}\right) \neq 12^{126}\ [253]$$

Test de Solovay-Strassen

- Si $a \equiv n \equiv 3\ [4]$:

$$\left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right)$$

Sinon :

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$$

- On a :

$$\left(\frac{1}{n}\right) = 1 \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{p-1}{2}}$$

Exemples :

$$\left(\frac{12}{257}\right) = 12^{128}\ [257]$$

Test de Solovay-Strassen

Si n n'est pas premier :

probabilité que a passe les tests quand-même :

$$\frac{1}{2}$$

Algorithme de primalité

Théorème

p est premier si et seulement si :

étant donné a premier avec p :

$$(X-a)^p = X^p - a^p$$

Complexités - Bilan

- Eratosthene :

$$\frac{\sqrt{n}}{\log(\sqrt{n})} \text{ operations}$$

Complexités - Bilan

- Eratosthene :

$$\frac{\sqrt{n}}{\log(\sqrt{n})} \text{ operations}$$

- Miller-Rabin, Solovay-Strassen : (N étapes)

$$\mathcal{O}(N \cdot \log(n)) \text{ operations}$$

Complexités - Bilan

- Eratosthene :

$$\frac{\sqrt{n}}{\log(\sqrt{n})} \text{ operations}$$

- Miller-Rabin, Solovay-Strassen : (N étapes)

$$\mathcal{O}(N \cdot \log(n)) \text{ operations}$$

- Algorithmes de primalité :

$$(\log(n))^{\mathcal{O}(\log(\log(\log n)))}$$

Complexités - Bilan

- Eratosthene :

$$\frac{\sqrt{n}}{\log(\sqrt{n})} \text{ operations}$$

- Miller-Rabin, Solovay-Strassen : (N étapes)

$$\mathcal{O}(N \cdot \log(n)) \text{ operations}$$

- Algorithmes de primalité :

$$(\log(n))^{\mathcal{O}(\log(\log(\log n)))}$$

$\rightarrow$ Les tests de primalité ne fournissent pas de factorisation

Factorisation

La méthode $p-1$ de Pollard

Marche bien pour des entiers n lisses.

La méthode $p-1$ de Pollard

Marche bien pour des entiers n lisses.

n est lisse si

$n-1$ n'a que des petits facteurs

La méthode $p-1$ de Pollard

Marche bien pour des entiers n lisses.

n est lisse si

$n-1$ n'a que des petits facteurs

Exemple :

257 est lisse (même très lisse) ...

La méthode $p-1$ de Pollard

Si p est un facteur premier de n.

Si $p-1 \mid q$. Petit théorème de Fermat :

$$a^q \equiv 1 \ [p]$$

La méthode $p-1$ de Pollard

Si p est un facteur premier de n.

Si $p-1 \mid q$. Petit théorème de Fermat :

$$a^q \equiv 1 \ [p]$$

Donc

$$p \mid n$$
$$p \mid a^q - 1$$

La méthode $p-1$ de Pollard

Si p est un facteur premier de n.

Si $p-1 \mid q$. Petit théorème de Fermat :

$$a^q \equiv 1 \ [p]$$

Donc

$$p \mid n$$
$$p \mid a^q - 1$$

Si n ne divise pas $a^q - 1$,

$\mathrm{pgcd}(a^q - 1, n)$ facteur propre de n

La méthode $p-1$ de Pollard

$\mathbb{P}$ ensemble des nombres premiers

Comment choisir q ?

La méthode $p-1$ de Pollard

$\mathbb{P}$ ensemble des nombres premiers

Comment choisir q ?

On fixe $B \in \mathbb{N}$

$$q = \prod_{\substack{p \in \mathbb{P} \\ p^e \leqslant B}} p^e$$

La méthode $p-1$ de Pollard

Algorithme :

- Choisir B
- Calculer q
- Choisir $a \in \{2 \dots n-1\}$:
  - Si $\mathrm{pgcd}(a,n) \neq 1$, alors a facteur de n
  - Sinon,

$$\mathrm{pgcd}(a^q - 1, n) \text{ facteur de } n$$

La méthode $p-1$ de Pollard

Exemple : $n = 1241143$

La méthode $p-1$ de Pollard

Exemple : $n = 1241143$

On pose $B = 7$ et $a = 2$

$$q = 4 \cdot 3 \cdot 5 \cdot 7 = 420$$

$$2^{420} - 1 \ [1241143] = 1113519$$

$$\mathrm{pgcd}(1113519, 1241143) = 1$$

La méthode $p-1$ de Pollard

Exemple : $n = 1241143$

On pose $B = 13$ et $a = 2$

$$q = 8 \cdot 9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 360360$$

$$2^{360360} - 1 \ [1241143] = 861525$$

$$\text{pgcd}(861525, 1241143) = 547$$

$$1241143 = 547 \cdot 2269$$

Le crible quadratique

Idée : trouver x et y tels que

$$x^2 \equiv y^2 \ [n]$$

mais

$$x \not\equiv \pm y \ [n]$$

Le crible quadratique

Idée : trouver x et y tels que

$$x^2 \equiv y^2 \ [n]$$

mais

$$x \not\equiv \pm y \ [n]$$

$n \mid x^2 - y^2$ mais $n \nmid (x \pm y)$

$\mathrm{pgcd}(x - y, n)$ diviseur de n

Le crible quadratique

On pose :

$$m = \lceil \sqrt{n} \rceil$$

$$P(X) = (X + m)^2 - n$$

Le crible quadratique

On pose :

$$m = \lceil \sqrt{n} \rceil$$

$$P(X) = (X + m)^2 - n$$

Exemple de $n = 7429$

Le crible quadratique

On pose :

$$m = \lceil \sqrt{n} \rceil$$

$$P(X) = (X + m)^2 - n$$

Exemple de $n = 7429$

$$P(X) = (X + 86)^2 - 7429$$

On a :

$$P(-3) \quad = \quad 83^2 - 7429 \quad =$$

Le crible quadratique

On a :

$$P(-3) \quad = \quad 83^2 - 7429 \quad = \quad -540 \quad =$$

On a :

$$P(-3) \quad = \quad 83^2 - 7429 \quad = \quad -540 \quad = \quad -1 \cdot 2^2 \cdot 3^3 \cdot 5$$

On a :

$$\begin{array}{lllll} P(-3) & = & 83^2 - 7429 & = & -540 & = & -1 \cdot 2^2 \cdot 3^3 \cdot 5 \\ P(1) & = & 87^2 - 7429 & = & 140 & = & 2^2 \cdot 5 \cdot 7 \end{array}$$

On a :

$$\begin{array}{lllll} P(-3) & = & 83^2 - 7429 & = & -540 & = & -1 \cdot 2^2 \cdot 3^3 \cdot 5 \\ P(1) & = & 87^2 - 7429 & = & 140 & = & 2^2 \cdot 5 \cdot 7 \\ P(2) & = & 88^2 - 7429 & = & 315 & = & 3^2 \cdot 5 \cdot 7 \end{array}$$

On a :

$$\begin{array}{lllll} P(-3) & = & 83^2 - 7429 & = & -540 & = & -1 \cdot 2^2 \cdot 3^3 \cdot 5 \\ P(1) & = & 87^2 - 7429 & = & 140 & = & 2^2 \cdot 5 \cdot 7 \\ P(2) & = & 88^2 - 7429 & = & 315 & = & 3^2 \cdot 5 \cdot 7 \end{array}$$

D'où :

$$\begin{array}{lll} 83^2 & \equiv & -1 \cdot 2^2 \cdot 3^3 \cdot 5 \mod 7429 \\ 87^2 & \equiv & 2^2 \cdot 5 \cdot 7 \mod 7429 \\ 88^2 & \equiv & 3^2 \cdot 5 \cdot 7 \mod 7429 \end{array}$$

On a :

$$\begin{array}{lllll} P(-3) & = & 83^2 - 7429 & = & -540 & = & -1 \cdot 2^2 \cdot 3^3 \cdot 5 \\ P(1) & = & 87^2 - 7429 & = & 140 & = & 2^2 \cdot 5 \cdot 7 \\ P(2) & = & 88^2 - 7429 & = & 315 & = & 3^2 \cdot 5 \cdot 7 \end{array}$$

D'où :

$$\begin{aligned} 83^2 &\equiv -1 \cdot 2^2 \cdot 3^3 \cdot 5 \mod 7429 \\ 87^2 &\equiv 2^2 \cdot 5 \cdot 7 \mod 7429 \\ 88^2 &\equiv 3^2 \cdot 5 \cdot 7 \mod 7429 \end{aligned}$$

$$(\underbrace{87 \cdot 88}_{7656})^2 \equiv (\underbrace{2 \cdot 3 \cdot 5 \cdot 7}_{210})^2 \mod 7429$$

Le crible quadratique

$$\left.\begin{array}{l} x = 87 \cdot 88 \mod n = 227 \\ y = 2 \cdot 3 \cdot 5 \cdot 7 = 210 \end{array}\right\} \rightarrow \left\{\begin{array}{l} x + y = 437 \\ x - y = 17 \end{array}\right.$$

Le crible quadratique

$$\left.\begin{array}{l} x = 87 \cdot 88 \mod n = 227 \\ y = 2 \cdot 3 \cdot 5 \cdot 7 = 210 \end{array}\right\} \rightarrow \left\{\begin{array}{l} x + y = 437 \\ x - y = 17 \end{array}\right.$$

$$\mathrm{pgcd}(7429, 437) = \mathrm{pgcd}(7429, 17) = 17$$

Le crible quadratique

On choisit $B \geqslant 0 \rightarrow$ entiers B lisses

On choisit $B \geqslant 0 \rightarrow$ entiers B lisses
Cible :

$$S = \{-C, -(C-1), \ldots, 0, \ldots, C-1, C\}$$

Le crible quadratique

On choisit $B \geqslant 0 \rightarrow$ entiers B lisses
Cible :

$$S = \{-C, -(C-1), \ldots, 0, \ldots, C-1, C\}$$

On chercher les $s \in S$:

$P(s)$ est B-lisse

On choisit $B \geqslant 0 \rightarrow$ entiers B lisses
Cible :

$$S = \{-C, -(C-1), \ldots, 0, \ldots, C-1, C\}$$

On chercher les $s \in S$:

$P(s)$ est B-lisse

$$\begin{array}{lllll} P(-3) & = & 83^2 - 7429 & = & -540 & = & -1 \cdot 2^2 \cdot 3^3 \cdot 5 \\ P(1) & = & 87^2 - 7429 & = & 140 & = & 2^2 \cdot 5 \cdot 7 \\ P(2) & = & 88^2 - 7429 & = & 315 & = & 3^2 \cdot 5 \cdot 7 \end{array}$$

Complexités - Bilan

$$L_n(u,v) = e^{v \log(n)^u (\log\log n)^{1-u}}$$

Complexités - Bilan

$$L_n(u,v) = e^{v \log(n)^u (\log\log n)^{1-u}}$$

$L_n(0,v) = (\log n)^v$ (polynomial)

$L_n(1,v) = e^{v \log n}$ (exponentiel)

Complexités - Bilan

- Méthode $p-1$

  pour des n lisses : $\mathcal{O}(\log(q))$

Complexités - Bilan

- Méthode $p-1$

  pour des n lisses : $\mathcal{O}(\log(q))$

- Crible quadratique

$$L_n(\frac{1}{2}, 1+o(1))$$

Complexités - Bilan

- Méthode $p-1$

  pour des n lisses : $\mathcal{O}(\log(q))$

- Crible quadratique

$$L_n(\frac{1}{2}, 1+o(1))$$

- Méthode des courbes elliptiques (p plus petit facteur de n)

$$L_p(1/2, \sqrt{1/2})$$

Complexités - Bilan

- Méthode $p-1$

  pour des n lisses : $\mathcal{O}(\log(q))$

- Crible quadratique

$$L_n(\frac{1}{2}, 1+o(1))$$

- Méthode des courbes elliptiques (p plus petit facteur de n)

$$L_p(1/2, \sqrt{1/2})$$

- Crible des corps de nombres (Pollard - 1988)

$$L_n(1/3, (64/9)^{1/3})$$

Retour à RSA

Choix de p et q

Contre le crible quadratique :

pas grand chose à faire ...

Les méthodes :

- méthode $p-1$
- méthode des courbes elliptiques

marchent bien si p et q sont lisses

Choix de e et d

Pour simplifier le cryptage : e petit

Choix de e et d

Pour simplifier le cryptage : e petit

Attaque des faibles exposants :

si on connait c_i pour (n_i, e) avec $1 \leqslant i \leqslant e$

Choix de e et d

Pour simplifier le cryptage : e petit

Attaque des faibles exposants :

si on connait c_i pour (n_i, e) avec $1 \leqslant i \leqslant e$

Théorème des restes Chinois :
c solution de :

$$\begin{cases} c \equiv c_1 & \mod n_1 \\ & \vdots \\ c \equiv c_e & \mod n_e \end{cases}$$

$$m = c^{-e}$$