Autour du cryptosystème RSA

Lycée Magendie

Avril 2014

Plan

Chiffrement

Alice 

veut écrire

à Bob 

Chiffrement

Alice 

veut écrire

à Bob 

Chiffrement

Alice 

veut écrire

à Bob 

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3

QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3

QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3

QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3

QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3

QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3 QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3 QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3

QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3 QUARTIQUE

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = {f_K}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = {f_K}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob 

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob 

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

- Trois étapes : création et distribution de clés, chiffrement, déchiffrement
- Boîte mail, consultation de compte en banque, ...
- Avantages : simple, rapide, bien connu
- Fragilités : attaques statistiques, gestion de clés

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$$

Chiffrement à clé publique

Alice veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé à Bob

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$$

Chiffrement à clé publique

Alice veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$$

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$$

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K^{sec}_{Bob}

$$m = f_{K^{pub}_{Bob}}{}^{(-1)}(c) = g_{K^{sec}_{Bob}}(c)$$

Chiffrement à clé publique

- Trois étapes : création et publication de clés, chiffrement, déchiffrement
- Avantages : gestion de clé simplifiée, solidité mathématique
- Fragilités : plus lent, plus compliqué à implémenter

En pratique on combine les deux chiffrements : clé publique pour échanger une clé de session (secrète) qui servira à chiffrer à la volée.

Histoire des nombres premiers

- Euclide, livre sept des Éléments, vers -300 donne la définition,
- Il existe une infinité de nombres premiers,
- Tout nombre entier ≥ 2 admet un diviseur premier,
- théorème fondamental de l'arithmétique (preuve par Gauss),
- $p_{k+1} \leq \prod_{l \leq k} p_l + 1$,
- algorithme pour pgcd et ppcm,
- crible d'Eratosthène.

Distribution des nombres premiers

A	10	100	1000	10000	100000
$\pi(A)$	4	25	168	1229	9592
$A/\pi(A)$	2.5	4	5.95	8.14	10.4
$\ln A$	2.3	4.6	6.9	9.2	11.5

Théorème des nombres premiers (Hadamard) :

$$\pi(A) \simeq \frac{A}{\ln A}$$

et

$$p_n \simeq n \ln n.$$

Assez nombreux !
Dans $[1, 10^{1000}]$ la proportion de nombres premiers est $\simeq 1/2303$.

Complexité des opérations arithmétiques

La complexité d'un calcul est le nombre d'opérations élémentaires nécessaires pour le mener à bien.

- complexité linéaire pour l'addition. Pour ajouter deux nombres de 120 chiffres il faut $\simeq 120$ opérations élémentaires.
- complexité quadratique pour la multiplication. Pour ajouter deux nombres de 120 chiffres il faut $\simeq 120 \times 120$ opérations élémentaires.
- complexité du crible d'Eratosthène : $T \simeq n^{1/2}$. Pour savoir si $n = 10^{120} + 1$ est premier on a $T \simeq 10^{60}$.
- Agrawal, Kayal, et Saxena (2002) : complexité polynomiale sextique. Pour savoir si n est premier, $T \simeq k^6$ où k est le nombre de chiffres de n. Si $n = 10^{120} + 1$ alors $T \simeq 121^6 \simeq 3 \times 10^{12}$.

Complexité des opérations arithmétiques

- Pour ajouter deux nombres de 120 chiffres il faut $\simeq 120$ opérations élémentaires.
- Pour multiplier deux nombres de 120 chiffres il faut $\simeq 120 \times 120$ opérations élémentaires.
- Crible d'Eratosthène : pour savoir si $n = 10^{120} + 1$ est premier on a $T \simeq 10^{60}$.
- Agrawal, Kayal, et Saxena (2002) : $T \simeq k^6$ où k est le nombre de chiffres de n. Si $n = 10^{120} + 1$ alors $T \simeq 121^6 \simeq 3 \times 10^{12}$.
- factorisation naïve : $T \simeq \sqrt{n}$,
- pas d'algorithme polynomial connu pour factoriser.

Factoriser n'est pas facile

$15 = 3 \times 5$, $8177 = 13 \times 17 \times 37$, $4391796557 = 653 \times 1237 \times 5437$

$$n = 775849600041239802219341428568066121637285305234191581868939200$$
$$715777450154428362991897517645317349639527419872935123434218610 3$$
$$444234732410533237803945118656187045235934686404170863623977008535965530 9$$

$n = pq$ avec

$$p = 949560147841981112843903371943829594727941901122900732068082 20$$
$$6398416244852852316714799889388537727 7$$

et

$$q = 817062091121320989342705429767363140592459673129423578208577 57$$
$$8700944741280937055731617496876746081 7$$

Factoriser n'est pas facile

$15 = 3 \times 5$, $8177 = 13 \times 17 \times 37$, $4391796557 = 653 \times 1237 \times 5437$

$$n = 775849600041239802219341428568066121637285305234191581868939200$$
$$715777450154428362991897517645317349639527419872935123434218610 3$$
$$444234732410533237803945118656187045235934686404170863623977008535965530 9$$

$n = pq$ avec

$$p = 949560147841981112843903371943829594727941901122900732068082 20$$
$$6398416244852852316714799889388537727 7$$

et

$$q = 817062091121320989342705429767363140592459673129423578208577 57$$
$$8700944741280937055731617496876746081 7$$

Factoriser n'est pas facile

$15 = 3 \times 5$, $8177 = 13 \times 17 \times 37$, $4391796557 = 653 \times 1237 \times 5437$

$n =$
7758496000412398022193414285680661216372853052341915818689392007157774501544283629918975176453173496395274198729351234342186103444234732410533237803945118656187045235934686404170863623977008535965530 9

$n = pq$ avec

$p =$
9495601478419811128439033719438295947279419011229007320680822063984162448528523167147998893885377277

et

$q =$
8170620911213209893427054297673631405924596731294235782085775787009447412809370557316174968767460817

Factoriser n'est pas facile

$15 = 3 \times 5$, $8177 = 13 \times 17 \times 37$, $4391796557 = 653 \times 1237 \times 5437$

$$n = 775849600041239802219341428568066121637285305234191581868939200$$
$$715777450154428362991897517645317349639527419872935123434218610 3$$
$$444234732410533237803945118656187045235934686404170863623977008535965530 9$$

$n = pq$ avec

$$p = 949560147841981112843903371943829594727941901122900732068082 20$$
$$6398416244852852316714799889388537727 7$$

et

$$q = 817062091121320989342705429767363140592459673129423578208577 57$$
$$8700944741280937055731617496876746081 7$$

Factoriser n'est pas facile

$15 = 3 \times 5$, $8177 = 13 \times 17 \times 37$, $4391796557 = 653 \times 1237 \times 5437$

$$n = 775849600041239802219341428568066121637285305234191581868939200$$
$$715777450154428362991897517645317349639527419872935123434218610 3$$
$$444234732410533237803945118656187045235934686404170863623977008535965530 9$$

$n = pq$ avec

$$p = 949560147841981112843903371943829594727941901122900732068082 20$$
$$6398416244852852316714799889388537727 7$$

et

$$q = 817062091121320989342705429767363140592459673129423578208577 57$$
$$8700944741280937055731617496876746081 7$$

Asymétrie

$$(p, q) \rightarrow N = pq$$

$$(p, q) \leftarrow N = pq$$

En décembre 2009, Thorsten Kleinjung et une dizaine de collègues ont factorisé un nombre de 232 chiffres.
The sieving, which was done on many hundreds of machines, took almost two years.

Calculer le produit de deux nombres de 116 chiffres prend 8 millionièmes de secondes sur mon ordinateur portable.

Critère de Fermat

Théorème

Si n est premier alors

$$x^n \equiv x \bmod n \tag{1}$$

pour tout entier x, et $x^{n-1} \equiv 1 \bmod n$ si $(x, n) = 1$.

Fermat, Octobre 1640, . . .*de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.*

Démonstration.

étape 1 : On montre que

$$(x+y)^n = \sum_{0 \le k \le n} \binom{n}{k} x^k y^{n-k} \equiv x^n + y^n \bmod n \tag{2}$$

étape 2 : On vérifie (1) pour $x = 1$ puis on utilise (2) pour montrer que si (1) est vraie pour x, elle est vraie pour $x + 1$. □

Critère de Fermat

Théorème

Si n est premier alors

$$x^n \equiv x \bmod n \tag{1}$$

pour tout entier x, et $x^{n-1} \equiv 1 \bmod n$ si $(x, n) = 1$.

Fermat, Octobre 1640, . . .*de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.*

Démonstration.

étape 1 : On montre que

$$(x+y)^n = \sum_{0 \le k \le n} \binom{n}{k} x^k y^{n-k} \equiv x^n + y^n \bmod n \tag{2}$$

étape 2 : On vérifie (1) pour $x = 1$ puis on utilise (2) pour montrer que si (1) est vraie pour x, elle est vraie pour $x + 1$. □

Critère de Fermat

Théorème

Si n est premier alors

$$x^n \equiv x \bmod n \tag{1}$$

pour tout entier x, et $x^{n-1} \equiv 1 \bmod n$ si $(x, n) = 1$.

Fermat, Octobre 1640, . . .*de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.*

Démonstration.

étape 1 : On montre que

$$(x+y)^n = \sum_{0 \leq k \leq n} \binom{n}{k} x^k y^{n-k} \equiv x^n + y^n \bmod n \tag{2}$$

étape 2 : On vérifie (1) pour $x = 1$ puis on utilise (2) pour montrer que si (1) est vraie pour x, elle est vraie pour $x + 1$. □

Condition nécessaire mais non-suffisante

Si $n = 5$ et $x = 3$ alors $3^2 \equiv 4 \bmod 5$, $3^3 \equiv 2 \bmod 5$, $3^4 \equiv 1 \bmod 5$, $3^5 \equiv 3 \bmod 5$.

Si $n = 15$ alors $14^{15} \equiv 14 \bmod 15$. On dit que 14 est un faux témoin.

Si $n = 1105 = 5 \times 13 \times 17$ alors tous les x premiers à n sont des faux témoins.

Il existe des raffinements du théorème de Fermat.

Condition nécessaire mais non-suffisante

Si $n = 5$ et $x = 3$ alors $3^2 \equiv 4 \bmod 5$, $3^3 \equiv 2 \bmod 5$, $3^4 \equiv 1 \bmod 5$, $3^5 \equiv 3 \bmod 5$.

Si $n = 15$ alors $14^{15} \equiv 14 \bmod 15$. On dit que 14 est un faux témoin.

Si $n = 1105 = 5 \times 13 \times 17$ alors tous les x premiers à n sont des faux témoins.

Il existe des raffinements du théorème de Fermat.

Critère de composition

Si l'on trouve x tel que $x^n \not\equiv x \bmod n$ alors n n'est pas premier.

Exemple : calculons $2^{15} \bmod 15$.

$2^{15} = 32768$ et $32768 = 15 \times 2184 + 8$.

Autre méthode

$2^2 \equiv 4 \bmod 15$, $2^3 \equiv 8 \bmod 15$, $2^4 \equiv 1 \bmod 15$, $2^5 \equiv 2 \bmod 15$,
$2^6 \equiv 4 \bmod 15$, $2^7 \equiv 8 \bmod 15$, $2^8 \equiv 1 \bmod 15$, $2^9 \equiv 2 \bmod 15$,
$2^{10} \equiv 4 \bmod 15$, $2^{11} \equiv 8 \bmod 15$, $2^{12} \equiv 1 \bmod 15$, $2^{13} \equiv 2 \bmod 15$,
$2^{14} \equiv 4 \bmod 15$, $2^{15} \equiv 8 \bmod 15$.

Critère de composition

Si l'on trouve x tel que $x^n \not\equiv x \bmod n$ alors n n'est pas premier.

Exemple : calculons $2^{15} \bmod 15$.

$2^{15} = 32768$ et $32768 = 15 \times 2184 + 8$.

Autre méthode

$2^2 \equiv 4 \bmod 15$, $2^3 \equiv 8 \bmod 15$, $2^4 \equiv 1 \bmod 15$, $2^5 \equiv 2 \bmod 15$,
$2^6 \equiv 4 \bmod 15$, $2^7 \equiv 8 \bmod 15$, $2^8 \equiv 1 \bmod 15$, $2^9 \equiv 2 \bmod 15$,
$2^{10} \equiv 4 \bmod 15$, $2^{11} \equiv 8 \bmod 15$, $2^{12} \equiv 1 \bmod 15$, $2^{13} \equiv 2 \bmod 15$,
$2^{14} \equiv 4 \bmod 15$, $2^{15} \equiv 8 \bmod 15$.

Critère de composition

Si l'on trouve x tel que $x^n \not\equiv x \bmod n$ alors n n'est pas premier.

Exemple : calculons $2^{15} \bmod 15$.

$2^{15} = 32768$ et $32768 = 15 \times 2184 + 8$.

Autre méthode

$2^2 \equiv 4 \bmod 15$, $2^3 \equiv 8 \bmod 15$, $2^4 \equiv 1 \bmod 15$, $2^5 \equiv 2 \bmod 15$,
$2^6 \equiv 4 \bmod 15$, $2^7 \equiv 8 \bmod 15$, $2^8 \equiv 1 \bmod 15$, $2^9 \equiv 2 \bmod 15$,
$2^{10} \equiv 4 \bmod 15$, $2^{11} \equiv 8 \bmod 15$, $2^{12} \equiv 1 \bmod 15$, $2^{13} \equiv 2 \bmod 15$,
$2^{14} \equiv 4 \bmod 15$, $2^{15} \equiv 8 \bmod 15$.

Exponentiation rapide, Piṅgala (entre -450 et -250).

Soit $n = 1031$ et $x = 5$.

On veut calculer $5^{1031} \bmod 1031$.

$b_0 = 5$, $b_1 = 5^2 = 25 \bmod n$, $b_2 = b_1^2 = 5^4 = 625 \bmod n$,
$b_3 = b_2^2 = 5^{2^3} = 390625 = 907 \bmod n$, $b_4 = b_3^2 = 5^{2^4} = 942 \bmod n$,
$b_5 = b_4^2 = 5^{2^5} = 704 \bmod n$, $b_6 = b_5^2 = 5^{2^6} = 736 \bmod n$,
$b_7 = b_6^2 = 5^{2^7} = 421 \bmod n$, $b_8 = b_7^2 = 5^{2^8} = 940 \bmod n$,
$b_9 = b_8^2 = 5^{2^9} = 33 \bmod n$, $b_{10} = b_9^2 = 5^{2^{10}} = 5^{1024} = 58 \bmod n$.

Or $1031 = 10^3 + 0 \times 10^2 + 3 \times 10 + 1 \times 1 = 2^{10} + 2^2 + 2 + 1$ s'écrit 10000000111 en base 2.

Donc $5^{1031} = 5^{2^{10}+2^2+2+1} = 5^{2^{10}} \times 5^{2^2} \times 5^{2^1} \times 5^{2^0} =$
$b_{10} \times b_2 \times b_1 \times b_0 = 58 \times 625 \times 25 \times 5 = 4531250 = 5 \bmod n$.

12 multiplications au lieu de 1030.

L'exponentiation rapide

Pour calculer $x^e \bmod n$

1. $R \leftarrow 1$ et $f \leftarrow e$ et $B \leftarrow x \bmod n$
2. Tant que $f \neq 0$ faire
   - Si f est pair alors $f \leftarrow f/2$ et $B \leftarrow B \times B \bmod n$
   - Si f est impair alors $f \leftarrow (f-1)/2$ et $R \leftarrow R \times B \bmod n$ et $B \leftarrow B \times B \bmod n$
3. Afficher R

Le critère de Miller-Rabin

Théorème

Soit $n \geq 3$ un entier impair et posons $n-1 = 2^k m$ avec m impair.
Si n est premier, alors pour tout x premier à n, on a

$$x^m \equiv 1 \bmod n \text{ ou } x^{2^i m} \equiv -1 \bmod n \text{ pour un } 0 \leqslant i < k\,. \qquad (3)$$

Peut importe ici le détail : ce critère est une variante du critère de Fermat.

Si l'on trouve un x tel que la condition (3) est fausse, alors n est composé.

On choisit x au hasard et on vérifie la condition (3).

Si elle est fausse alors n est composé. Critère de composition.

Si elle est vraie que dire ?

Le critère de Miller-Rabin

Théorème

Soit $n \geq 3$ un entier impair et posons $n-1 = 2^k m$ avec m impair.
Si n est premier, alors pour tout x premier à n, on a

$$x^m \equiv 1 \bmod n \text{ ou } x^{2^i m} \equiv -1 \bmod n \text{ pour un } 0 \leqslant i < k\,. \qquad (3)$$

Peut importe ici le détail : ce critère est une variante du critère de Fermat.

Si l'on trouve un x tel que la condition (3) est fausse, alors n est composé.

On choisit x au hasard et on vérifie la condition (3).

Si elle est fausse alors n est composé. Critère de composition.

Si elle est vraie que dire ?

Le critère de Miller-Rabin

Théorème

Soit $n \geq 3$ un entier impair et posons $n-1 = 2^k m$ avec m impair.
Si n est premier, alors pour tout x premier à n, on a

$$x^m \equiv 1 \bmod n \text{ ou } x^{2^i m} \equiv -1 \bmod n \text{ pour un } 0 \leqslant i < k\,. \qquad (3)$$

Peut importe ici le détail : ce critère est une variante du critère de Fermat.

Si l'on trouve un x tel que la condition (3) est fausse, alors n est composé.

On choisit x au hasard et on vérifie la condition (3).

Si elle est fausse alors n est composé. Critère de composition.

Si elle est vraie que dire ?

Le test de Miller-Rabin

Théorème

Si $n \geq 15$ est composé et impair, alors

$$\frac{\#\{x \text{ in } [1,n] : \mathrm{pgcd}(x,n) = 1 \text{ et la condition (3) est vraie}\}}{\#\{x \text{ in } [1,n] : \mathrm{pgcd}(x,n) = 1\}} \leqslant \frac{1}{4}.$$

Au plus un quart de faux témoins.

Remarque 1 : Après λ tests, la probabilité de manquer un composé est majorée par $1/4^{\lambda}$.

Remarque 2 : Si n est premier, on n'aura jamais de certitude avec ce test.

Agrawal, Kayal et Saxena

$$T \simeq k^6$$

où k est le nombre de chiffres décimaux de n.
Pas de faux témoins pour leur test.