Cryptage RSA

Damien LEGROS et Danil BERRAH

Projet étoile

Table des matières

Fonctionnement général

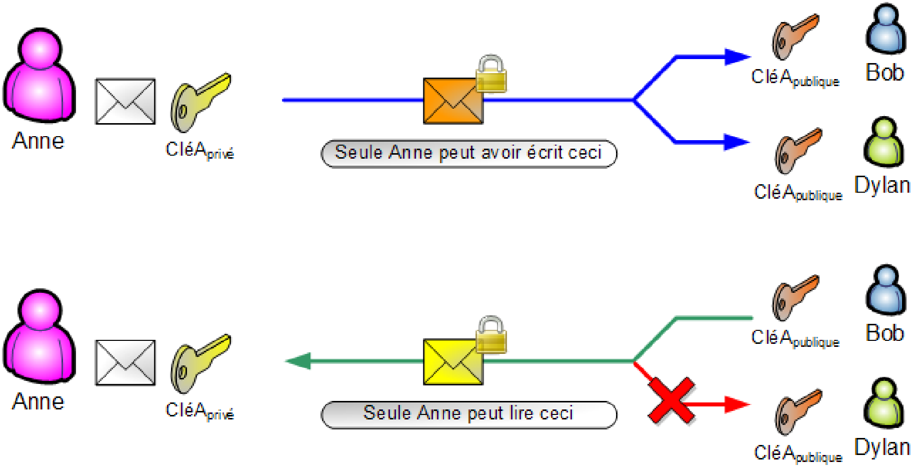

Figure: Chiffrement et Dechiffrement RSA

Création des Clés

- On choisit deux nombres premiers p et q

Création des Clés

- On choisit deux nombres premiers p et q
- On calcule leur produit $n = pq$

Création des Clés

- On choisit deux nombres premiers p et q
- On calcule leur produit $n = pq$
- On calcule l'indicatrice d'Euler en n :

$$\Phi(n) = (p-1)(q-1)$$

Création des Clés

- On choisit deux nombres premiers p et q
- On calcule leur produit $n = pq$
- On calcule l'indicatrice d'Euler en n :

$$\Phi(n) = (p-1)(q-1)$$

- Exposant de chiffrement : un entier naturel e premier avec $\Phi(n)$ et strictement inférieur à $\Phi(n)$

Création des Clés

- On choisit deux nombres premiers p et q
- On calcule leur produit $n = pq$
- On calcule l'indicatrice d'Euler en n :

$$\Phi(n) = (p-1)(q-1)$$

- Exposant de chiffrement : un entier naturel e premier avec $\Phi(n)$ et strictement inférieur à $\Phi(n)$
- Exposant de déchiffrement : d, l'inverse de e modulo $\Phi(n)$

Création des Clés

- On choisit deux nombres premiers p et q
- On calcule leur produit $n = pq$
- On calcule l'indicatrice d'Euler en n :

$$\Phi(n) = (p-1)(q-1)$$

- Exposant de chiffrement : un entier naturel e premier avec $\Phi(n)$ et strictement inférieur à $\Phi(n)$
- Exposant de déchiffrement : d, l'inverse de e modulo $\Phi(n)$
- Il existe deux entiers d et k tels que $ed + k\Phi(n) = 1$, on a donc $ed \equiv 1(\Phi(n))$

Création des Clés

- On choisit deux nombres premiers p et q
- On calcule leur produit $n = pq$
- On calcule l'indicatrice d'Euler en n :

$$\Phi(n) = (p-1)(q-1)$$

- Exposant de chiffrement : un entier naturel e premier avec $\Phi(n)$ et strictement inférieur à $\Phi(n)$
- Exposant de déchiffrement : d, l'inverse de e modulo $\Phi(n)$
- Il existe deux entiers d et k tels que $ed + k\Phi(n) = 1$, on a donc $ed \equiv 1(\Phi(n))$
- Le couple (n,e) est la clé publique, le couple (n,d) est la clé privée

Indicatrice d'Euler

- L'indicatrice d'Euler est la fonction Φ qui s'obtient à partir de la décomposition en facteurs premiers de n

Indicatrice d'Euler

- L'indicatrice d'Euler est la fonction Φ qui s'obtient à partir de la décomposition en facteurs premiers de n
- Si

$$n = \prod_{i=1}^{r} p_i^{k_i}$$

Indicatrice d'Euler

- L'indicatrice d'Euler est la fonction Φ qui s'obtient à partir de la décomposition en facteurs premiers de n
- Si

$$n = \prod_{i=1}^{r} p_i^{k_i}$$

- Alors

$$\Phi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{k_i - 1} = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

Théorème de Bachet-Bézout

- Soient a et b deux entiers relatifs. Si d est le PGCD de a et b,

Théorème de Bachet-Bézout

- Soient a et b deux entiers relatifs. Si d est le PGCD de a et b,
- Il existe deux entiers relatifs x et y tels que

$$ax + by = d$$

Théorème de Bachet-Bézout

- Soient a et b deux entiers relatifs. Si d est le PGCD de a et b,
- Il existe deux entiers relatifs x et y tels que

$$ax + by = d$$

- Deux entiers relatifs a et b sont premiers entre eux si et seulement si,

Théorème de Bachet-Bézout

- Soient a et b deux entiers relatifs. Si d est le PGCD de a et b,
- Il existe deux entiers relatifs x et y tels que

$$ax + by = d$$

- Deux entiers relatifs a et b sont premiers entre eux si et seulement si,
- Il existe deux entiers relatifs x et y tels que

$$ax + by = 1$$

Algorithme d'Euclide étendu

- Variante de l'algorithme d'Euclide qui permet à partir de deux entiers a et b, de calculer leur PGCD et un de leurs couples de coefficients de Bézout

Algorithme d'Euclide étendu

- Variante de l'algorithme d'Euclide qui permet à partir de deux entiers a et b, de calculer leur PGCD et un de leurs couples de coefficients de Bézout
- Deux entiers u et v tels que

$$au + bv = \mathrm{PGCD}(a, b)$$

Algorithme d'Euclide étendu

- Variante de l'algorithme d'Euclide qui permet à partir de deux entiers a et b, de calculer leur PGCD et un de leurs couples de coefficients de Bézout
- Deux entiers u et v tels que

$$au + bv = \mathrm{PGCD}(a, b)$$

- Détermine la solution d'une équation diophantienne

$$ax + by = c$$

Méthode de chiffrement

- Si M est un entier naturel strictement inférieur à n représentant un message.

Méthode de chiffrement

- Si M est un entier naturel strictement inférieur à n représentant un message.
- Alors le message chiffré sera représenté par

$$C \equiv M^e \pmod{n}$$

Méthode de dechiffrement

- Pour déchiffrer C, on utilise d, l'inverse de e modulo $(p-1)(q-1)$.

Méthode de dechiffrement

- Pour déchiffrer C, on utilise d, l'inverse de e modulo $(p-1)(q-1)$.
- On retrouve le message clair M par

$$M \equiv C^d \pmod{n}$$

Table des matières

Forme des nombres premiers pythagoricien

- Nombre premier p qui est l'hypoténuse d'un triangle rectangle à côtés entiers

Forme des nombres premiers pythagoricien

- Nombre premier p qui est l'hypothénuse d'un triangle rectangle à côtés entiers
- S'ecrit sous la forme :

$$p = x^2 + y^2 \ (x, y \in \mathbb{N})$$

Forme des nombres premiers pythagoricien

- Nombre premier p qui est l'hypothénuse d'un triangle rectangle à côtés entiers
- S'ecrit sous la forme :

$$p = x^2 + y^2 \ (x, y \in \mathbb{N})$$

- Nombres premiers impaires sommes de deux carrés

Forme des nombres premiers pythagoricien

- Nombre premier p qui est l'hypothénuse d'un triangle rectangle à côtés entiers
- S'ecrit sous la forme :

$$p = x^2 + y^2 \ (x, y \in \mathbb{N})$$

- Nombres premiers impaires sommes de deux carrés
- pPuvent s'écrire sous la forme :

$$p = 4k + 1 \ (k \in \mathbb{N})$$

Forme des nombres premiers pythagoricien

- Nombre premier p qui est l'hypothénuse d'un triangle rectangle à côtés entiers
- S'ecrit sous la forme :

$$p = x^2 + y^2 \ (x, y \in \mathbb{N})$$

- Nombres premiers impaires sommes de deux carrés
- pPuvent s'écrire sous la forme :

$$p = 4k + 1 \ (k \in \mathbb{N})$$

- Dix premiers nombres premiers de Pythagore : 5, 13, 17, 29, 37, 41, 53, 61, 73 et 89

Théorème des deux carrés de Fermat

- Nombre premier impair p est somme de deux carrés parfaits si et seulement si p est un nombre premier de Pythagore

Théorème des deux carrés de Fermat

- Nombre premier impair p est somme de deux carrés parfaits si et seulement si p est un nombre premier de Pythagore
- p congru à 1 modulo 4 :

$$(\exists (x,y) \in \mathbb{N}^2 \; p = x^2 + y^2) \iff p \equiv 1 \pmod 4$$

Théorème des deux carrés de Fermat

- Nombre premier impair p est somme de deux carrés parfaits si et seulement si p est un nombre premier de Pythagore
- p congru à 1 modulo 4 :

$$(\exists (x,y) \in \mathbb{N}^2 \ p = x^2 + y^2) \iff p \equiv 1 \pmod 4$$

- Décomposition unique et infinité de nombre premiers impairs sous cette forme

Adaptation du théorème d'Euclide aux nombres premiers

- p un nombre premier et $q = (2^2 \times 3 \times 5 \times 7 \times ... \times p) - 1$

Adaptation du théorème d'Euclide aux nombres premiers

- p un nombre premier et $q = (2^2 \times 3 \times 5 \times 7 \times ... \times p) - 1$
- Tous les facteurs premiers de q sont strictement supérieurs à p, et puisque $q \equiv -1 \bmod 4$

Adaptation du théorème d'Euclide aux nombres premiers

- p un nombre premier et $q = (2^2 \times 3 \times 5 \times 7 \times ... \times p) - 1$
- Tous les facteurs premiers de q sont strictement supérieurs à p, et puisque $q \equiv -1 \bmod 4$
- Il y a une infinité de nombres premiers congru à -1 modulo 4

Adaptation du théorème d'Euclide aux nombres premiers

- p un nombre premier et $q = (2^2 \times 3 \times 5 \times 7 \times \ldots \times p) - 1$
- Tous les facteurs premiers de q sont strictement supérieurs à p, et puisque $q \equiv -1 \mod 4$
- Il y a une infinité de nombres premiers congru à -1 modulo 4
- p un nombre premier et $q = (3^2 \times 5^2 \times 7^2 \times \ldots \times p^2) + 2^2$

Adaptation du théorème d'Euclide aux nombres premiers

- p un nombre premier et $q = (2^2 \times 3 \times 5 \times 7 \times ... \times p) - 1$
- Tous les facteurs premiers de q sont strictement supérieurs à p, et puisque $q \equiv -1 \bmod 4$
- Il y a une infinité de nombres premiers congru à -1 modulo 4
- p un nombre premier et $q = (3^2 \times 5^2 \times 7^2 \times ... \times p^2) + 2^2$
- $q \equiv 5 \bmod 8$ et q est une somme de deux carrés premiers entre eux, tous ses facteurs premiers sont de la forme $4k + 1$

Adaptation du théorème d'Euclide aux nombres premiers

- p un nombre premier et $q = (2^2 \times 3 \times 5 \times 7 \times ... \times p) - 1$
- Tous les facteurs premiers de q sont strictement supérieurs à p, et puisque $q \equiv -1 \mod 4$
- Il y a une infinité de nombres premiers congru à -1 modulo 4
- p un nombre premier et $q = (3^2 \times 5^2 \times 7^2 \times ... \times p^2) + 2^2$
- $q \equiv 5 \mod 8$ et q est une somme de deux carrés premiers entre eux, tous ses facteurs premiers sont de la forme $4k + 1$
- Il y a une infinité de nombres premiers congrus à 5 modulo 4 et 5 modulo 8

Les nombres de Mersenne

- Nombres de la forme :

$$M_n = 2^n - 1,\ n \geq 1$$

Les nombres de Mersenne

- Nombres de la forme :
$$M_n = 2^n - 1,\ n \geq 1$$
- Pour que le n-ième nombre de Mersenne M_n soit premier, il est nécessaire (mais non suffisant, contrairement à ce qu'affirmait Mersenne) que n soit premier

Les nombres de Mersenne

- Nombres de la forme :

$$M_n = 2^n - 1, \; n \geq 1$$

- Pour que le n-ième nombre de Mersenne M_n soit premier, il est nécessaire (mais non suffisant, contrairement à ce qu'affirmait Mersenne) que n soit premier
- Premiers nombres premiers de Mersenne :

$$M_2 = 2^2 - 1 = 3$$

$$M_3 = 2^3 - 1 = 7$$

$$M_5 = 2^5 - 1 = 31$$

$$M_7 = 2^7 - 1 = 127$$

$$M_{13} = 2^{13} - 1 = 8191$$

Forme des nombres de Fermat

- S'écrit sous la forme :

$$2^{2^n} + 1, \ (n \in \mathbb{N})$$

Forme des nombres de Fermat

- S'écrit sous la forme :

$$2^{2^n} + 1,\ (n \in \mathbb{N})$$

- Fermat avait émis la conjecture que tous ces nombres étaient premiers, or cette conjecture est fausse dès F_5.

Démonstration

- Deux entiers a impair et b tels que $k = a2^b$

Démonstration

- Deux entiers a impair et b tels que $k = a2^b$
- Avec $c = 2^{(2^b)}$, on dispose alors des égalités suivantes :

$$1 + 2^k = 1 + c^a = (1 + c) \sum_{i=0}^{a-1} (-1)^i c^i$$

Démonstration

- Deux entiers a impair et b tels que $k = a2^b$
- Avec $c = 2^{(2^b)}$, on dispose alors des égalités suivantes :

$$1 + 2^k = 1 + c^a = (1 + c)\sum_{i=0}^{a-1}(-1)^i c^i$$

- $1 + c$ est un diviseur du nombre premier $1 + 2^k$, on en déduit que $k = 2^b$

Table des matières

Petit théorème de Fermat

- Le petit théorème de Fermat dit que si p est premier et que a est premier avec p alors on a

Petit théorème de Fermat

- Le petit théorème de Fermat dit que si p est premier et que a est premier avec p alors on a
- $a^{p-1} - 1$ divisible par p :

$$a^{p-1} \equiv 1(p)$$

Démonstration

- a non divisible par p
  $N = a * 2a * 3a * 4a * 5a * ... * (p-1)a$
  $N = 1 * 2 * 3 * 4 * 5 * ... * (p-1) * a^{p-1} = (p-1)! * a^{p-1}$
  r_k tel que $ka = pq + r_k$

Démonstration

- a non divisible par p
  $N = a * 2a * 3a * 4a * 5a * ... * (p-1)a$
  $N = 1 * 2 * 3 * 4 * 5 * ... * (p-1) * a^{p-1} = (p-1)! * a^{p-1}$
  r_k tel que $ka = pq + r_k$
- On remplace les ka par r_k, on obtient :

$$N \equiv r_1 * r_2 * r_3 * r_4 * r_5 * ... * r_{p-1} (p)$$

Démonstration

- a non divisible par p
  $N = a * 2a * 3a * 4a * 5a * ... * (p-1)a$
  $N = 1 * 2 * 3 * 4 * 5 * ... * (p-1) * a^{p-1} = (p-1)! * a^{p-1}$
  r_k tel que $ka = pq + r_k$
- On remplace les ka par r_k, on obtient :

$$N \equiv r_1 * r_2 * r_3 * r_4 * r_5 * ... * r_{p-1} (p)$$

- $(r_1, r_2, ..., r_{p-1})$ est une permutation de $(1, 2, ..., p-1)$:

$$r_1 * r_2 * r_3 * r_4 * r_5 * ... * r_{p-1} = (p-1)!$$

Démonstration

- a non divisible par p
  $N = a * 2a * 3a * 4a * 5a * ... * (p-1)a$
  $N = 1 * 2 * 3 * 4 * 5 * ... * (p-1) * a^{p-1} = (p-1)! * a^{p-1}$
  r_k tel que $ka = pq + r_k$
- On remplace les ka par r_k, on obtient :

$$N \equiv r_1 * r_2 * r_3 * r_4 * r_5 * ... * r_{p-1} (p)$$

- $(r_1, r_2, ..., r_{p-1})$ est une permutation de $(1, 2, ..., p-1)$:

$$r_1 * r_2 * r_3 * r_4 * r_5 * ... * r_{p-1} = (p-1)!$$

- On en déduit :

$$(p-1)! * a^{p-1} \equiv (p-1)!(p)$$

$$r_1 * r_2 * r_3 * r_4 * r_5 * ... * r_{p-1} * (a^{p-1} - 1) \equiv 1(p)$$

$$a^{p-1} \equiv 1(p)$$

Test de Fermat

- Si p n'est pas premier alors a^{p-1} n'est probablement pas divisible par p

Test de Fermat

- Si p n'est pas premier alors a^{p-1} n'est probablement pas divisible par p
- Le test PGP est un logiciel de chiffrement cryptographique utilisant la logique du test de primalité de Fermat

Test de Fermat

- Si p n'est pas premier alors a^{p-1} n'est probablement pas divisible par p
- Le test PGP est un logiciel de chiffrement cryptographique utilisant la logique du test de primalité de Fermat
- Pour 4 valeurs de a différentes $(2, 3, 5, 7)$ si,

$$2^{p-1} \equiv 3^{p-1} \equiv 5^{p-1} \equiv 7^{p-1} \equiv 1(p)$$

Test de Fermat

- Si p n'est pas premier alors a^{p-1} n'est probablement pas divisible par p
- Le test PGP est un logiciel de chiffrement cryptographique utilisant la logique du test de primalité de Fermat
- Pour 4 valeurs de a différentes $(2, 3, 5, 7)$ si,

$$2^{p-1} \equiv 3^{p-1} \equiv 5^{p-1} \equiv 7^{p-1} \equiv 1(p)$$

- Alors p est probablement un nombre premier sinon p n'est pas premier

Symbole de Legendre

- Le symbole de Legendre $\left(\frac{a}{p}\right)$ retourne une valeur entiere comprise dans $[-1, 1]$

Symbole de Legendre

- Le symbole de Legendre $\left(\frac{a}{p}\right)$ retourne une valeur entiere comprise dans $[-1, 1]$
- Soit p un nombre premier et a un entier, alors le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut,

Symbole de Legendre

- Le symbole de Legendre $\left(\frac{a}{p}\right)$ retourne une valeur entiere comprise dans $[-1, 1]$
- Soit p un nombre premier et a un entier, alors le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut,
  - -1 si a n'est pas un residu quadratique modulo p.

Symbole de Legendre

- Le symbole de Legendre $\left(\frac{a}{p}\right)$ retourne une valeur entiere comprise dans $[-1, 1]$
- Soit p un nombre premier et a un entier, alors le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut,
  - -1 si a n'est pas un residu quadratique modulo p.
  - 0 si a est divisble par p.

Symbole de Legendre

- Le symbole de Legendre $\left(\frac{a}{p}\right)$ retourne une valeur entiere comprise dans $[-1, 1]$
- Soit p un nombre premier et a un entier, alors le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut,
  - -1 si a n'est pas un residu quadratique modulo p.
  - 0 si a est divisble par p.
  - 1 si a est un residu quadratique modulo p mais n'est pas divisible par p.

Symbole de Legendre

- Le symbole de Legendre $\left(\frac{a}{p}\right)$ retourne une valeur entiere comprise dans $[-1, 1]$
- Soit p un nombre premier et a un entier, alors le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut,
  - -1 si a n'est pas un residu quadratique modulo p.
  - 0 si a est divisble par p.
  - 1 si a est un residu quadratique modulo p mais n'est pas divisible par p.
- Un residu quadratique a modulo p signifie qu'il existe un entier k tel que,

$$a \equiv k^2 (p)$$

Symbole de Jacobi

- Le Symbole de Jacobi $\left(\frac{a}{n}\right)$ est une généralisation du symbole de Legendre

Symbole de Jacobi

- Le Symbole de Jacobi $(\frac{a}{n})$ est une généralisation du symbole de Legendre
- Produit de symbole de Legendre $(\frac{a}{p_k})$ pour tout $k \in \mathbb{N}$ selon la décomposition en facteur premier de n:

$$p_1 * p_2 * p_3 * p_4 * p_5 * \ldots * p_k = n$$

Symbole de Jacobi

- Le Symbole de Jacobi $(\frac{a}{n})$ est une généralisation du symbole de Legendre
- Produit de symbole de Legendre $(\frac{a}{p_k})$ pour tout $k \in \mathbb{N}$ selon la décomposition en facteur premier de n:

$$p_1 * p_2 * p_3 * p_4 * p_5 * \ldots * p_k = n$$

- Ainsi,

$$(\frac{a}{\prod_{1 \leq i \leq k} p_i}) = (\frac{a}{p_1}) * (\frac{a}{p_2}) * (\frac{a}{p_3}) * (\frac{a}{p_4}) * (\frac{a}{p_5}) * \ldots * (\frac{a}{p_k}) = \prod_{1 \leq i \leq k} (\frac{a}{p_i}) = (\frac{a}{n})$$

Critère d’Euler

- Le Critère d’Euler permet de déterminer si un entier est un residu quadratique modulo un nombre premier ou non

Critère d'Euler

- Le Critère d'Euler permet de déterminer si un entier est un residu quadratique modulo un nombre premier ou non
- Soient p un nombre premier différent de 2 et a un entier premier avec p,

Critère d'Euler

- Le Critère d'Euler permet de déterminer si un entier est un residu quadratique modulo un nombre premier ou non
- Soient p un nombre premier différent de 2 et a un entier premier avec p,
  - Si a est un residu quadratique modulo p alors $a^{\frac{p-1}{2}} \equiv 1(p)$.

Critère d'Euler

- Le Critère d'Euler permet de déterminer si un entier est un residu quadratique modulo un nombre premier ou non
- Soient p un nombre premier différent de 2 et a un entier premier avec p,
  - Si a est un residu quadratique modulo p alors $a^{\frac{p-1}{2}} \equiv 1(p)$.
  - Si a n'est pas un residu quadratique modulo p alors $a^{\frac{p-1}{2}} \equiv -1(p)$.

Critère d'Euler

- Le Critère d'Euler permet de déterminer si un entier est un residu quadratique modulo un nombre premier ou non
- Soient p un nombre premier différent de 2 et a un entier premier avec p,
  - Si a est un residu quadratique modulo p alors $a^{\frac{p-1}{2}} \equiv 1(p)$.
  - Si a n'est pas un residu quadratique modulo p alors $a^{\frac{p-1}{2}} \equiv -1(p)$.
- Avec le symbole de Legendre on a :

$$a^{\frac{p-1}{2}} \equiv (\frac{a}{p})(p)$$

Test de Solovay-Strassen

- Test probabiliste permettant de determiner si un entier impair n est premier ou non

Test de Solovay-Strassen

- Test probabiliste permettant de determiner si un entier impair n est premier ou non
- On test pour un nombre a la congruence :

$$a^{\frac{p-1}{2}} \equiv (\frac{a}{p})(p)$$

Test de Solovay-Strassen

- Test probabiliste permettant de determiner si un entier impair n est premier ou non
- On test pour un nombre a la congruence :

$$a^{\frac{p-1}{2}} \equiv (\frac{a}{p})(p)$$

- Si elle est satisfaite alors a est probablement premier, sinon a n'est pas premier

Petit théorème de Fermat

- Le petit théorème de Fermat dit que si p est premier et que a est premier avec p

Petit théorème de Fermat

- Le petit théorème de Fermat dit que si p est premier et que a est premier avec p
- $a^{p-1} - 1$ divisible par p :

$$a^{p-1} \equiv 1(p)$$

Petit théorème de Fermat

- Le petit théorème de Fermat dit que si p est premier et que a est premier avec p
- $a^{p-1} - 1$ divisible par p :

$$a^{p-1} \equiv 1(p)$$

- Dans un anneau $\mathbb{Z}/p\mathbb{Z}$ si p est premier alors l'équation $x^2 = 1$ n'a pour solutions que 1 et -1

$$1^2 = 1(p)$$

$$(-1)^2 = 1(p)$$

Théorème de Rabin

- Pour un entier impair composé n superieur a 9 et d impair tel que $n - 1 = 2^s * d$

Théorème de Rabin

- Pour un entier impair composé n superieur a 9 et d impair tel que $n - 1 = 2^s * d$
- Alors il existe $\varphi(n)/4$ menteurs forts a pour $1 < a < n$ avec $\varphi(n)$ fonction indicatrice d'Euler

Théorème de Rabin

- Pour un entier impair composé n superieur a 9 et d impair tel que $n-1 = 2^s * d$
- Alors il existe $\varphi(n)/4$ menteurs forts a pour $1 < a < n$ avec $\varphi(n)$ fonction indicatrice d'Euler
- a est un menteur fort si il verifie soit $a^d \equiv 1(p)$, soit $a^{2^r d} \equiv -1(p)$ pour r tel que $0 \leq r < s$

Théorème de Rabin

- Pour un entier impair composé n superieur a 9 et d impair tel que $n-1 = 2^s * d$
- Alors il existe $\varphi(n)/4$ menteurs forts a pour $1 < a < n$ avec $\varphi(n)$ fonction indicatrice d'Euler
- a est un menteur fort si il verifie soit $a^d \equiv 1(p)$, soit $a^{2^r d} \equiv -1(p)$ pour r tel que $0 \leq r < s$
- Pour un nombre impair composé n, 3/4 au moins des entiers a tel que $1 < a < n$ sont des témoins de Miller pour n

Théorème de Rabin

- Pour un entier impair composé n superieur a 9 et d impair tel que $n-1=2^s*d$
- Alors il existe $\varphi(n)/4$ menteurs forts a pour $1<a<n$ avec $\varphi(n)$ fonction indicatrice d'Euler
- a est un menteur fort si il verifie soit $a^d\equiv 1(p)$, soit $a^{2^r d}\equiv -1(p)$ pour r tel que $0\leq r<s$
- Pour un nombre impair composé n, 3/4 au moins des entiers a tel que $1<a<n$ sont des témoins de Miller pour n
- Si n est compose alors a est un témoin de Miller si $a^d\not\equiv 1(p)$ et pour quelque soit $r\in[0,s-1]$ $a^{2^r d}\not\equiv -1(p)$

Test de Miller-Rabin

- Test probabiliste de type Monte Carlo donnant une réponse oui ou non permettant de savoir si un nombre est de facon certaine composé ou si il est probablement premier

Test de Miller-Rabin

- Test probabiliste de type Monte Carlo donnant une réponse oui ou non permettant de savoir si un nombre est de facon certaine composé ou si il est probablement premier
- Pour p premier, un entier a non divisble par p, s non nul et d impair,

$$a^{p-1} = (a^d)^{2^s} \equiv 1(p)$$

Test de Miller-Rabin

- Test probabiliste de type Monte Carlo donnant une réponse oui ou non permettant de savoir si un nombre est de facon certaine composé ou si il est probablement premier
- Pour p premier, un entier a non divisble par p, s non nul et d impair,

$$a^{p-1} = (a^d)^{2^s} \equiv 1(p)$$

- Pour verifier si n est premier on prend une valeur de a aléatoire non divisble par n est on verifie $a^d \equiv 1(n)$ et $r \in [0, s-1]$ $a^{2^r d} \equiv -1(n)$

Test de Miller-Rabin

- Test probabiliste de type Monte Carlo donnant une réponse oui ou non permettant de savoir si un nombre est de facon certaine composé ou si il est probablement premier
- Pour p premier, un entier a non divisble par p, s non nul et d impair,

$$a^{p-1} = (a^d)^{2^s} \equiv 1(p)$$

- Pour verifier si n est premier on prend une valeur de a aléatoire non divisble par n est on verifie $a^d \equiv 1(n)$ et $r \in [0, s-1]$ $a^{2^r d} \equiv -1(n)$
  - Si les congruences sont valides alors a n'est pas un témoin de Miller et n est probablement premier.

Test de Miller-Rabin

- Test probabiliste de type Monte Carlo donnant une réponse oui ou non permettant de savoir si un nombre est de facon certaine composé ou si il est probablement premier
- Pour p premier, un entier a non divisble par p, s non nul et d impair,

$$a^{p-1} = (a^d)^{2^s} \equiv 1(p)$$

- Pour verifier si n est premier on prend une valeur de a aléatoire non divisble par n est on verifie $a^d \equiv 1(n)$ et $r \in [0, s-1]$ $a^{2^r d} \equiv -1(n)$
  - Si les congruences sont valides alors a n'est pas un témoin de Miller et n est probablement premier.
  - Sinon a est un témoin de Miller et n est de facon certaine composé.

Merci de votre temps !

Nous sommes là si vous avez des questions !