Rappels

C'est une sous-branche de la sécurité.

Même si l'adverse connait votre algorithme de cryptage, il doit être impossible pour l'adverse de décrypter votre message.

Pour cela, on étudie Z/nZ, permettant de travailler sur des blocs de taille finie.

(Z/nZ, +) => groupe commutatif.

(Z/nZ, +, *) => anneau commutatif unitaire

(Z/nZ, +, *) => corps ssi n est premier

Dans Z/nZ: a $\in$ Z/nZ inversible ssi a et n premier entre eux de plus, et dans ce dernier cas:

$\exists$s,t : as + nt = 1

s $\equiv a^{-1}$(mdn)

Existe-t-il n tel que a : 1 $\leq$ a $\leq$ n - 1 est premier avec n ? $\leftrightarrows$ n premier ?

P1 => P2: *n premier*

d = pgcd(a, n)

n = dq, dq = 1aun

si d = n, a = qd' != 0, a > n !

P2 => P1

On suppose n non premier, n = dc, c,d != 1 et n.

2 $\leq$ d $\leq$ n - 1, *d est premier avec n.*

pgcd(d, n) = 1, *d = 1* et n est premier

Bien entendu, les calculs vont plus loin que de l'addition ou de la multiplication.

Nous verrons des algorithmes et des propriétés basiques puis nous regarderons des structures de Z/nZ, enfin nous verrons le RSA, avec des tests de primalités.

Exponentiation modulaire (général)

Astuce :

x^{2q} = $(x^q)^2$ 1 multiplication

x^{2q+1} = $x * (x^q)^2$ 2 multiplication

q a un chiffre de moins, en base 2, que 2q ou 2q + 1

Exemple :

5^{77} (mod 9)

77 = 2 * 38 + 1

5^{77} = $5 * (5^{38})^2 \equiv 5 * 7^2 \equiv$ 5 * 49 $\equiv$ 20 $\equiv$ 2

5^{38} = $(5^{19})^2$ = $5^2 \equiv$ 25 $\equiv$ 7

19 = 2 * 9 + 1

5^{19} = $5 * (5^9)^2 \equiv 5 * 8^2$ = 5 * 64 $\equiv$ 5

9 = 2^3 + 1

5^9 = $5 * (5^{2^3}) \equiv$ 5 * 7 = 35 $\equiv$ 8

Lemme Chinois

Soient n1, n2, …, nk des nombres premiers entre eux deux à deux.

Soient a1, a2, …, ak des entiers quelconques

Il existe un entier a $\forall$i a $\equiv a_i$ (mod n_i)

Exemple :

n1 = 5, a1 = 2, n2 = 7, a2 = 3

n1 = 2 n2 = 3

0 0 0

1 1 1

0 2 2

1 0 3

0 1 4

1 2 5

0 0 6

1 1 7

On a a = 1.

Demonstration avec k = 2:

n1, n2; (n1,n2) = 1 et a1, a2

1) Cas particulier

a1 = 0, a2 = 0; a = n1 * n2

a1 = 1, a2 = 0 ?

? a = q * n2 et q * n2 $\equiv$ 1 (mod n1)

(n1, n2) = 1, n2 inversible mod n1

{Euclide etendu} ($\exists$q) q * n2 $\equiv$ 1 (mod n1)

Il existe a10 $\equiv$ 1 (mod n1) $\equiv$ 0 (mod n2).

a10 = $n2^{-1}$ (mod n1) * n2

a01 $\equiv$ 0 (mod n1) $\equiv$ 1 (mod n2)

a01 = n^{-1} (mod n2) * n1

Une solution : a = a1 * a10 + a2 * a01

Reprenons l'exemple d'en haut :

7^{-1} (mod 5) $\equiv$ 3, a10 = 3 * 7 = 21

5^{-1} (mod 7) $\equiv$ 3, a01 = 3 * 5 = 15

a = 2 * 21 + 3 * 15 = 42 + 45 = 87 = 70 + 17

Fonction indicatrice d'Euler

Question: Combien d'éléments inversibles dans Z/nZ ?

{a $\in$ N, 1 $\leq$ a $\leq$ n - 1; a et n premiers entre eux} = ϕ(n) "Euler totient function"

101 premier

(Z/101Z, +, *) Corps

((Z/101Z), *) groupe

Il y a ϕ(101) = 100 élèments

ϕ(100) = ?

Bibliothéque C++

gmp : calcul sur les grands nombres