Rappel

En cryptographie, l'adversaire connait problablement votre algorithme, exemple: Enigma.

Le secret du chiffrement se cache dans la clé.

(Z/nZ) = Anneau commutatif unitaire

n premier $\leftrightarrows$ corps

Division

Bezout, Algorithme d'Euclide Etendu

Z/nZ, diviser par ((a,n) = 1), c'est multiplier par a^{-1}

$\exists\, s_1$ t: s * a + t * n = 1

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

Exponentiation modulaire

a^{2q} = $(a^q)^2$

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

Fonction indicatrice d'Euler

Φ(n) = # { k | k inversible dans Z/nZ }

> = # { k | 1 $\leq$ k $\leq$ n - 1, k est premier avec n }

Remarque 1: : Φ(1) = 1

Remarque 2: si p premier, # {k | 1 $\leq$ p - 1, et k premier avec p } = p - 1

Φ(p) = p - 1

n = 8 = 2^3

1 2 3 4 5 6 7 8

Φ(8) = 4

n = 9 = 3^2

1 2 3 4 5 6 7 8 9

Φ(9) = 6

En généralisant: n = p^v

1 2 … p (p + 1) … 2p … 3p … p^v

Sur les p^v 1 … p^v [0 … (p^v - 1)], exactement (1/p) * p^v (= p^{v-1}) divisibles par p

$\Phi(p^v)$ = p^v - p^{v-1} = p^{v-1} * (p - 1) = p^v (1 - (1/p))

Proposition

Si m et n premiers entre eux, Φ(mn) = Φ(m) * Φ(n)

Z/mnZ	$\leftrightarrows$	Z/mZ	Z/nZ
a	$\leftrightarrows$	a1	a2
inversible	$\leftrightarrows$	inversible	inversible
Φ(mn) = Φ(m) * Φ(n)	$\leftrightarrows$	Φ(m)	Φ(n)

Consequence:

Si n = $p_1^{v_1} \dots p_m^{v_m}$

Φ(n) = $\Phi(p_1 v_1 \dots \Phi(p_m v_m$ = $\prod_{i=1}^{m} p_i^{v_1 - 1}(p_i$ - 1)

> = $\prod_{i-1}^{m} p_i^{v_i}$(1 - (1/$p_i$)) = n $\prod$(1 - (1/p_i))

n $\leq 10^{1000}$

n = $p_1^{v_1} \dots p_m^{v_m}$

$2^m \leq p_1 \, p_2 \dots p_m \leq$ n $\leq 10^{1000}$

m * log2 $\leq$ 1000 * log10

m $\leq$ 1000 * ($\frac{log10}{log2}$) $\leq$ 3322

n = $p_1^{v_1} \dots p_m^{v_m}$

Φ(n) = $\prod_{i=1}^{m} p_i^{v_i - 1}(p_i$ - 1)

> = n $\prod_{i=1}^{m}$(1 - $\frac{1}{p_i}$)

Exemple

210	
210	2
105	3
35	5
7	7

Φ(210) = 2^0(2-1) * 3^0(3 - 1) * 5^0(5 - 1) * 7^0(7 - 1)

> = 2 * 4 * 6

> = 48

Si G est un groupe fini, avec n éléments

- en notation additif, (+, 0 élément neutre) $\forall$x $\exists$p, q $\in$ N p $\neq$ q px = qx (p - q)x = 0, un multiple rx = 0, nx = 0
- en notation multiplicative: G, x, 1 $\forall$x, x^n = 1

Z/nZ $\forall$ a $\in$ Z/nZ: na = 0

Elements inversibles de Z/nZ

Cet ensemble: note $(Z/nZ)^X$

$(Z/nZ)^X$ = Φ(n)

Proposition: $(Z/nZ)^X$, X est un groupe.

Il a Φ(n) éléments.

($\forall$a $\in$ Z/nZ) $a^{\Phi(n)}$ = 1

($\forall$a $\in$ Z) si (a, n) $a^{\Phi(n)}$ = 1 (mod n)

Structure du groupe additif Z/nZ

Z/nZ = {$\bar{0}$, $\bar{1}$, $\dots$, $\overline{n-1}$}

$\bar{0}$ = 0 * $\bar{1}$

$\bar{1}$ = $\bar{1}$ = 1 * $\bar{1}$

$\bar{2}$ = $\bar{1}$ + $\bar{1}$ = 2 * $\bar{1}$

> = {0 * $\bar{1}$, 1 * $\bar{1}$, …, (n - 1) * $\bar{1}$}

$\bar{1}$ est générateur de Z/nZ

Z/nZ est cyclique

a premier avec n $\leftrightarrows$ $\bar{a}$ générateur de Z/nZ

1. si $\bar{a}$ générateur, $\bar{1}$ est un multiple de $\bar{a}$! ∃k $\bar{1}$ = k * $\bar{a}$ = $\bar{k}$ * $\bar{a}$. $\bar{a}$ inversible dans Z/nZ, a premier avec n
2. Réciproquement, a premier avec n: Il existe s tq a * s $\equiv$ 1 mod n Soit $\bar{u}$ quelconque dans Z/nZ. $\bar{u}$ = u * $\bar{1}$ = u * $s \bar{*} a$ = u * $\bar{s}$ * $\bar{a}$ = (u * s) * $\bar{a}$ = (us) * $\bar{a}$ Le nombre de générateurs de (Z/nZ, +) est Φ(n)