Example

n premier $Z/nZ^*, X$

1
$2 \equiv 2^1$
$4 \equiv 2^2$
$8 \equiv 2^3$
$5 \equiv 2^4$
$10 \equiv 2^5$
$9 \equiv 2^6$
$7 \equiv 2^7$
$3 \equiv 2^8$
$6 \equiv 2^9$
$1 \equiv 2^{10}$

Groupe cyclique, 10 elements, φ(10) generateurs

$\forall$a $\in Z/nZ^* a^{10} \equiv$ 1 (mod 11)

Groupe Z/pZ^* quand p est premier

si g est un generateur

Z/pZ^* = { $1, g, g^2, g^3, ..., g^{p-2}$ }

On admet sans demonstration

($Z/pZ^*, X$) est un groupe cyclique

Il a p-1 elements.
Il a φ(p-1) generateurs.

Exemple

$p = 101$
$Z/101Z^*$ a 100 elements
$\varphi(100) = 40$ generateurs

$\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = 2 * 4 * 5^1 = 40$

$\forall a \in Z/nZ^*$ $a^{p-1} \equiv$ 1 (mod p)

Petit theoreme de Fermat

Pout tout a $\in Z$, p premier,
si $(a,p)=1$ $\quad a^{p-1} \equiv 1(modp)$

Soit e premier avec (p-1)

a $\in Z/pZ^* \longrightarrow a^e$

Cette application est inversible

Bezout: $ d et v tq: $de+v(p-1)=1$
d: image de e modulo (p-1)

$a^{ed} \equiv a^{ed+v(p-1)}$
$\equiv a$ (mod p)

Exemple

$p=11$
$g=2$
$p-1=10$
e premier avec 10
$e=3$
$d=7$ $(3*7=21)$

Si m $\in Z/11Z*$
$m \longrightarrow e=m^e=m^3$
$e \longrightarrow e^d=m=e^7$

Exemple

$m=5$
$e=5^3 \equiv 25*5 \equiv 3*5 \equiv 15 \equiv 4$
$e \equiv 4$
$4^7 \equiv 4*(4^2)^3 \equiv 4*5^3 \equiv 4*4 \equiv 16 \equiv 5$

$m'=2^u$
$c^1=2^{3u}$
$c^7=2^{21u}=2^u=m'$

Remarque 1

p premier
Z/pZ^* a φ(p-1) generateurs
$\longrightarrow$ “facile a trouver” si je peux factoriser p-1
$\longrightarrow$ si on connait g
$\longrightarrow$ etant donne a$\ trouver n tq $a \equiv g^n$ est $\underline{difficile}$

Remarque 2

p: premier
e: premier avec p-1
d: $ed \equiv 1$ (mod p-1)

$\forall a \in Z/pZ \qquad a^{ed} \equiv a$ (mod p)

Remarque 3

Premier $\underline{toy - algo}$
p: premier
e: premier avec p-1
$\hookrightarrow$ cle de l’algo
$m \longrightarrow c = m^e$

Remarque 4

Petit theoreme de Fermat
$\longrightarrow$ test de primalite

Propriete analogue avec n=pq, p et q: premiers

- $n = pq$
- e est premier avec $\varphi(n) = (p-1)(q-1)$
- d: $ed \equiv 1$ mod $\varphi(n)$
- Si m $\in Z/nZ$ quelconque

si $c \equiv m^e$ (mod n) alors $c^d \equiv m$ (mod n)

RSA (Rivest - Shamir - Adleman)

- On part de:
  - $n = pq$, p et q premiers
  - e: permier avec $\varphi(n) = (p - 1(q - 1)$
  - d: inverse de e modulo $\varphi(n)$
- Cle publique: n, e
- Cle privee: d
- m: message a chiffrer

Chiffrement(public) $m \longrightarrow c = m^e$
Dechiffrement(secret) $c \longrightarrow e^d = m$

Signature d'un message M

Fonction de Hashage H -connue-testee- tenir sur { 0, . . . , n-1 }

Alice $\longrightarrow$ Bob

Alice:

- cle publique: n, e
- secrete: d

Alice calcule:
$m = H(M)$
$c \equiv m^d$ (mod n)

Alice envoie a Bob: M, e

c est la signature de M

Bob:

1) $m = H(M)$
2) c =? m