

Example

n premier $\mathbb{Z}/n\mathbb{Z}^*, X$

$$1$$

$$2 \equiv 2^1$$

$$4 \equiv 2^2$$

$$8 \equiv 2^3$$

$$5 \equiv 2^4$$

$$10 \equiv 2^5$$

$$9 \equiv 2^6$$

$$7 \equiv 2^7$$

$$3 \equiv 2^8$$

$$6 \equiv 2^9$$

$$1 \equiv 2^{10}$$

Groupe cyclique, 10 elements, $\varphi(10)$ generateurs

$$\forall a \in \mathbb{Z}/n\mathbb{Z}^* a^{10} \equiv 1 \pmod{11}$$

Groupe $\mathbb{Z}/p\mathbb{Z}^*$ quand p est premier

si g est un generateur

$$\mathbb{Z}/p\mathbb{Z}^* = \{1, g, g^2, g^3, \dots, g^{p-2}\}$$

On admet sans demonstration

$(\mathbb{Z}/p\mathbb{Z}^*, X)$ est un groupe cyclique

Il a $p-1$ elements.

Il a $\varphi(p-1)$ generateurs.

Exemple

$$p = 101$$

$\mathbb{Z}/101\mathbb{Z}^*$ a 100 elements

$$\varphi(100) = 40 \text{ generateurs}$$

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

$$\forall a \in \mathbb{Z}/n\mathbb{Z}^* \quad a^{p-1} \equiv 1 \pmod{p}$$

Petit theoreme de Fermat

Pout tout $a \in \mathbb{Z}$, p premier,

$$\text{si } (a, p) = 1 \quad a^{p-1} \equiv 1 \pmod{p}$$

Soit e premier avec $(p-1)$

$$a \in \mathbb{Z}/p\mathbb{Z}^* \longrightarrow a^e$$

Cette application est inversible

Bezout: $\exists d$ et v tq: $de + v(p-1) = 1$

d : image de e modulo $(p-1)$

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

$$\equiv a \pmod{p}$$

Exemple

$$p = 11$$

$$g = 2$$

$$p-1 = 10$$

e premier avec 10

$$e = 3$$

$$d = 7 \quad (3 * 7 = 21)$$

Si $m \in \mathbb{Z}/11\mathbb{Z}^*$

$$m \longrightarrow e = m^e = m^3$$

$$e \longrightarrow e^d = m = e^7$$

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

$\mathbb{Z}/p\mathbb{Z}^*$ a $\varphi(p-1)$ generateurs

→ “facile a trouver” si je peux factoriser $p-1$

→ si on connaît g

→ étant donné $a \in \mathbb{Z}/p\mathbb{Z}^*$ trouver n tq $a \equiv g^n$ est difficile

Remarque 2

p : premier

e : premier avec $p-1$

d : $ed \equiv 1 \pmod{p-1}$

$$\forall a \in \mathbb{Z}/p\mathbb{Z} \quad a^{ed} \equiv a \pmod{p}$$

Remarque 3

Premier 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

→ 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 : $ed \equiv 1 \pmod{\varphi(n)}$
- Si $m \in \mathbb{Z}/n\mathbb{Z}$ quelconque

$$\text{si } c \equiv m^e \pmod{n} \text{ alors } c^d \equiv m \pmod{n}$$

RSA (Rivest - Shamir - Adleman)

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

Chiffrement(public) $m \rightarrow c = m^e$

Dechiffrement(secret) $c \rightarrow c^d = m$

Signature d'un message M

Fonction de Hashage H -connue-testee- tenir sur $\{0, \dots, n-1\}$

Alice \rightarrow Bob

Alice:

- cle publique: n, e
- secrete: d

Alice calcule:

$$m = H(M)$$

$$c \equiv m^d \pmod{n}$$

Alice envoie a Bob: M, e

c est la signature de M

Bob:

1) $m = H(M)$

2) $c \stackrel{?}{=} m$