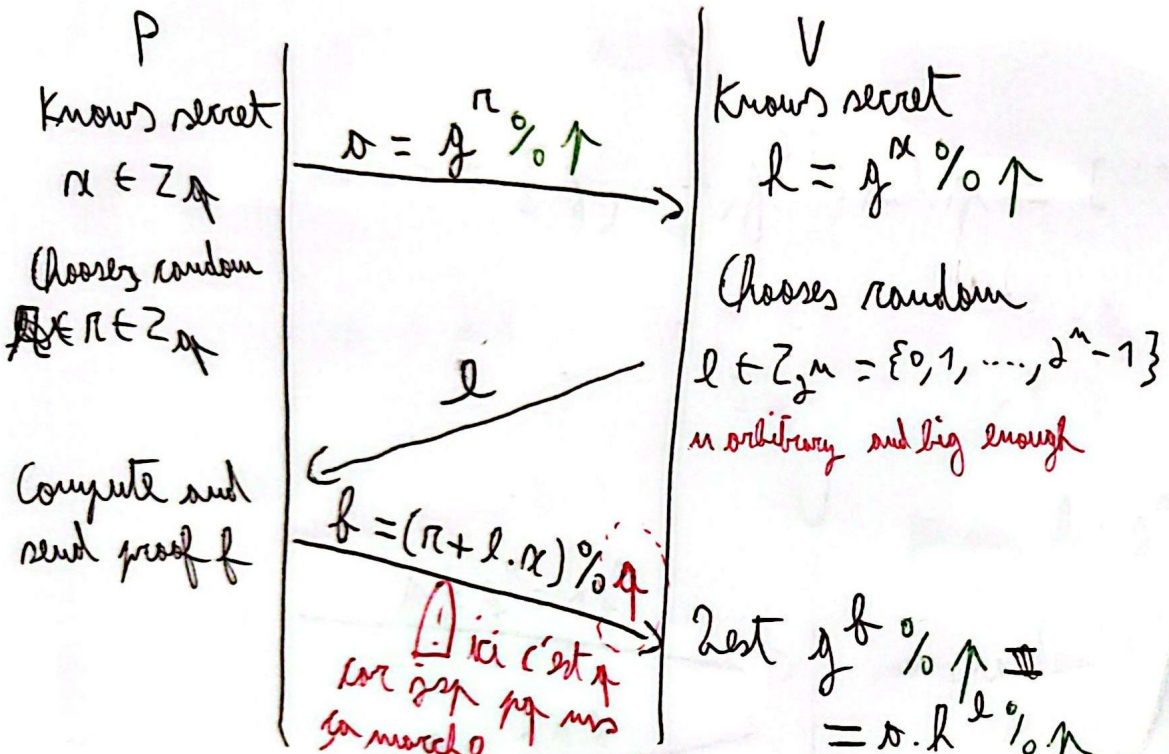
Note : $p \neq q$ et $q < p$, $\{p, q, g\}$ sont connus par P et V



Comment trouver q ? Avec $G = \langle g \rangle$

$q = |G| = \{g^1 \% p, \ldots, g^q \% p\} = \langle g \rangle$

Tel que $g^q \% p = 1$

Donc q est la taille de G

$G \neq \mathbb{Z}_p \wedge \mathbb{Z}_p \neq \mathbb{Z}_p^*$

$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$

$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$

↳ Pas de zéros

SCHNORR 0

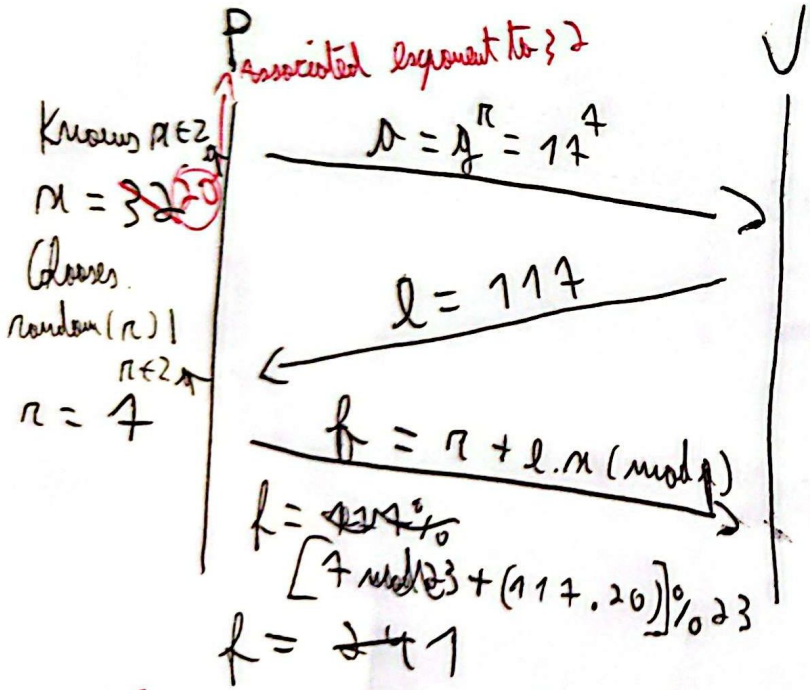
P chooses $p = 47$ $q = 17$ ~~$\Rightarrow x = 46 = 23 \cdot 2 \Rightarrow q = 23$~~

$Z_p^*[i] = g^i \% p \mid 1 \le i \le p$

$\mathbb{Z}_p^* \; G = \langle 17 \rangle = \{g, \dots, g^{23}\} \bmod p = [17, 7, 25, 2, 34, 14, 3, 4, 21, 28, 5, 8, 42, 9, 12, 15, 10, 17, 18, 19, 20, 27, 22, 23]$ = ~~$\mathbb{Z}_p^*$~~

$|G| = q = 23$ $\quad G \neq Z_p$ but $|G| = q$

$Z_p = \{0; \dots; p-1\}$



Knows $h = g^x = 17^{20}$ mod p

Chooses random(e) | $e \in Z_{2^m} = \{0; \dots; 2^m - 1\}$

Test $g^f = a \cdot h^e \Leftrightarrow g^f = a \cdot h^e = g^r \cdot (g^x)^e \pmod p$

$\Leftrightarrow 17^{7} \% 47 = (17^7 \cdot (17^{20})^{117}) \% 47$

$17 = 17$

if $a = g^r \bmod p$ and $h = g^x \bmod p$ is it still correct ?

$\Rightarrow a = 20^3$ et $h = 20^{32}$ donc $f = 7$ (inchangé) $\Rightarrow 17^7 \% 47 = (20^3 \cdot (20^{32})^{117}) \% 47$

SCHNORR 1

EXAMPLE

$p = 47 \wedge g = 17$ (1 2 3 4 5)

6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

$G = \langle 17 \rangle = [17, 7, 25, 2, 34, 14, 3, 4, 21, 28, 6, 8, 42, 9, 12, 16, 37, 18, 24, 32, 27, 30, 1]$

$\Rightarrow \boxed{|G| = p = 23}$

$\Rightarrow \mathbb{Z}_p = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, \cancel{23}\}$

```
for i in range(1, 100000):
    tmp = g**i % p (= 17^i % 47)
    G.append(tmp)
    if tmp == 1:
        break
```

P

Suppose secret $x \in \mathbb{Z}_p$

$x = 14$

Choisit random $r \in \mathbb{Z}_p$, $r = 17$

$t = g^r \% p = 17^{17} \% 47$

$\Leftrightarrow t = 37$

$t \rightarrow$ V

Calcul preuve et envoie

$l = 41308$ ← V

$s = (r + l \cdot x) \% \cancel{47}\ p$

$s = (17 + 41308 \cdot 14) \% \cancel{47}$

$= \cancel{41}\ 17\ 23$

$s \rightarrow$ V

V

Du coup connait $h = g^x \% p = 17^{14} \% 47 = 9$

Choisit random $l \in \mathbb{Z}_M$

On dit arbitrairement $M = 1000$

donc $l = 41308$

Test $g^s \% p = (t \cdot h^l) \% p$

$\Leftrightarrow 17^{17} \% 47 = (37 \cdot 9^{41308}) \% 47$

$\Leftrightarrow \boxed{37 = 37}$ SUCCESS