TD - Cryptographie par résidu quadratique

1. Dénombrement des carrés dans $\mathbb{Z}/n\mathbb{Z}^\star$

a. $(b-x)^2 = b^2 - 2bx + x^2 = x^2 = a \mod b$.

b. $a = x^2 + kpq$; donc $a \equiv x^2 \mod p$ est un carré modulo p (de même pour q).

c. Soit x et y distincts tels que $a = x^2 = y^2 \mod p$. D'où $x^2 - y^2 = (x-y)(x+y) = 0 \mod p$. Comme $\mathbb{Z}/p\mathbb{Z}$ est intègre (car p est premier) et $x - y \neq 0 \mod p$, on en déduit que $x + y = 0 \mod p$; d'où $y = p - x$.

d. D'après b., tout carré $a \mod n$ est un carré $\mod p$ et $\mod q$. Comme $a \neq 0 \mod p$, a admet exactement 2 racines $u_1 = u$ et $u_2 = p - u$ modulo p (resp. $v_1 = v$ et $v_2 = q - v$ modulo q). On en déduit, par le théorème chinois des restes, l'existence de exactement 4 racines distinctes pour a dans n : $u_i.q.q^{-1[p]} + v_j.p.p^{-1[q]} \mod n$ avec $1 \leq i, j \leq 2$.
D'après a., on déduit que ces racines s'écrivent nécessairement x_1, $n - x_1$, x_2 et $n - x_2$.

e. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z}^\star, .)$ qui est cyclique. Supposons qu'il existe x tel que $g = x^2$. D'après Fermat, $g^{p-1} = 1 \mod p$; comme g est générateur et p impair, on en déduit que $g^{\frac{p-1}{2}} = -1$. D'où $x^{p-1} = -1 \neq 1$ car $p \neq 2$. Donc, d'après le théorème de Fermat, x n'appartient pas à $\mathbb{Z}/p\mathbb{Z}$. Ainsi, g n'est pas un carré modulo p.
On en déduit que les seuls carrés non nuls sont les éléments g^{2i}; il y en a $\frac{p-1}{2}$.
NB: g^{2i} a deux uniques racines carrées: $x = g^i$ et $g^{i+\frac{p-1}{2}} = -x = p - x$.

f. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z}^\star, .)$ qui est cyclique. Par le théorème chinois des restes, à tout couple de carré $(u, v) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, on associe un et un seul carré dans $\mathbb{Z}/n\mathbb{Z}$. En comptant 0, il y a $\frac{p+1}{2}$ carrés modulo p. D'où $\frac{(p+1)(q+1)}{4}$ carrés modulo n, soit $\frac{n+p+q-3}{4}$ carrés non nuls modulo n.

2. Difficulté du calcul des racines carrées.

a. $u.v = x_1^2 - x_2^2 = a^2 - a^2 = 0 \mod n$.

b. On peut supposer $1 \leq x_1, x_2 < n$. Comme $x_1 \neq x_2$, $u = x_1 - x_2 \neq 0$. Comme $x_1 \neq n - x_2$, $v = x_1 + x_2 = x_1 - (n - x_2) \neq 0$. Donc $1 \leq u, v < n$.
On a $u.v = k.n$; donc $n = p.q$ divise $u.v$. Comme $u < p.q$, et p et q premiers, on en déduit que p divise u ou q divise u mais $p.q$ ne divise pas u. Donc pgcd(n, u) fournit un des 2 facteurs de n et $n/pgcd$(n,u) l'autre.

c. Il suffit de faire une addition, un pgcd et une division. Le coût dominant est le pgcd; par Euclide, cela donne un coût en $O(t^2)$ (ou $O(t \log^2 t \log\log t)$ par Schonhagge).

d. Calculer $x^2 \mod n$ se calcule efficacement en $O(t^{1+\epsilon})$. Par contre le calcul de sa réciproque est plus difficile que la factorisation; en effet, si on sait calculer les racines carrées de $a \mod p$, on sait factoriser a. Comme la factorisation est un problème réputé difficile, on en déduit que *carré* peut être considérée comme une fonction à sens unique.

3. Protocole d'identification quadratique.

a. On ne connaît pas d'algorithme rapide (inférieur à 5 ans disons, la durée d'un passeport) pour factoriser un entier de 512 bits. Donc, on peut supposer que personne ne connaît p et q sauf TTP.
De plus, on peut supposer que personne ne connaît x_A sauf Alice et éventuellement TTP. La seule solution pour calculer x_A est alors d'extraire la racine carrée de $a \mod n$; d'après 2., ce calcul des racines carrées x_a de a est plus difficile que factoriser n. Donc on peut supposer que personne ne connaît x_A. L'hypothèse est donc raisonable.
Hors-question: en fait, même si cela n'est pas demandé, on peut supposer que TTP, qui connaît p et q ne connaît pas x_A. En effet, connaitre x_A à partir de a demande de savoir calculer des racines carrées modulo p. Or, montrons qu'alors TTP saurait calculer le log discret, qui est supposé difficile. En effet, soit g un générateur de $\mathbb{Z}/p\mathbb{Z}^\star$. Soit $y < p$; en calculant une racine carrée de $y \mod p$ (ou de y/g si y n'a pas de racine carrée), TTP peut trouver y_1 tel que $y_1^2 = y$. Si $y_1 = g$, il en déduit l'indice de y: 2 (ou 1). Sinon, en réitérant ce calcul de racine carré à partir de y_1 jusqu'à trouver $y_k = g$, il peut en déduire l'indice i de y_1; et donc l'indice $2.i$ (ou $2.i + 1$) de y. TTP saurait donc calculer le log discret modulo p.

b. Si l'on ne sait pas calculer les racines carrées, r étant pris au hasard, la connaissance de y n'est d'aucune utilité. La seule solution pour calculer r est alors d'utiliser z; mais calculer r à partir de z est équivalent à calculer x_A. La seule solution pour calculer r est donc de connaître x_A.
On en déduit que Bob peut ainsi identifier Alice.

c. D'après 2., sans connaître la clef de Alice et sans savoir calculer les recines carrées, la seule solution pour l'espion est de tricher. Il doit parier sur ce que Bob va lui envoyer (0 ou 1) pour envoyer y. Mais sa probabilité de parier juste à 1 tirage est $1/2$. Donc sa probabilité de tromper Bob après k tirages est inférieure à 2^{-k}.