Recherche de générateurs

Soit $p \geq 3$ un nombre premier. Le groupe $\mathbf{G} = \mathbb{Z}_p^*$ est cyclique. Le but de cet exercice est de trouver un générateur de ce groupe, i.e., un élément g tel que $\mathbb{Z}_p^* = \{g^k, k \in \mathbb{Z}\}$. Pour $g \in \mathbf{G}$, l'ordre de g est le plus petit $k > 0$ tel que $g^k = 1$, noté $\mathrm{ord}(g)$.

Question 1. *Montrer que pour tout $g \in \mathbf{G}$, $\mathrm{ord}(g) \,|p-1$.*

Question 2. *Donner un élément de $\mathbf{G}$ qui n'est pas un générateur de $\mathbf{G}$. Combien d'éléments de $\mathbf{G}$ sont générateurs ?*

On se restreint au cas où $p - 1 = 2q$ pour q premier.

Question 3. *Donner un algorithme efficace qui trouve un générateur de $\mathbf{G}$. Comment trouver un tel premier p ?*

Algorithme de Shanks

Soit $\mathbf{G}$ un groupe cyclique généré par g, d'ordre premier q connu, et $h \in \mathbf{G}$.

Question 4. *Soit $m = \lceil \sqrt{q} \rceil$. Montrer qu'il existe $i, j \leq m$ tels que : $g^i = h(g^{-m})^j$.*

Question 5. *En déduire un algorithme de résolution du DLP, et sa complexité.*

Algorithme Rho de Pollard

Soit $\mathbf{G}$ comme dans la question précédente, $F : \mathbf{G} \to \mathbb{Z}_q$ une fonction non-nulle, et $H : \mathbf{G} \to \mathbf{G}$ définie par $H(\alpha) = \alpha \cdot h \cdot g^{F(\alpha)}$. Nous étudions l'algorithme suivant.

Algorithm 1 Algorithme Rho de Pollard.

Input : deux éléments $h, g \in \mathbf{G}$
Output : $x \in [0; q-1]$ tel que $h = g^x$ ou $\perp$

$i \leftarrow 1$, $x \leftarrow 0$, $\alpha \leftarrow h$
$y \leftarrow F(\alpha), \beta \leftarrow H(\alpha)$
while $\alpha \neq \beta$ **do**
    $x \leftarrow x + F(\alpha) \mod q, \alpha \leftarrow H(\alpha)$
    $y \leftarrow y + F(\beta) \mod q, \beta \leftarrow H(\beta)$
    $y \leftarrow y + F(\beta) \mod q, \beta \leftarrow H(\beta)$
    $i \leftarrow i + 1$
end while
if $i < q$ **then**
    Return $(x - y)i^{-1} \mod q$
else
    Return $\perp$
end if

Nous définissons inductivement la séquence (γ_i) par $\gamma_1 = h$ et $\gamma_{i+1} = H(\gamma_i)$ pour $i \geq 1$.

Question 6. *Montrer que dans la boucle While de l'algorithme, on a $\alpha = \gamma_i = g^x h^i$ et $\beta = \gamma_{2i} = g^y h^{2i}$.*

Question 7. *Montrer que si on sort de la boucle avec $i < q$, alors l'algorithme renvoie le logarithme discret de h en base g.*

Question 8. *Soit j le plus petit entier tel que $\gamma_j = \gamma_k$ pour $k < j$. Montrer que $j \leq q + 1$ et qu'en sortant de la boucle on a $i < j$.*

Question 9. *Montrer que si F est une fonction aléatoire, alors le temps d'exécution moyen de l'algorithme est en $\mathcal{O}(q^{1/2})$ multiplications dans $\mathbf{G}$. Comment l'implémenter dans la pratique ?*

Collisions des Fonctions de Hachage

L'algorithme rho est un exemple particulier de l'algorithme de recherche de cycles de Floyd, que nous allons maintenant utiliser pour trouver une collision dans une fonction de hachage $H : \{0,1\}^n \to \{0,1\}^n$ (notez que pour une fonction de hachage quelconque, il doit d'abord réduire arbitrairement la taille de son entrée à n bits).

Soit X_0 une valeur de départ ; on définit la séquence $X_{i+1} := H(X_i)$. Comme elle prend des valeurs dans un ensemble fini, elle est périodique après un certain point.

Soit c la longueur de la *pré-période* $X_0, \ldots, X_{c-1}$ et ℓ la longueur du *cycle*, tels que : • $X_0, \ldots, X_{c+\ell-1}$ sont tous distincts ; • pour tout $i \geq c$, $X_{i+\ell} = X_i$. On admet que pour une fonction aléatoire, $c = \mathcal{O}\big(2^{n/2}\big)$ et $\ell = \mathcal{O}\big(2^{n/2}\big)$.

On exécute l'algorithme Algorithm 2 donné ci-dessous.

Algorithm 2 Algorithme de recherche de cycle de Floyd.

```
x ← H(X_0)
y ← H(H(X_0))
while x ≠ y do
    x ← H(x)
    y ← H(H(y))
end while
```

Question 10. *Justifier que l'algorithme renvoie un élément x appartenant au cycle.*

Question 11. *Donner un algorithme pour trouver la longueur ℓ du cycle.*

Si $c > 0$ et $\ell > 1$, on a :

$$H(X_{c-1}) = X_c = X_{c+\ell} = H(X_{c+\ell-1})$$

et par définition $X_{c-1} \neq X_{c+\ell-1}$. La paire $(X_{c-1}, X_{c+\ell-1})$ est donc une collision de H. Pour la trouver, on calcule deux nouvelles séquences partant de X_0 et X_ℓ. Le premier indice i tel que $X_i = X_{i+\ell}$ est égal à c.

Question 12. *En déduire qu'on peut calculer une collision de la fonction H en temps $\mathcal{O}\big(2^{n/2}\big)$ et mémoire $\mathcal{O}(1)$.*