Examen de cryptologie

Durée : 2 heures; cours et notes de cours autorisées; autres documents interdits.

Notation

Pour-tout entier n, Z_n^* désigne l'ensemble des nombres premiers avec n appartenant à $[1, n-1]$.

1 Problème

Soient un entier premier p et α un générateur de Z_p^* c'est à dire tel que $Z_p^* = \{\alpha^i \ mod \ p \mid 0 \leq i \leq p-2\}$. On suppose que ces deux quantités sont choisies de telle façon que les problèmes LOGDISCRET et DIFFIE-HELMANN sont difficiles.

On suppose que la communauté, y compris donc le Vérificateur, est convaincu que seul le Prouveur connaît $l := \log_\alpha(\beta)$ le logarithme discret en base α modulo p d'un entier public β (c.a.d l'unique entier $l \in [0, p-2]$ tel que $\beta = \alpha^l \ mod \ p$).

L'objet de ce problème est l'étude d'un protocole à divulgation nulle permettant au Prouveur de prouver sa connaissance de l au Vérificateur. Soit P le protocole suivant où le Prouveur a pour donnée privée l et où (p, α, β) ainsi qu'un paramètre de sécurité k sont publiques.

Faire k fois :
- Prouveur tire un nombre aléatoire $0 \leq j \leq p-2$.
- Prouveur calcule $\gamma := \alpha^j \ mod \ p$ et envoie γ au Vérificateur.
- Vérificateur tire aléatoirement un entier $i \in \{0, 1\}$.
- Vérificateur envoie i au Prouveur.
- Prouveur calcule $h := (j + i \cdot l) mod p$ et envoie h au Vérificateur.
- Vérificateur calcule $verif := (\alpha^h \equiv \beta^i \gamma \ mod \ p)$.
- Si (non $verif$) Vérificateur retourne NON.

FinFaire
Vérificateur retourne OUI.

Vous répondrez aux questions suivantes :

1. Ecrire précisément les problèmes LOGDISCRET et DIFFIE-HELMANN. Peut-on les comparer, si oui établir une preuve.

2. Que signifie qu'un protocole est consistant, significatif et à divulgation nulle ?

3. Quel est l'intérêt d'un tel protocole ? Citer d'autres protocoles les utilisant.

4. En fonction de p et k, calculer la complexité en temps du protocole P (si besoin est, réécrire plus proprement les instructions).

5. Prouver que P est consistant.

6. Prouver que P est significatif.

7. Prouver que P est à divulgation nulle.
   Pour cela, vous pourrez considérer des triplets *valides*, c'est à dire des triplets de la forme (γ, i, h) où $\gamma \in Z_p^*$, $i \in 0, 1$, $h \in Z_p^*$ et tels que $\alpha^h \equiv \beta^i \gamma \ mod\ p$. Vous pourrez démontrer que le nombre de triplets valides est exactement $2 \cdot (p-1)$ et que Vérificateur peut tous les construire.