MHT633 - Arithmétique et Cryptologie - Année 2009-2010

Examen du 6 mai 2010, durée 1h30

Documents interdits

Exercice 1 - Expliquez les principes de fonctionnement de la cryptographie symétrique et de la cryptographie asymétrique, en mettant en évidence les différences entre ces deux catégories, leurs avantages et leurs inconvénients respectifs. Vous pourrez illustrer votre réponse par un exemple de chaque catégorie, décrit aussi précisément que possible. Réponse limitée à une page.

Exercice 2 - Dans un protocole d'identification, un vérificateur V veut vérifier l'identité d'un prouveur P. Pour cela, P doit convaincre V qu'il est en possession d'un certain secret s. Les deux objectifs essentiels d'un tel protocole sont d'une part qu'un usurpateur U ne connaissant pas s ne puisse pas convaincre V, et d'autre part que P puisse convaincre V qu'il possède s sans lui révéler la valeur de s (sinon V pourrait devenir à son tour un usurpateur de l'identité de P).

Nous décrivons maintenant le protocole d'identification de Schnorr:
p et q sont des nombres premiers tels que q divise $p-1$ et α est un élément d'ordre q du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Un nombre $s \mod q$ est le secret de P, tandis que les valeurs de p, q, α, et $v := \alpha^{-s} \mod p$ sont publiques. Le protocole d'identification se déroule en quatre étapes:

(1. Engagement:) P choisit aléatoirement un entier $r \mod q$ et transmet $x = \alpha^r \mod p$ à V.

(2. Challenge:) V envoie un challenge $e \in [0, q-1[$ à P.

(3. Réponse:) P envoie $y = r + es \mod q$ à V.

(4. Vérification:) V vérifie que $x = \alpha^y v^e \mod p$.

P a réussit son identification auprès de V si la vérification est positive.

1. Montrer que P réussit toujours son identification auprès de V.

2. Comment doit-on choisir les nombres premiers p et q pour que personne d'autre que P ne puisse calculer s en un temps raisonnable ?

3. U tente de s'identifier auprès de V. Pour cela il répond un y aléatoire à l'étape 3. Quelles sont ses chances de succès ?

4. Supposons que le protocole précédent soit mal exécuté, et que l'ordre des étapes 1 et 2 soit inversé. Montrez que U peut alors réussir son identification auprès de V.

5. Montrez que, si pour un même engagement r, U est capable de répondre correctement à deux questions e et e' distinctes posées par V, alors il connait s.

Exercice 3 Dans cet exercice vous pouvez utiliser le résultat suivant: si n est un nombre premier, alors le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique.

1. Donnez la définition de l'ordre d'un élément dans un groupe.

2. On suppose n premier. Montrez qu'il existe un entier a tel que $a^{n-1} = 1 \mod n$ et tel que, pour tout nombre premier p divisant $(n-1)$, $a^{(n-1)/p} \neq 1 \mod n$.

3. Réciproquement, on suppose que n est un entier tel qu'il existe un entier a tel que $a^{n-1} = 1 \mod n$ et tel que, pour tout nombre premier p divisant $(n-1)$, $a^{(n-1)/p} \neq 1 \mod n$. Montrez que n est premier.

4. On souhaite utiliser les deux propriétés précédentes pour tester la primalité d'un entier n. À quelle difficulté se heurte-t-on ? Qu'en pensez-vous ?

5. On suppose maintenant que n est un entier tel que, pour tout nombre premier p divisant $(n-1)$, il existe un entier a_p tel que $a_p^{n-1} = 1 \mod n$, et $a_p^{(n-1)/p} \neq 1 \mod n$. Montrez que n est premier.