MHT633 - Arithmétique et Cryptologie - Année 2009-2010

Corrigé de l'examen du 6 mai 2010, durée 1h30

Documents interdits

Exercice 1 -

En cryptographie symétrique, une même clé K est utilisée pour le chiffrement et pour le déchiffrement, alors qu'en cryptographie asymétrique, une clé publique K_{pub} est utilisée pour chiffrée et une clé privée K_{priv} est utilisée pour déchiffrer. Rappelons que les clés paramétrisent les algorithmes de chiffrement et de déchiffrement, mais que ces algorithmes sont supposés connus de tous. Pour assurer la confidentialité en symétrique, il faut que les protagonistes de l'échange, Alice et Bob, possèdent tous les deux la clé K, mais pas l'attaquant Oscar. Le problème majeur est donc celui de l'échange initial de cette clé. En contrepartie, les algorithmes symétriques sont très rapides et utilisent des clés courtes (ex: 128 bits pour AES).

En asymétrique, seul le destinataire doit posséder K_{priv}, laquelle ne doit pas être en possession de l'attaquant Oscar. Par contre la clé publique K_{pub} peut être connue de tous donc il n'y a pas de problème d'échange de clé. Bien sur, on ne doit pas pouvoir calculer K_{priv} à partir de K_{pub}. Ces algorithmes sont plus lents et les clés sont plus grandes (ex: 1024 bits pour RSA).

Un exemple simple d'algorithme symétrique peut être pris parmi les chiffrements anciens (à détailler dans la rédaction); ces chiffrements sont abandonnés depuis bien longtemps. Un exemple d'algorithme symétrique moderne et sûr est l'algorithme Rijndael, actuel standard du chiffrement symétrique (AES). Pour le chiffrement asymétrique, RSA est l'exemple standard (à détailler dans la rédaction).

Exercice 2 -

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

   Comme P connait s, il calcule $y = r + es \mod q$ et le transmet à V. Alors

   $$\alpha^y v^e = \alpha^{r+es}\alpha^{-es} = \alpha^r = x \mod p$$

donc la vérification est positive.

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 ?

   Pour que le calcul de s soit impossible, il faut que le log discret en base α soit impossible à calculer en temps raisonnable. D'après ce qui a été vu en cours, il faut donc choisir q suffisamment grand pour qu'un algorithme générique comme Shanks, de complexité exponentielle, soit inefficace et p suffisament grand pour que l'algorithme "calcul d'index" qui lui est spécifique à $(\mathbb{Z}/pZ)^*$ et de complexité sous-exponentielle soit aussi inefficace, soit $q \approx 160$ bits et $p \approx 1024$ bits.

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 ?

   U réussit son identification si $x = \alpha^y v^e \mod p$, soit si $\alpha^y = xv^{-e} = \alpha^{r-se} \mod p$, ce qui est équivalent à $y = r - se \mod q$. Donc U a une chance sur q 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.

   U peut procéder de la façon suivante: il choisit d'abord y aléatoirement, puis calcule $x = \alpha^y v^e \mod p$. Notons qu'il n'a pas besoin de connaitre s pour cela, et que le calcul de x est " rapide". Il envoie ensuite x, puis y.

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.

   En effet, U a trouvé y tel que $y = r+es \mod q$ et y' tel que $y' = r+e's \mod q$. Alors $y-y' = (e-e')s$ et, comme $(e-e') \neq 0 \mod q$, $(e-e')$ est inversible modulo q. Il peut donc calculer s par la formule

$$s = (e - e')^{-1}(y - y') \mod q.$$

   Notons que pour cela il a seulement besoin d'inverser un entier modulo q et de multiplier deux entiers modulo q, toutes opérations "rapides".

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.

   Un élément g d'un groupe multiplicatif G de neutre e est d'ordre n si $g^n = e$ et si $g^d \neq e$ pour tout entier $1 \leq d \leq n-1$.

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 $(n-1)$, $a^{(n-1)/p} \neq 1 \mod n$.

   Si n est premier, d'un part le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est d'ordre $n-1$ et d'autre part il est cyclique. Donc il existe un élément a d'ordre $n-1$ dans ce groupe. Cela implique que $a^{n-1} = 1 \mod n$. Si p est un premier divisant n, notons $mp = (n-1)$. Alors $a^{(n-1)/p} = a^m \neq 1 \mod n$ sinon a serait d'ordre plus petit que 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.

   Notons d'abord que, si $a^{n-1} = 1 \mod n$ alors a est premier avec n et donc appartient au groupe $(\mathbb{Z}/n\mathbb{Z})^*$. Si on montre que a est d'ordre exactement $n-1$ dans ce groupe, on a terminé car on aura bien montré que ce groupe est d'ordre au moins $n-1$, donc bien égal à $(\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$. Or on sait que $(Z/n\mathbb{Z})$ est un corps si et seulement si n est premier.

   Soit maintenant d l'ordre de $a \mod n$. Alors d est un diviseur de $(n-1)$. Écrivons $(n-1) = dm$. Si $m > 1$, m a un diviseur premier p; soit $m = pm'$ et $(n-1) = dpm'$. Alors on aurait $a^{(n-1)/p} = a^{dm'} = (a^d)^{m'} = 1 \mod p$ ce qui contredit l'hypothèse.

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 ?

   On pourrait chercher aléatoirement un a répondant à ces conditions, mais pour tester ces conditions il faudrait connaitre la liste des diviseurs premiers de $(n-1)$. Si $(n-1)$ a seulement des petits diviseurs premiers c'est facile sinon c'est un problème difficile, équivalent au problème de la factorisation.

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.

Décomposons $(n-1)$ *en produit de puissances de nombres premiers:* $(n-1) = \prod_p p^{\alpha_p}$. *À partir de chaque* a_p, *on construit un élément* b_p *d'ordre exactement* p^{α_p}. *Pour cela, on écrit l'ordre* d_p *de* a_p *sous la forme* $d_p = p^{\delta_p} d'_p$ *avec* d'_p *premier à* p; *l'hypothèse sur* a_p *montre que* $\delta_p = \alpha_p$; $b_p = a_p^{d'_p}$ *convient. Alors, on montre facilement que* $a := \prod_p b_p$ *est d'ordre* $(n-1)$ *et donc* n *est premier.*