TD8 – Chiffrement asymétrique

Exercice 1. *Attaques sur El Gamal*

1. On veut montrer que le chiffrement El Gamal n'est pas CCA-sûr, c'est-à-dire qu'un attaquant qui peut demander le déchiffrement des messages de son choix peut avoir une probabilité de succès non-négligeable dans l'expérience d'indistinguabilité (on va en fait montrer une probabilité 1 de succès).
   L'attaquant produit des messages $m^0, m^1 \in G$ (quelconques), et reçoit un chiffré $c = (c_1, c_2)$ qui est soit le chiffré de m^0, soit le chiffré de m^1. Il demande alors le déchiffrement de $c' = (c_1, h \cdot c_2)$ où h est la clef publique.
   - **i.** Montrer que c' est bien le chiffré d'un message m' que l'on décrira.
   - **ii.** En déduire que l'attaquant peut avoir un succès avec probabilité 1.
2. On veut montrer que le chiffrement El Gamal est *malléable* : étant donné un chiffré c d'un message m, on peut calculer le chiffré c' du message $m' = \alpha \cdot m$ pour l'élément α de notre choix.
   - **i.** Montrer que si $c = (c_1, c_2)$, on peut calculer $c' = (c_1, c_2')$ qui soit le chiffré de $\alpha \cdot m$.
   - **ii.** L'attaque précédente n'est pas *discrète* : la première composante c_1 est inchangée. Montrer qu'on peut construire, étant donné c, un chiffré $c' = (c_1', c_2')$ de $\alpha \cdot m$ où $c_1' \neq c_1$ et $c_2' \neq c_2$. *Indication. Trouver une solution où $c_1' = c_1 g^r$ pour un r quelconque.*

Exercice 2. *Attaques sur RSA simple*

Dans cet exercice, on s'intéresse à RSA simple.

1. On veut montrer une attaque à chiffré choisi. Décrire un attaquant qui, étant donné la clef publique (N, e) et un chiffré c, peut calculer le message m tel que $m^e = N$ en temps polynomial. *Indication. L'attaquant peut demander le déchiffrement de chiffrés $c' \neq c$ de son choix, en particulier de $c' = r \cdot c$ pour n'importe quel r.*
2. On veut montrer qu'utiliser deux couples de clefs reliées au même module N est dangereux. On suppose que les clefs d'Alice sont (e_1, d_1), et celles de Bob sont (e_2, d_2), avec $\text{PGCD}(e_1, e_2) = 1$. Supposons qu'un attaquant Charlie intercepte deux chiffrés du même message m : c_1 chiffré avec e_1 et c_2 chiffré avec e_2. Montrer que Charlie peut calculer m à l'aide de l'algorithme d'Euclide étendu.

Exercice 3. *KEM basé sur El Gamal*

Le but de cet exercice est d'étudier un mécanisme d'encapsulation de clef (KEM), inspiré du chiffrement El Gamal. Formellement, un KEM est constitué de trois algorithmes Gen, Encaps et Decaps. Sur l'entrée 1^n, Gen produit un couple (pk, sk) de clefs publique et privée. L'algorithme Encaps prend en entrée la clef publique pk et produit un chiffré c et une clef $k \in \{0,1\}^{\ell(n)}$ pour une certaine fonction ℓ : on note $(c, k) \leftarrow \mathsf{Encaps}_{pk}(1^n)$. L'algorithme Decaps prend en entrée la clef secrète sk et le chiffré c et renvoie un clef $\hat{k}$. Le protocole est correct si lorsque $(c, k) \leftarrow \mathsf{Encaps}_{pk}(1^n)$, alors $\mathsf{Decaps}_{sk}(c) = k$.

1. *Construction naïve.* On peut créer un KEM à partir d'un chiffrement asymétrique, où Encaps tire simplement une clef k aléatoire et la chiffre avec la clef publique pk.
   - **i.** Soit $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ un protocole de chiffrement asymétrique. Décrire formellement les trois algorithmes Gen, Encaps et Decaps d'un KEM basé sur ce protocole.
   - **ii.** Préciser cette construction lorsque le protocole est le chiffrement El Gamal. *On fixe pour cela un groupe cyclique G d'ordre q, et un générateur g de G.*

On va décrire maintenant un KEM qui n'utilise pas directement et complètement le chiffrement El Gamal. On fixe un groupe cyclique G d'ordre q et un générateur g de G. On suppose disposer d'une fonction de hachage $H : G \to \{0,1\}^{\ell(n)}$. L'algorithme Gen est celui du chiffrement El Gamal, et produit une clef privée x et une clef publique $h = g^x$. Pour encapsuler une clef k, $\mathsf{Encaps}_{pk}(1^n)$ tire y dans $\{0, \dots, q-1\}$ uniformément, et renvoie $(c, k) = (g^y, H(h^y))$.

2. Écrire l'algorithme Decaps qui prend en entrée la clef secrète et le chiffré c, et renvoie la clef k.
3. Comparer la solution naïve et le KEM que l'on vient de décrire, en termes de quantités de calcul et de communications.