X. Exercices

8.1. *

Supposons qu'Alice et Bob partagent une clé aléatoire K dans $\{0,1,2\}$ et qu'Alice veuille envoyer à Bob un message M de $\{0,1,2\}$.
1) On suppose tout d'abord qu'elle procède en convertissant K et M en ensembles de deux bits (00, 01, 10) et qu'elle fait un XOR entre les deux représentations binaires. Montrer qu'un tel schéma n'est pas bon, en ce sens qu'il y a de l'information qui fuit et que ce schéma n'est pas parfaitement sûr. On pourra montrer que tous les chiffrés c_1, c_2 (où c_i est un bit) n'ont pas la même probabilité d'exister.
2) Proposer un autre schéma à base de modulo qui serait parfaitement sûr.

8.2. **

On considère les trois registres à décalage R_1, R_2 et R3, de polynômes de rétroaction respectifs $C_1(x) = x^3 + x + 1$, $C_2(x) = x^5 + x + 1$ et $C_3(x) = x^4 + x + 1$. On considère le générateur aléatoire obtenu en combinant les trois registres R_1, R_2 et R3 de sorties respectives x_1, x_2 et x_3, par la fonction booléenne $z = x_1 + x_2x_3$.
1) Expliquer pourquoi il est plus intéressant d'attaquer par corrélation le registre R_1 que les registres R_2 et R_3. Donner la corrélation entre x_1 et z par une table de vérité et de façon théorique.
2) On suppose que l'on observe pour le générateur combiné précédent la sortie 1000011100. Retrouver l'initialisation du registre R_1.

8.3. ✓ **

On considère un module R.S.A., $n = pq$ et d l'exposant privé. Soit un m un message à signer. On cherche à calculer $S = m^d \pmod n$. On note $d_p = d \pmod{p-1}$, $d_q = d \pmod{q-1}$ et $i_q = q^{-1} \pmod p$. Soient $S_p = m^{d_p} \pmod p$ et $S_q = m^{d_q} \pmod q$.
1) Rappeler le théorème des restes chinois. Montrer que $S \pmod p = S_p$ et $S \pmod q = S_q$. Expliquer alors pourquoi on peut retrouver S à partir de S_p et S_q.
2) Montrer que $S = S_q + q(i_q \cdot (S_p - S_q)) \pmod n$.
3) Expliquer l'intérêt (en termes de coût calculatoire) de calculer S par cette méthode plutôt que directement en calculant $m^d \pmod n$?

8.4. ✓ **

Supposons que l'on ait 3 modules R.S.A. N_1, N_2 et N_3 distincts, mais que chacun des systèmes utilise la valeur d'exposant 3. Montrer que si un même message m tel que $m^3 < N_1N_2N_3$ est envoyé pour les trois modules N_1, N_2 et N_3, alors il est possible de retrouver m par les restes chinois.

8.5. **

Soit $N = pq$ un module R.S.A. Soient $a \in (\mathbb{Z}/N\mathbb{Z})^*$ et $g = aN + 1 \pmod{N^2}$. On considère le schéma de chiffrement suivant. La clé publique est (N, g). Pour chiffrer un message $m \in (\mathbb{Z}/N\mathbb{Z})^*$, on procède de la façon suivante : on prend un h aléatoire dans $\{1, \cdots, N-1\}$ et l'on calcule $C = g^m.h^N \pmod{N^2}$. On voudrait trouver un algorithme de déchiffrement.
1) Soit $x \in \{1, \cdots, N-1\}$. Montrer que, pour un g donné et $B = g^x \pmod{N^2}$, il existe un algorithme efficace pour retrouver $x \pmod N$ (c'est-à-dire que, pour $0 < x < N$, le problème de logarithme discret en base g est facile). On pourra utiliser le fait que $g = aN + 1$.
2) Montrer que, si l'on connaît g et la factorisation de N, déchiffrer $C = g^m.h^N \pmod{N^2}$ peut être réalisé efficacement. Montrer que $C \pmod N = h^N \pmod N$.
3) On veut établir que l'on peut construire des chiffrés à partir de chiffrés connus (on appelle cette propriété la *malléabilité*). Montrer qu'étant donné N ainsi que le chiffré de x et y, il est possible de construire le chiffré de $x + y$ et le chiffré de $c.x$ pour c dans $(\mathbb{Z}/N\mathbb{Z})^*$. On dit alors que ce chiffrement est un homomorphisme additif.

8.6. ✓ **

On suppose qu'un groupe de n personnes qui n'ont pas de secret commun veulent partager un secret commun pour communiquer entre elles de manière confidentielle. Proposer un schéma basé sur l'échange de clé de Diffie-Hellman qui permette cela. Compter le nombre global d'exponentiations modulaires nécessaires. Essayer d'optimiser ce nombre, par rapport à chaque individu et globalement.

8.7. ✓ *

On considère le schéma de signature suivant. On suppose que l'on a une fonction de hachage f qui renvoie des hachés de longueur n. On va maintenant expliquer comment, à partir de f, on peut signer un message m de longueur k. Notons $m = (m_1, m_2, \ldots, m_k)$ avec $m_i \in \{0,1\}$. Pour $1 \leqslant i \leqslant k$ et $j \in \{0,1\}$, on prend $2k$ valeurs aléatoires y_{ij} de longueur k et l'on calcule $z_{ij} = f(y_{ij})$. Les $2k$ nombres z_{ij} forment la clé publique et les $2k$ nombres y_{ij} sont la clé secrète. Pour signer un message $m = (m_1, m_2, \ldots, m_k)$