Exercice 1 : Cryptographie asymétrique – Chiffrement de Paillier

Soient p et q deux nombres premiers impairs tels que $p \nmid q-1$ et $q \nmid p-1$ et $N = pq$.

1.a] Soient x et y deux entiers premiers avec N. Montrer que $x \equiv y \bmod N$ si et seulement si $x^N \equiv y^N \bmod N^2$.

1.b] Soit k un nombre entier tel que $\mathrm{pgcd}(k, N) = 1$ et soit $g = 1 + kN$. Montrer que g est d'ordre N dans $(\mathbb{Z}/N^2\mathbb{Z})^*$.

1.c] Montrer que tout élément $g \in (\mathbb{Z}/N^2\mathbb{Z})^*$ d'ordre N s'écrit $g = 1 + kN$ avec k un nombre entier tel que $\mathrm{pgcd}(k, N) = 1$.

1.d] Soit k un nombre entier tel que $\mathrm{pgcd}(k, N) = 1$ et soit $g = 1 + kN$. Donner un algorithme polynomial pour résoudre le problème du logarithme discret dans $\langle g \rangle \subset (\mathbb{Z}/N^2\mathbb{Z})^*$ le sous-groupe engendré par g. L'algorithme prendra en entrée N, g et $y \in \langle g \rangle$ et devra retourner en $O(\log(N)^c)$ opérations dans le groupe (pour une constante c indépendante de N à déterminer), la valeur $x \in \{0, 1, \ldots, N-1\}$ telle que $y = g^x \bmod N^2$.

Nous considérons le cryptosystème suivant (appelé chiffrement de Paillier) :

Génération de clés : L'utilisateur tire uniformément aléatoirement p et q deux nombres premiers impairs tels que $p \nmid q-1$ et $q \nmid p-1$ et poser $N = pq$. Soit k un nombre entier tel que $\mathrm{pgcd}(k, N) = 1$ et soit $g = 1 + kN$. La clé publique de l'utilisateur est (N, g) et la clé secrète est le couple (λ, μ) où $\lambda = \mathrm{ppcm}(p-1, q-1)$ et $\mu = (k\lambda)^{-1} \bmod N$.

Chiffrement : Étant donnée la clé publique (N, g), pour chiffrer un message m de l'ensemble $\{0, \ldots, N-1\}$, on tire uniformément aléatoirement un entier r dans $\{1, \ldots, N-1\}$ et on retourne le chiffré $c = g^m r^N \bmod N^2$.

Déchiffrement : Étant donnés un chiffré $c \in (\mathbb{Z}/N^2\mathbb{Z})^*$ et la clé secrète (λ, μ), le message clair associé à c est égal à $(\mu \cdot \frac{c^\lambda - 1}{N} \bmod N)$.

1.e] Montrer que le déchiffrement d'un chiffré d'un message m redonne bien la valeur m.

1.f] Expliquer pourquoi la valeur r utilisée lors du chiffrement est tirée dans $\{1, \ldots, N-1\}$ et non pas dans $\{1, \ldots, N^2-1\}$.

1.g] Donner des arguments appuyant la sécurité de ce cryptosystème (on pourra notamment discuter la difficulté de retrouver la clé secrète à partir de la clé publique et celle de retrouver le message clair à partir d'un chiffré).

1.h] Montrer comment calculer le chiffré du message $(m_1+m_2) \bmod N$ étant donnés les chiffrés de $m_1 \in \{0, \ldots, N-1\}$ et $m_2 \in \{0, \ldots, N-1\}$ (mais pas les valeurs m_1 et m_2 elles-mêmes). En déduire que le cryptosystème considéré n'est pas résistant à une attaque à chiffrés choisis adaptative.