**Université Claude Bernard Lyon 1**
**Institut de Science financière et d'Assurances (ISFA)**

50 avenue Tony Garnier
69007 Lyon, France

# Master 1 informatique
# Université Claude Bernard Lyon 1

## Cryptologie : TP n° 4

**Introduction :** Dans ce TP, nous nous intéressons à un autre cryptosystème à clé publique proposé par Pascal Paillier en 1999. Une partie de ce TP ne nécessite qu'un papier et un crayon : il s'agit de comprendre le cryptosystème, et de vérifier son bon fonctionnement.

**Génération des clès :** Pour la génération des clès, il n'y a normalement pas besoin de beaucoup se fouler, car le principe est le même que pour RSA... L'utilisateur qui souhaite créer une paire de clés commence par générer deux grands nombres premiers $p$ et $q$ (logiquement, pas n'importe comment...), puis calcule $N = p \cdot q$ et $\phi = (p-1) \cdot (q-1)$. Les clés sont
- la clé publique : $N$,
- la clé privée $(N, \phi)$.

**Chiffrement :** L'utilisateur qui souhaite chiffrer commence par se procurer la clé publique $N$ de son interlocuteur. Le message qu'il va transmettre est un entier $m$ tel que $0 \leq m < N$. Ensuite, il génère un entier $r$ aléatoire tel que $0 < r < N$. Il calcule alors le chiffré $c$ comme suit :

$$c = (1+N)^m \cdot r^N \mod N^2. \tag{1}$$

**Déchiffrement :** L'utilisateur qui reçoit un chiffré $c$ va le déchiffrer à l'aide de sa clé privée.

1. Montrez que $c \equiv r^N \pmod N$. Indication : $(1+N)^m = 1 + \sum_{i=1}^{m} \binom{m}{i} N^i$, d'après le formule du binôme.
2. Montrez que si $\mu$ est un entier tel que $\mu \equiv N^{-1} \pmod \phi$, alors $r \equiv c^\mu \pmod N$. Indications : utilisez l'équivalence de la question précédente, ainsi que le théorème d'Euler.
3. Montrez que $c \cdot r^{-N} \equiv 1 + m \cdot N \pmod{N^2}$. Indication : $(1+N)^m = 1 + m \cdot N + \sum_{i=2}^{m} \binom{m}{i} N^i$.
4. Vérifiez que $1 + m \cdot N = c \cdot r^{-N} \mod N^2$. Indication : il suffit de vérifier que $0 \leq 1 + m \cdot N < N^2$.
5. Déduire des questions précédentes que
$$m = \frac{(c \cdot r^{-n} \mod N^2) - 1}{N}. \tag{2}$$
6. Donnez l'algorithme pour déchiffrer $c$ en utilisant (2). Quel est le coût de cet algorithme ?
7. Quel est l'intérêt de $r$ dans ce chiffrement ?

**Application au vote électronique :** On note $C_N : (m, r) \to c$ la fonction de chiffrement d'après l'équation (1). Inversement, $D_\phi : c \to m$ désigne la fonction de déchiffrement d'après (2).

1. Montrez que, si $m_1, m_2$ sont deux messages et $r_1$, $r_2$ deux entiers tels que $0 \leq m_1, m_2, r_1, r_2 < N$ alors
$$D_\phi(C_N(m_1, r_1) \times C_N(m_2, r_2) \mod N^2) = m_1 + m_2 \mod N.$$
2. La relation précédente montre comment, en multipliant des chiffrés entres-eux, on peut « ajouter les messages en utilisant uniquement les chiffrés » : en utilisant cette propriété, décrivez un système de vote électronique basé sur le cryptosystème de Paillier.

**Implantation :** Implantez un système de référendum électronique utilisant le cryptosystème de Paillier : chaque votant utilise la clé publique pour envoyer un message chiffré codant « pour » ou « contre ». Un utilisateur utilise la clé publique pour compter les voix. L'organisateur du référendum doit pouvoir, à l'aide de la clé privée, le résultat du vote.