Université de Limoges
Faculté des Sciences et Techniques

Année universitaire ~~2016-2017~~ 2017-2018

Master 2 Math - CRYPTIS

Examen TP - Magma

- Durée 2h.
- Manuscrits et documents autorisés. Les documents du voisin ne sont pas des documents autorisés.
- Pour chaque programme, on rédigera des explications et on joindra le fichier source magma associé
- Les documents électroniques sont à envoyer par mail à `duong-hieu.phan@unilim.fr` avant la fin de l'épreuve

Vote elecronique avec le chiffrement de PAILLIER Soit $N = p \times q$ le produit de deux nombres premiers distincts. La fonction de chiffrement est défini par :

$$\begin{aligned} E : \ \mathbb{Z}_N \times \mathbb{Z}_N^* &\to \mathbb{Z}_{N^2}^* \\ (m, r) &\mapsto (1+N)^m r^N \end{aligned}$$

- Démontrer en mode d'écriture de texte que la fonction E est une bijection.
- Installer ce chiffrement avec Magma, avec un choix aléatoire de deux nombres premiers p et q de taille 256 bits.
- La fonction de chiffrement de PAILLIER a la propriété intéressante d'homomorphisme suivante :

$$E(m_1, r_1) \times E(m_2, r_2) = E(m_1 + m_2, r_1 r_2)$$

  Simuler un vote électronique pour deux candidats A et B : 1 pour A et 0 pour B.
  - Générer une suite binaire de 1000 bits aléatoire, stocker cette suite dans votre fichier
  - Chiffrer chaque bit de cette suite avec le chiffrement Paillier, puis multiplier toutes les chiffrées. Le résultat est stocké dans R.
- Étant donné la clé privée (p, q), décrire la fonction de déchiffrement en texte, puis déchiffrer R et conclure celui qui gagne.