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° 3

Cryptographie et théorème des restes chinois.

L'objectif de ce TP est d'illustrer l'usage du théorème des restes chinois en cryptographie à clé publique. Le premier exercice est une utilisation positive de ce résultat pour accélérer le déchiffrement RSA. Le second concerne son utilisation dans une attaque contre RSA.

Le théorème des restes chinois se trouve page 26 des slides `https://clarolineconnect.univ-lyon1.fr/resource/open/file/3418262`. Vous devez prendre le temps de l'étudier.

Exercice (Accélération du déchiffrement RSA)**.**

Il est possible d'utiliser le théorème des restes chinois pour accélérer le déchiffrement (et seulement le déchiffrement, car pour l'appliquer, il est nécessaire de connaître p et q qui font partie de la clé secrète).

L'idée est qu'au lieu de calculer le déchiffrement traditionnel $c^d \mod N$, on va commencer par faire des pré-calculs, puis effectuer des exponentiations modulaires modulo p, puis modulo q, et reconstituer le résultat final (le message en clair) modulo N.

Pour cela, j'appelle $d_p = d \mod p-1$ et $d_q = d \mod q-1$. J'appelle aussi $P = p^{-1} \mod q$ et $Q = q^{-1} \mod p$.

— Commencez par modifier votre méthode de génération des paires de clés (`KeyGen`) pour que ces pré-calculs soient faits dans celle-ci (vous voyez que ces valeurs ne dépendent pas du message ou du chiffré, donc peuvent être pré-calculées), et que d_p, d_q, P, Q fassent partie de la clé secrète.

Le déchiffrement se passe alors de la façon suivante. Vous commencez par calculer $c_p = c \mod p$ et $c_q = c \mod q$, puis vous calculez $m_p = c_p^{d_p} \mod p$ et $m_q = c_q^{d_q} \mod q$.

À ce stade, le message m (calculez normalement comme $c^d \mod N$) vérifie

$$\begin{cases} m = m_p \mod p \\ m = m_q \mod q \end{cases}$$

et vous voyez que vous êtes devant un système qui se résoud grâce au théorème des restes chinois.

— Crééez maintenant une méthode de déchiffrement `Decrypt_CRT` qui renvoie le message clair en finalisant cette procédure (notez qu'il va ralloir utiliser P et Q)

— Comparez expérimentalement le temps de déchiffrement de la méthode classique avec celui de la méthode `Decrypt_CRT`. Vous devez voir apparaître un facteur entre 2 et 4. Faites des tests sur des grands entiers (2000 ou 4000 bits).

Exercice (Cryptanalyse : RSA avec exposant public égal à 3)**.**

Trois utilisateurs Bob_1, Bob_2 et Bob_3 de RSA utilisent comme exposant public $e = 3$. On note alors leur clé publique respective $(3, N_1)$, $(3, N_2)$, $(3, N_3)$.

1. Pourquoi ces trois utilisateurs pourraient décider d'utiliser comme exposant public $e = 3$?

2. Alice chiffre un même message m à ces 3 utilisateurs. On note c_1, c_2 et c_3 les 3 chiffrés correspondants.
   Vous allez montrer, en utilisant le théorème des restes chinois, qu'un attaquant peut retrouver le message à partir de ces 3 chiffrés et des modules de Bob_1, Bob_2 et Bob_3, à l'aide d'un algorithme de racine cubique entière.

3. Implémentez cette attaque. Pour calculer des racines cubiques dans $\mathbb{Z}$, vous pouvez utilisez l'algorithme d'approximation de Newton.