Licence première année 2011-2012

M1MI2016 Codes et Cryptologie : feuille d'exercices 7

– Exercice 1. Calculer $25^{2012} \mod 56$ et $20^{2222222} \mod 33$.

(*Indication :* on pourra utiliser le théorème d'Euler.)

– Exercice 2. **Le test de primalité de Fermat** consiste à tester si un nombre est premier en vérifiant pour des valeurs de a que $a^p = a \mod p$.

Ce critère permet en pratique, en testant quelques petites valeurs de a, de détecter rapidement que certains nombres ne sont pas premiers.

Il existe en revanche des nombres non premiers tels que pour tout a premier avec n on ait $a^{n-1} = 1 \mod n$. Ces nombres sont appelés **nombres de Carmichael**.

1. Calculer $\varphi(561)$ et montrer que pour tout a premier avec 561, $a^{560} = 1 \mod 561$.
2. Montrer que si n, dont la décomposition en facteurs premiers est donné par $n = p_1 p_2 \cdots p_k$ où les p_i sont distincts, est tel que pour tout $1 \leq i \leq k$, $(p_i - 1)|(n-1)$ alors pour tout a premier avec n, $a^{n-1} = 1 \mod n$.

– Exercice 3. Alice et Bob utilisent le système de chiffrement RSA avec la clé publique $(N, e) = (2773, 51)$.

1. Factoriser N.
2. Quelle est la valeur de $\varphi(N)$?
3. Déterminer l'exposant de déchiffrement d.
4. Chiffrer le message $m = 1322$.
5. Déchiffrer le cryptogramme $c = 23$.

– Exercice 4. Soit une clé publique de chiffrement RSA (N, e).

1. Si un attaquant connaît $\varphi(N)$, comment peut il retrouver la clé privé ?
2. Même question connaissant p ou q.

– Exercice 5. On veut calculer x^k avec $x \in \mathbb{Z}$ et $k \in \mathbb{N}$.

1. Un premier algorithme naïf consiste à utiliser les formules suivantes :

$$x^0 = 1$$
$$x^k = x * x^{k-1}$$

   Quelle est sa complexité en nombre de multiplications ?

2. **L'algorithme d'exponentiation rapide**, plus astucieux, utilise les relations suivantes :

$$x^0 = 1$$
$$x^k = \begin{cases} x^{\frac{k}{2}} * x^{\frac{k}{2}} \text{ si k est pair} \\ x * x^{k-1} \text{ si k est impair} \end{cases}$$

   Pourquoi est-il particulièrement simple à formuler lorsque k est donné en base 2 ? Quelle est sa complexité ?

3. Calculer $54^{13} \mod 59$ et $563^{1234} \mod 612$.

– Exercice 6. Pour accélérer le déchiffrement RSA, on peut utiliser le théorème des restes chinois de la manière suivante. On suppose que les clés ont été générées à partir des nombres premiers p et q. Soit d la clé privée, on définit $d_p = d \mod (p-1)$ et $d_q = d \mod (q-1)$, ainsi que $u_p = p^{-1} \mod q$ et $u_q = q^{-1} \mod p$.

Pour déchiffrer le cryptogramme c provenant d'un message m, on calcule :

$$x_p = c^{d_p} \mod p$$
$$x_q = c^{d_q} \mod q$$
$$x = x_p u_q q + x_q u_p p \mod N$$

1. Montrer qu'on a bien $x = c^d$ et donc $x = m$.
2. Pour $p = 1511$, $q = 2003$ et $d = 1234577$, calculer d_p, d_q, u_p, u_q et déchiffrer $c = 152702$.

– Exercice 7. Le nombre $N = 16459$ est utilisé pour un chiffrement RSA. Sachant que $12534^2 = 1 \mod N$, utiliser un calcul de PGCD pour trouver la factorisation de N.