Licence 3 – MHT633 Université Bordeaux 1
2009/2010

Feuille 3 : RSA

Exercice 1. Théorème chinois

1. Soit $a, b \in \mathbb{Z}$ premiers entre eux. On considère l'application suivante :

$$\begin{array}{cccc} \Phi & \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & x \mod ab & \longmapsto & (x \mod a, x \mod b) \end{array}$$

   Montrer que Φ est un isomorphisme d'anneaux.

2. Expliciter Φ^{-1}.

Exercice 2. Indicatrice d'Euler

Soit φ la fonction indicatrice d'Euler définie sur $\mathbb{N}$ par

$$\varphi(n) = |\{k \in \mathbb{N} \text{ tel que } 1 \leq k \leq n \text{ et } \operatorname{pgcd}(k, n) = 1\}|$$

1. Montrer que $\varphi(n)$ est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.
2. Soit p un nombre premier et $k \in \mathbb{N}$. Calculer $\varphi(p)$ et $\varphi(p^k)$.
3. Se servir du théorème chinois pour établir que si

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

   est la décomposition en produit de facteurs premiers de n on a

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Exercice 3. Le groupe $(\mathbb{Z}/pq\mathbb{Z})^\times$

Soit p et q deux nombres premiers distincts et $n = pq$.

1. Déterminer les inversibles de $\mathbb{Z}/n\mathbb{Z}$.
2. Calculer l'ordre du groupe $(\mathbb{Z}/pq\mathbb{Z})^\times$.
3. Faire le lien avec l'indicatrice d'Euler.

Exercice 4. Ordre d'un élément

1. Si $x^a = 1$ pour un entier naturel a et un élément x de $(\mathbb{Z}/n\mathbb{Z})^\times$, montrer que l'ordre de x divise a.
2. Montrer que pour tout x de $\mathbb{Z}/p\mathbb{Z}$ on a $x^p = x$.
3. Montrer que pour tout x de $(\mathbb{Z}/n\mathbb{Z})^\times$ on a $x^{\phi(n)} = 1$.
4. En déduire une façon de calculer l'inverse de x dans $(\mathbb{Z}/n\mathbb{Z})^\times$, qui ne fasse pas appel à l'algorithme d'Euclide étendu. Application : calcul de l'inverse de 7 dans $(\mathbb{Z}/15\mathbb{Z})^*$.

Exercice 5. Chiffrement RSA

1. Soit $n = pq$ où p et q sont des nombres premiers distincts. Le système RSA chiffre $x \in \mathbb{Z}/n\mathbb{Z}$ en $x^b \in \mathbb{Z}/n\mathbb{Z}$. Puis on déchiffre $y \in \mathbb{Z}/n\mathbb{Z}$ par $y^a \in \mathbb{Z}/n\mathbb{Z}$ pour $a \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{\varphi(n)}$
   (a) Quelle est la clé publique ? la clé privée ?
   (b) Montrer que si $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ alors $d \circ e(x) = x$.
   (c) La composée de deux chiffrements RSA est-elle un chiffrement RSA ?
   (d) Dans cette question on fixe p et q deux nombres premiers distincts. Combien a-t-on de choix de clé ?
2. Dans cette question on souhaite implémenter un système RSA avec $n = 221$.
   (a) Calculer $\varphi(n)$.
   (b) Vérifier que l'on peut choisir 7 comme exposant de chiffrement.
   (c) Chiffrer le message $M = 3$ pour cette exposant.
   (d) Calculer l'exposant de déchiffrement. Préciser alors la clé publique et la clé privée.
   (e) Déchiffrer le message $C = 2$.

Exercice 6. Mauvais choix de p et q

On note (n, b) la clé publique d'un système RSA.

1. Si $n = 35$ déterminer tous les b possibles.
2. Si $n = 211 \times 499$ peut-on prendre $b = 1623$?
3. Si la clé publique est $(407109, 11309)$, quelle est la clé privée ?
4. Même question avec $(2173, 361)$. Lequel de ces deux choix de clé privée est le plus judicieux ? Que doit-on éviter dans les choix de p et q ?

Exercice 7. Déchiffrement de RSA

Dans cette exercice, on montre comment on peut accélérer le déchiffrement du système RSA en utilisant le théorème des restes chinois.
Soit $n = pq$ produit de deux nombres premiers et $d \in \mathbb{N}$. Supposons que la fonction de déchiffrement de RSA soit donnée par : $d_K(y) = y^d \pmod{n}$.

1. Calculer $y_p = y^d \pmod{p}$ et $y_q = y^d \pmod{q}$.
2. Résoudre le système dans $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{cases} x \equiv x_p \pmod{p}, \\ x \equiv x_q \pmod{q}. \end{cases}$$

   Justifier que si x est solution du système ci dessus alors $x \equiv y^d \pmod{n}$.
3. En utilisant cette méthode déchiffrer le message $C = 2$ pour $n = 221 = 13.17$ et $d = 63$.

Exercice 8. Connaître p et q, c'est connaître $\varphi(n)$

On suppose que n est un entier naturel non nul dont la décomposition en facteurs premiers est $n = pq$.

1. Exprimer $\varphi(n)$ en fonction de p et q.
2. Exprimer pq et $p+q$ en fonction de n et $\varphi(n)$. En déduire une méthode pour obtenir p et q lorsque l'on connait n et $\varphi(n)$.
3. Si $n = 17063$ et $\varphi(n) = 16800$, calculer p et q.

Exercice 9. Test de Fermat

Dans cet exercice on décrit un test de primalité utilisant le petit théorème de Fermat et plus précisément en étudiant sa réciproque.

1. Rappeler le petit théorème de fermat.

   On dit qu'un nombre n est pseudo premier en base a si n n'est pas premier et vérifie l'égalité :

$$a^{n-1} \equiv 1 \pmod{n}$$

2. Dans cette question on montre l'existence d'une infinité de nombre premier en base a.
   (a) Soit $a \geq 2$ un entier, $p > 2$ un nombre premier tel que $p \nmid a(a^2-1)$. On pose :

$$n = \frac{a^{2p}-1}{a^2-1}$$

   Montrer que n n'est pas premier.

(b) Montrer que $a^{2p} \equiv 1 \pmod{n}$.

(c) Calculer $(a^2-1)(n-1)$, puis montrer que $p \mid n-1$.

(d) Montrer que $2 \mid n-1$.

(e) Conclure que n est pseudo premier en base a. En déduire que pour tout $a \geq 2$ il existe une infinité de nombre pseudo premier en base a.

3. Un entier $n \geq 2$ est appelé nombre de Carmichaël si n n'est pas premier et si pour tout a premier avec n on a $a^{n-1} \equiv 1 \pmod{n}$.

(a) Soit $n = p_1 \dots p_k$ tel que $p_i - 1 \mid n-1$ pour tout $1 \leq i \leq k$. Montrer que $a^{n-1} \equiv 1 \pmod{p_i}$ pour tout a premier avec n et pour tout $1 \leq i \leq k$.

(b) Conclure.