Licence 3 – MHT633 Université Bordeaux 1
2009/2010

Feuille 3 : RSA

Exercice 1. 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 2. 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 $(492153, 2237)$, 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 3. Une majoration de la complexité de l'algorithme d'Euclide

Soient a et b deux entiers tels que $a > b$. On note $r_0 = a$ et $r_1 = b$. On applique l'algortihme d'Euclide à a et b de la manière suivante :

$$\begin{aligned} a = r_0 =& r_1 q_1 + r_2 \\ r_1 =& r_2 q_2 + r_3 \\ &\vdots \\ r_{n-2} =& r_{n-1} q_{n-1} + r_n \end{aligned}$$

où $r_n = \mathrm{pgcd}(a, b)$. L'objectif de cet exercice est de majorer la complexité de l'algorithme d'Euclide. On rappelle que la complexité de la division euclidienne de x par y peut s'écrire $\mathcal{O}(\log y \log q)$ où q est le quotient de la division euclidienne de x par y.

1. Montrer que la complexité est majorée par $\mathcal{O}\big(\log b \log\left(\prod_{i=1}^{n} q_i\right)\big)$.
2. Prouver que pour $k = 1, \ldots, n$, on a $a > r_k q_k q_{k-1} \ldots q_1$. Conclure.
3. En remarquant, que la multiplication et la division euclidienne ont la même complexité, que peut-on dire de la complexité de l'algorithme d'Euclide étendu.

Exercice 4. 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 $x_p = y^d \pmod{p}$ et $x_q = y^d \pmod{q}$.
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. Sachant que la complexité de l'algorithme d'Euclide étendu entre deux entiers a et b est $\mathcal{O}(\log a \log b)$. Calculer la complexité de cet algorithme de déchiffrement Comparer avec la complexité de l'algorithme de déchiffrement naïf.
4. En utilisant cette méthode déchiffrer le message $C = 2$ pour $n = 221 = 13.17$ et $d = 63$.

Exercice 5. 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 6. Une attaque sur RSA : petit exposant public commun

On suppose que k personnes $B_1, \ldots, B_k$ ont pour exposant public RSA $e = 3$ avec des modules respectifs n_i, $1 \leq i \leq k$.

1. Pourquoi est-il raisonnable de supposer que les n_i, $1 \leq i \leq k$ sont deux à deux premiers entre eux ?
2. Alice envoie les chiffrés d'un même message m à tous les B_i. Montrer qu'un attaquant peut déterminer m^3 modulo $P := \prod_{i=1}^{k} n_i$; en déduire qu'il peut calculer m si $P > m^3$.
3. Quel est la valeur minimale de k qui permet de toujours faire cette attaque ?

Exercice 7. Une attaque sur RSA : module commun

Bob et Catherine ont choisi le même module RSA n. Leurs exposants publics e_B et e_C sont distincts.

1. Expliquez pourquoi Bob peut déchiffrer les messages reçus par Catherine et réciproquement.
2. On suppose que e_B et e_C sont premiers entre eux et qu'Alice envoie les chiffrés d'un même message m à Bob et à Catherine. Expliquez comment l'attaquant Oscar peut obtenir m.
3. Application : Bob a la clef publique $(221, 11)$ et Catherine la clef $(221, 7)$. Oscar intercepte les chiffrés 210 et 58 à destinations respectives de Bob et Catherine. Retrouver le message m.

Exercice 8. Module RSA avec deux facteurs proches

Supposons que n soit un entier produit de deux nombres premiers p et q, $p > q$. On suppose que p et q sont proches, c'est à dire que $\epsilon := p - q$ est petit. On pose $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$.

1. Montrer que $n = t^2 - s^2$.
2. Quel est la taille de s ? Comparer t et $\sqrt{n}$.
3. Montrer comment utiliser cela pour écrire un algorithme (de Fermat) factorisant n.
4. Application : factoriser 11598781.
5. Déterminer le nombre d'itérations de l'algorithme en fonction de p et de n. Que se passe t'il si $p - \sqrt{n} < \sqrt[4]{4n}$?

Exercice 9. Dans RSA, connaître d est équivalent à connaître p et q

Supposons que n soit un entier produit de deux nombres premiers distincts p et q. On note e, premier avec $\varphi(n)$, l'exposant public d'un système RSA de modulo n. Connaissant p et q, l'exposant privé d se calcule en temps polynomial. Le but de l'exercice est de montrer que si un attaquant connaît d alors il peut factoriser n en temps polynomial.

1. Montrer comment à partir de e, d et n on peut construire un multiple B de $\varphi(n)$.
2. On note $\lambda = \mathrm{ppcm}(p-1, q-1)$.Montrer que pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^\times, a^\lambda = 1$. Montrer que $a^{\lambda/2}$ peut prendre 4 valeurs et que 2 de ces valeurs permettent de factoriser n.
3. On pose $H = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times,\ a^{\lambda/2} \equiv \pm 1\}$. Montrer que H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.
4. Montrer qu'il existe $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que b soit d'ordre $p-1$ modulo p et d'ordre $(q-1)/2$ modulo q.
5. On pose $p - 1 = 2^{v_p}p'$ et $q - 1 = 2^{v_q}q'$ avec p', q' impairs et on suppose, sans perte de généralité que $v_p \geq v_q$. Exprimer $\lambda/2$ en fonction de v_p et du ppcm de p', q'. En déduire que b n'appartient pas à H. Si on prend x au hasard dans $(\mathbb{Z}/n\mathbb{Z})^\times$, montrer que la probabilité que x n'appartienne pas à H est supérieure ou égale à $1/2$.
6. Soit $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Montrer que λ divise B et en déduire qu'il existe un entier k tel que $x^{\lambda/2} = x^{B/2^{k+1}}$.
7. Conclure : donner un algorithme probabiliste polynomial qui factorise n étant donné n, e et d et donner sa probabilité de succés.
8. Application : $n = 77$, $e = 7$, $d = 43$