Feuille 5 : Retour sur RSA et factorisation

Exercice 1. Une attaque sur RSA : petit exposant public commun

On suppose que k personnes $B_1, \dots, B_k$ 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 2. 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 3. 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 4. Algorithme de Dixon

Trouvez un diviseur non trivial de $N = 1829$ avec l'algorithme de Dixon et la base de facteurs $\mathcal{B} = \{2, 5, 7\}$. On pourra utiliser les entiers $43, 49, 52, 53, \dots$.

Exercice 5. L'algorithme ρ de Pollard pour la factorisation

Soit n un nombre entier dont on veut calculer un facteur non trivial. Soit p le plus petit facteur premier (inconnu) de n. L'idée est de construire une suite « aléatoire » $x_1, x_2, \dots, x_i, \dots$ d'éléments de $\mathbb{Z}/n\mathbb{Z}$, de sorte qu'une collision $x_i = x_j \mod p$ pour $i < j$ permette de trouver un facteur de n donné par $\mathrm{pgcd}(x_i - x_j, n)$.

On admettra le résultat suivant, connu sous le nom de *paradoxe des anniversaires* : en tirant au hasard des éléments d'un ensemble de cardinal N, on obtient une collision avec probabilité supérieure à $1/2$ au bout d'environ $\sqrt{N}$ tirages.

1. Estimez le nombre de termes de la suite et le nombre de pgcd à calculer avant de trouver un facteur de n.
2. On choisit de définir la suite x_i par la donnée de x_1 et la formule de récurrence $x_{i+1} = P(x_i)$, où $P \in \mathbb{Z}[X]$.
   (a) Montrez que $x_i = x_j \mod p \Longrightarrow x_{i+1} = x_{j+1} \mod p$.
   (b) En déduire que, si $x_i = x_j \mod p$ avec $i < j$ alors $x_u = x_{2u} \mod p$ pour un indice u tel que $u < j$.
   (c) Comment calculer $(x_{i+1}, x_{2(i+1)})$ à partir de (x_i, x_{2i}) ?
   (d) On *suppose* que la suite (x_i) obtenue a le même comportement qu'une suite de tirages indépendants dans $\mathbb{Z}/n\mathbb{Z}$, et donc qu'on peut appliquer le paradoxe des anniversaires. En déduire un algorithme qui nécessite environ $\sqrt{p}$ calculs de pgcd de nombres entiers naturels $\leq n$ pour factoriser n.
3. Factorisez $n = 7171$ avec $x_1 = 39$ et $P(x) = x^2 + 1$.

Exercice 6. 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 : $n = 77$, $e = 7$, $d = 43$