
Cryptographie à clé publique – Solutions feuille de TD 2

29/01/2024

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

<https://lvz1.fr/teaching/2023-24/cp.html>

(★) exercice fondamental (★★) pour s'entraîner (★★★) pour aller plus loin  sur machine

Exercice 1. (★) Application de RSA brut.

Dans cet exercice, on s'intéresse à une version « jouet » (c'est-à-dire, avec de petites valeurs) du chiffrement RSA brut.

Les nombres premiers $p = 17$ et $q = 23$ ont été engendrés par Alice, et l'entier $n = pq = 9191$ a été publié.

Question 1.– Alice peut-elle utiliser $e = 50$ comme seconde partie de sa clé publique ?

Question 2.– On suppose maintenant que $e = 3$. Calculer la valeur de $\phi(n)$, puis de l'exposant privé d .

Question 3.– Chiffrer le message $m = 10$ avec la clef publique (n, e) .

Question 4.– Calculer $d_p := d \bmod (p - 1)$ et $d_q := d \bmod (q - 1)$.

Question 5.– Calculer deux entiers u et v tels que $up + vq = 1$.

Question 6.– Étant donné le chiffré $c = 2$, calculer $c^{d_p} \bmod p$ et $c^{d_q} \bmod q$. Puis en déduire la valeur du message associé au chiffré c .

Solutions de l'Exercice 1.

Solution Q1. Non, car e est pair et $\phi(n)$ également (car p et q sont impairs), donc e et $\phi(n)$ ne sont pas premiers entre eux.

Solution Q2. On a $\phi(n) = 16 \times 22 = 352$. Puis, pour calculer d , il faut calculer l'inverse de 3 modulo 352. Pour cela, on exécute l'algorithme d'Euclide étendu. Ici, il peut se résumer à :

$$352 = 3 \times 117 + 1$$

puisqu'on en déduit que

$$3 \times (-117) + 352 \times 1 = 1$$

puis que $d = 3^{-1} \bmod 352$ vaut $352 - 117 = 235$.

Solution Q3. On calcule $m^e = 10^3 \bmod n$, autrement dit le reste de la division euclidienne de 1000 par 352. On obtient 296.

Exercice 3. (★) Attaque sur RSA à module identique.

Deux amis qui se font mutuellement confiance utilisent le même module RSA $n = pq$, mais avec des exposants (e_1, d_1) et (e_2, d_2) différents.

On se place dans un scénario où une troisième personne souhaite envoyer les chiffrés d'un même message m aux deux amis. On suppose qu'il utilise le mode d'utilisation « brut » du chiffrement RSA.

Question 1.– On suppose que les exposants e_1 et e_2 choisis par les deux amis sont premiers entre eux. Expliquer pourquoi, dans ce cas, un attaquant passif peut retrouver le message m .

Solutions de l'Exercice 3.

Solution Q1. On note $c_1 = m^{e_1} \pmod n$ et $c_2 = m^{e_2} \pmod n$ les deux chiffrés envoyés aux deux amis. L'attaquant cherche la valeur $m = m^1 \pmod n$. Pour cela, une idée pour être de calculer un produit de la forme :

$$c_1^u c_2^v \pmod n$$

qui soit égal à m .

Rappelons maintenant que les exposants e_1 et e_2 sont publics. On peut donc calculer les coefficients de Bezout associés à e_1 et e_2 . C'est-à-dire, on calcule grâce à l'algorithme d'Euclide étendu deux entiers u et v tels que

$$ue_1 + ve_2 = \text{pgcd}(e_1, e_2) = 1.$$

Alors, dans ce cas on obtient m en calculant simplement

$$c_1^u c_2^v = m^{ue_1 + ve_2} = m.$$

Cela nécessite deux exponentiations et une multiplication modulaires.

Exercice 4. (★★) Attaque de Håstad avec $e = 3$.

Trois utilisateurs ont engendré des clés RSA de modules n_1, n_2 et n_3 . On fait l'hypothèse que ces modules sont deux-à-deux premiers entre eux, mais observons que c'est extrêmement probable si leur génération est aléatoire (comme les n_i sont produit de deux grand nombres premiers).

Les trois utilisateurs choisissent le même exposant de chiffrement $e = 3$, et on suppose qu'un même message m est envoyé aux trois utilisateurs.

Question 1.– Comment peut-on calculer $m^e \pmod{n_1 n_2 n_3}$ à partir des chiffrés de m par les 3 clés publiques ?

Question 2.– En déduire une attaque passive permettant de retrouver le message m .

Question 3.– Cette attaque se généralise-t-elle, en pratique, pour n'importe quel exposant $e \geq 3$? Si oui, avec quelle contrainte ?

Solutions de l'Exercice 4.

Solution Q1. Notons $c_i := m^3 \pmod{n_i}$ le chiffré de m par le i -ème utilisateur. La valeur de c_i est connue de l'attaquant.

Si a et b sont premiers entre eux, le théorème des restes chinois donne un isomorphisme d'anneaux :

$$\begin{aligned} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\rightarrow \mathbb{Z}/ab\mathbb{Z} \\ (x = c \pmod a, y = c \pmod b) &\mapsto z = c \pmod{ab}. \end{aligned}$$

On rappelle que cet isomorphisme est explicite et calculable efficacement. Il suffit de retrouver les coefficients de Bezout u et v tels que $au + bv = 1$, puis de calculer

$$xbv + yau \pmod{ab}.$$

En utilisant cet isomorphisme avec les $c_i = m^3 \pmod{n_i}$ pour les paramètres $(a, b) = (n_1, n_2)$ puis $(a, b) = (n_1n_2, n_3)$, on obtient alors la valeur de $m^3 \pmod{n_1n_2n_3}$.

Solution Q2. Le message m a été choisi de sorte que $m < n_i$ pour tout i . On note donc que $m^3 < n_1n_2n_3$, donc le reste $m^3 \pmod{n_1n_2n_3}$ est toujours égal à l'entier m^3 .

Il suffit donc d'extraire une racine cubique de la valeur obtenue après application de l'isomorphisme des restes chinois. L'extraction d'une racine cubique est une opération très efficace dans les entiers naturels (cela requiert moins de $\log(m^3)$ opérations élémentaires sur les entiers).

Solution Q3. En théorie, l'attaque peut être généralisée à $e > 3$, mais il faut qu'il y ait e participants. Il y a alors deux contraintes importantes :

- il faut que e participants envoient le même message, ce qui est peu probable si e est grand,
- la complexité de l'attaque est polynomiale en e , donc une nouvelle fois, il ne faut pas que e soit trop grand.

Exercice 5. (★) RSA brut avec un petit message.

On considère le chiffrement RSA dans son mode de fonctionnement « brut ». On note $n = pq$ le module et e l'exposant public.

Question 1.— Soit c le chiffré d'un message m tel que $m < n^{1/e}$. Expliquer pourquoi, si un attaquant sait que le message envoyé m est plus petit que $n^{1/e}$, alors il peut retrouver m à partir de c .

Solutions de l'Exercice 5.

Solution Q1. Si l'on sait que $m < n^{1/e}$, alors $m^e < n$, donc $m^e \pmod{n}$ vaut m^e . Pour retrouver m à partir de $c = m^e \pmod{n}$, il suffit d'extraire une racine e -ème de c dans \mathbb{Z} . Cette opération est facile (extraction bit-à-bit, méthode de Newton, etc...).

Exercice 6. (★★) RSA brut avec clairs liés.

On considère le chiffrement RSA dans son mode de fonctionnement « brut ». On note $n = pq$ le module public. **On suppose que l'exposant public est $e = 3$.**

On chiffre successivement les messages $m, m + 1$ et $m + 2$ où $m \in \mathbb{Z}/n\mathbb{Z}$.

Question 1.— Donner (en fonction de m) la valeur des chiffrés c_0, c_1 et c_2 correspondant respectivement aux messages $m, m + 1$ et $m + 2$.

Question 2.— Comment un attaquant passif peut-il retrouver le message m en effectuant des combinaisons linéaires des chiffrés c_0, c_1 et c_2 ?

On fixe maintenant un entier $r \in (\mathbb{Z}/n\mathbb{Z})^\times$, que l'on suppose public. On chiffre ensuite les messages z et $z + r$ où $z \in \mathbb{Z}/n\mathbb{Z}$.

Question 3.— Expliquer comment, avec grande probabilité sur la valeur de z , un attaquant passif peut retrouver la valeur de z à partir des chiffrés de z et $z + r$.

Solutions de l'Exercice 6.

Solution Q1. Si on note $c_i = (m+i)^3 \pmod n$, alors on a

$$\begin{cases} c_0 &= m^3 & \pmod n \\ c_1 &= m^3 + 3m^2 + 3m + 1 & \pmod n \\ c_2 &= m^3 + 6m^2 + 12m + 8 & \pmod n \end{cases}$$

Solution Q2. On essaie de trouver une bonne combinaison linéaire des c_i pour trouver m . Ici,

$$c_2 + c_0 - 2c_1 = 6m + 6 \pmod n \implies m = 6^{-1}(c_2 + c_0 - 2c_1) - 1 \pmod n$$

Notons que 6 est bien inversible modulo n , car 2 et 3 ne sont pas des diviseurs de n .

Solution Q3. Si on note $c = z^3 \pmod n$ et $c' = (z+r)^3 \pmod n$, alors on a

$$\begin{cases} c &= z^3 & \pmod n \\ c' &= z^3 + 3z^2r + 3zr^2 + r^3 & \pmod n \end{cases}$$

Puis, il faut trouver une écriture de z en fonction de c , c' et r (connu). On a :

$$\begin{cases} c' - c + 2r^3 &= 3r(z^2 + zr + r^2) & \pmod n \\ c' + 2c - r^3 &= 3z(z^2 + zr + r^2) & \pmod n \end{cases}$$

Par conséquent, si $r(z^2 + zr + r^2)$ est inversible modulo n , alors on obtient :

$$z = \frac{r(c' + 2c - r^3)}{c' - c + 2r^3} \pmod n$$

On observe que $r(z^2 + zr + r^2)$ est inversible modulo n avec grande probabilité sur la valeur de z . En revanche, il est nécessaire que r soit inversible modulo n pour l'attaque fonctionner (mais c'est bien une hypothèse de l'énoncé).
