Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Cryptographie à clé publique – Feuille de TD 2

29/01/2024

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`https://lvzl.fr/teaching/2023-24/cp.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

Exercice 1. $(\star)$ 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 $d_p := d \mod (p-1)$ et $d_q := d \mod (q-1)$.

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

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

Exercice 2. $(\star)$ Factorisation de n grâce à $\phi(n)$.

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

Question 1.– Rappeler comment calculer l'indicatrice d'Euler $\phi(n)$ à partir de p et q, les entiers qui composent la factorisation de n.

Question 2.– Supposons maintenant que l'on connaisse n et $\phi(n)$. Donner une méthode pour factoriser n. On précisera un ordre de grandeur pour sa complexité.

Exercice 3. $(\star)$ 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.

Exercice 4. $(\star\star)$ 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 (les n_i sont des produits de deux grands 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 $m^e \mod n_1 n_2 n_3$ 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 ?

Exercice 5. $(\star)$ 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.

Exercice 6. $(\star\star)$ 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 $z + r$.