Faculté des Sciences et Techniques de Limoges 2018–2019
Master 2 — Sécurité de l'Information et Cryptologie — Parcours MCCA
Cryptographie à clé publique

Examen du 19 février 2019

Durée : 2 heures

Les exercices sont indépendants.

A. Signature

Soit $\mathbf{cK}_{\mathrm{rsa}}$ l'algorithme de génération des clés RSA associé au paramètre de sécurité λ (λ est la longueur du module RSA N). Soit $H : \{0,1\}^* \to \{0,1\}^{\lambda-1}$ une fonction de hachage. Considérons l'algorithme de signature suivant :

[Algorithme cK :]

$$\mathbf{cK}_{\mathrm{rsa}}(1^\lambda) \to (N, p, q, e, d)$$

Retourner (N, e) comme clé publique et (N, d) comme clé secrète.

[Algorithme Sig$((N, d), M)$:]

— Réécrire M (M est supposé de longueur paire) en deux parties de la même longueur :

$$M = M_0 \| M_1$$

— Calculer

$$y = H(0\|M_0) \times H(1\|M_1) \bmod N$$

— Retourner la signature $s = y^d \bmod N$.

1. – Décrire l'algorithme de vérification.

2. – Déterminer si ce schéma de signature est sûr face aux attaques à messages choisis (UF-CMA), lorsque la fonction H est considérée comme un oracle aléatoire.

B. Construction théorique d'un chiffrement asymétrique

3. – Supposons qu'il existe un chiffrement asymétrique IND-CPA sûr $\pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$. Montrer qu'il existe un chiffrement $\pi' = (\mathcal{G}', \mathcal{E}', \mathcal{D}')$ qui est IND-CPA sûr mais pas IND-CCA sûr.
Indication : Il peut être judicieux de modifier très légèrement le schéma π pour obtenir π' tel que π' reste IND-CPA (comme π) mais qu'il existe un attaquant de type CCA qui peut exploiter quelques propriétés particulières introduites dans la construction de π' pour casser le schéma π'.

C. Cryptosystème de Paillier

Soit $N = pq$ un entier RSA (donc p, q deux nombres premiers impairs distincts). On supposera de plus que

$$\mathrm{pgcd}(pq, (p-1)(q-1)) = 1.$$

4. – Quel est l'ordre du groupe $(\mathbb{Z}/N^2\mathbb{Z})^*$?

5. – Montrer que $(\mathbb{Z}/N^2\mathbb{Z})^*$ contient un élément g d'ordre N.

6. – Montrer qu'on définit bien une application E de $\mathbb{Z}/N\mathbb{Z} \times (\mathbb{Z}/N\mathbb{Z})^*$ dans $(\mathbb{Z}/N^2\mathbb{Z})^*$ en posant

$$E(m, r) = g^m r^N.$$

7. – Montrer que, si $E(m_1, r_1) = E(m_2, r_2)$ alors $g^{(p-1)(q-1)(m_1-m_2)} = 1$ (dans le groupe $(\mathbb{Z}/N^2\mathbb{Z})^*$).

8. – En déduire que E est une bijection.

D. Méthode ρ

Soit E un ensemble fini, $a \in E$ et f une application de E dans lui-même. On considère la suite (u_n) suivante d'éléments de E :

$$u_0 = a \qquad u_{n+1} = f(u_n) \quad \text{pour } n \in \mathbb{N}.$$

9. – Montrer que la suite $(u_n)_{n\in\mathbb{N}}$ est ultimement périodique (i.e. périodique à partir d'un certain rang).

10. – Soit q le plus petit entier tel que la sous-suite $(u_n)_{n\geqslant q}$ soit périodique et c sa période. Pour $e \in \mathbb{N}$, montrer que les conditions (i) et (ii) suivantes sont équivalentes :

(a) $c \mid e$ et $e \geqslant q$.

(b) $u_e = u_{2e}$.

On rappelle que le plus petit entier vérifiant ces conditions est appelé l'*épacte* de la suite (u_n).

11. – Pour $E = \mathbb{Z}/53\mathbb{Z}$, $a = 2$ et $f : x \mapsto x^2 + 1$, quel est l'épacte de la suite (u_n) ?

12. – Factoriser 4399 avec la méthode ρ de Pollard, en utilisant cette suite (u_n).