Faculté des Sciences et Techniques de Limoges 2016–2017
Master 2 — Sécurité de l'Information et Cryptologie — Parcours MCCA
Cryptographie à clé publique

Examen du 14 février 2017

Durée : 2 heures

Seuls documents autorisés : Notes personnelles manuscrites.

Les exercices sont indépendants.

A. Protocole d'identification de Schnorr

Soient p, q deux grands (donc impairs) nombres premiers tels que $q \mid p-1$.

1. – Montrer qu'il existe un entier g d'ordre q modulo p.

Soit $a \in [0, q-1]$ un entier connu d'Alice seulement. Soit $A = g^a \bmod p$. Les données p, q, g et A sont publiques. Alice s'identifie auprès de Bob à l'aide du protocole suivant :

• Alice choisit un engagement aléatoire k dans l'intervalle $\{0, \dots, q-1\}$ et calcule $K = g^k \bmod p$. Elle transmet K à Bob.

• Bob choisit un défi r au hasard dans l'intervalle $\{0, \dots, q-1\}$ et le transmet à Alice.

• Alice calcule la réponse $y = k + ar \bmod q$ et la transmet à Bob. Bob accepte Alice si et seulement si $g^y \equiv KA^r$ modulo p.

Alice		**Bob**
$k \in [0, q-1],\ K = g^k \bmod p$	$\xrightarrow{K}$	
	$\xleftarrow{r}$	$r \in [0, q-1]$
$y = k + ar \bmod q$	$\xrightarrow{y}$	$g^y \stackrel{?}{\equiv} KA^r \pmod p$

Protocole 1. Identification par Schnorr

2. – Montrer que ce protocole est consistant.

3. – Montrer que ce protocole est significatif.

4. – Montrer que, si un attaquant peut à l'avance (avant d'envoyer K) deviner le défi r que Bob va lui proposer, alors il peut être accepté.

5. – Montrer qu'un attaquant peut simuler les T triplets (K_i, r_i, y_i) (pour $1 \leqslant i \leqslant T$) obtenus lors de T identifications d'Alice auprès de Bob ? Avec quel coût ?

6. – Ce protocole d'identification vérifie-t-il la propriété de *Zero-Knowledge* ? (Remarque : je tiendrai plus compte ici de l'argumentation que de l'exactitude de la réponse).

B. Courbe elliptique

On rappelle que, pour $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points sur une courbe elliptique d'équation $y^2 = x^3 + ax + b$, les coordonnées (x_3, y_3) du troisième point P_3 de E aligné avec P_1 et P_2 s'expriment avec les formules :

$$\begin{cases} x_3 = m^2 - x_1 - x_2, \\ y_3 = y_1 + m(x_3 - x_1) \end{cases} \qquad \text{où} \quad m = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{si } x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{si } P_1 = P_2 \end{cases} \tag{1}$$

On considère la courbe E définie sur le corps $\mathbb{F}_{11}$ par l'équation $y^2 = x^3 + 2x + 6$.

7. – Montrer que E est une courbe elliptique.

8. – Quel est l'ordre du groupe correspondant ?

9. – Quel est l'ordre du point de coordonnées affines $(1, 3)$ sur E ?

C. Cryptosystème de Paillier

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

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

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

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

12. – 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

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

13. – 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 $(\mathbb{Z}/N^2\mathbb{Z})^*$).

14. – En déduire que E est une bijection.

D. Signature

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

[Algorithme $\mathcal{K}$:]

$$\mathcal{K}_{\mathrm{rsa}}(1^\lambda) \to (N, p, q, e, d).$$

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

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

— Réécrire M (M est supposé à 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 $s = y^d \bmod N$.

15. – Décrire l'algorithme de vérification.

16. – Déterminer si ce schéma de signature est UF-CMA sûr (c-à-d. infalsifiable face aux attaques à messages choisis). Prouvez la sécurité ou donnez une attaque.