Examen du 9 février 2016

Durée : 2 heures

Seuls documents autorisés : Notes personnelles manuscrites.

Les exercices sont indépendants.

A. El Gamal

Soient p un nombre premier et g un entier d'ordre $p-1$ modulo p. On suppose que $p-1$ possède un petit facteur k.

1. – Soit A un entier tel que $p \nmid A$. Montrer que A est une puissance k-ième modulo p si et seulement si $A^{(p-1)/k} \equiv 1$ modulo p.

2. – Soit $a \in \{0, 1, \ldots, p-2\}$ tel que $A \equiv g^a$ modulo p. Ecrire un algorithme permettant de calculer $a \bmod k$ (lorsque k est petit). Evaluer la complexité de votre algorithme en fonction de k et p.

3. – On utilise le nombre premier p pour faire du chiffrement El Gamal. Montrer que ce chiffrement n'est pas sémantiquement sûr.

4. – Proposer une modification pour remédier à ce défaut (tout en gardant le même module p).

B. Epacte

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 :

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

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

6. – 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 : (i) $c \mid e$ et $e \geqslant q$. (ii) $u_e = u_{2e}$.

Le plus petit entier vérifiant ces conditions est parfois appelé l'*épacte* de la suite (u_n).

7. – Pour $E = \mathbb{Z}/47\mathbb{Z}$, $a = 1$ et $f : x \mapsto x^2 + 1$, quel est l'épacte de la suite (u_n) ?

8. – Factoriser 4183 en vous appuyant sur les questions précédentes.

C. Non résidus quadratiques

Soit N un entier RSA (un produit pq de deux nombres premiers impairs distincts). On note

$$\mathbb{Z}_N = \{1, \ldots, N-1\} \qquad \mathbb{Z}_N^+ = \left\{x \in \mathbb{Z}_N \,\middle|\, \left(\frac{x}{N}\right) = 1\right\}$$

$$\mathcal{Q} = \{x \in \mathbb{Z}_N \mid \exists y \in \mathbb{Z},\quad y^2 \equiv x \text{ modulo } n\}, \qquad \overline{\mathcal{Q}} = \mathbb{Z}_N^+ \setminus \mathcal{Q}.$$

L'entier N est public. Paula connaît les facteurs p et q, mais Victor les ignore.

9. – Rappeler les relations que vérifient les ensembles $\mathbb{Z}_N$, $\mathbb{Z}_N^*$, Q et $\overline{Q}$.

Soit $R \in \mathbb{Z}_N^*$, public aussi. Paula et Victor échangent des données selon le protocole suivant.

(a) Victor choisit au hasard uniforme s dans $\mathbb{Z}_N^*$ et un bit b, au hasard uniforme aussi.

(b) Victor calcule $W := s^2 R^b \bmod N$ et l'envoie à Paula

(c) Paula détermine si $W \in Q$. Si oui, elle pose $b' = 0$. Sinon, elle pose $b' = 1$. Elle envoie b' à Victor.

(d) Victor compare b et b'.

Paula		Victor
		$s \in \mathbb{Z}_N^*$, $b \in \{0,1\}$
	$\xleftarrow{W}$	$W := s^2 R^b \bmod N$
$b' = 0$ si W carré, $b' = 1$ sinon	$\xrightarrow{b'}$	$b' \stackrel{?}{=} b$

Protocole 1. Preuve pour NQR

10. – A l'étape (c), comment Paula peut-elle savoir si W est un carré modulo N, afin de déterminer b' ?

11. – Si $R \in Q$. Avec quelle probabilité, la relation $b' \stackrel{?}{=} b$ observée par Victor est vraie ?

12. – Paula peut-elle modifier cette probabilité, en utilisant une autre stratégie pour le choix de b' ?

On suppose désormais que $R \in \overline{Q}$.

13. – Avec quelle probabilité la relation $b' \stackrel{?}{=} b$ observée par Victor est vraie ?

14. – Paula peut-elle utiliser ce protocole pour convaincre Victor que $R \in \overline{Q}$, et comment ?

15. – Quel est l'ensemble des valeurs que peut prendre le W envoyé par Victor à Paula, et avec quelle distribution de probabilités ?

16. – Le bit b' est il indépendant de W ?

17. – Est-il possible pour Victor, de simuler seul la production de quadruplets (s, b, W, b'), avec la même distribution de probabilités que lors d'une utilisation répétée du protocole avec Paula ?

18. – Victor, en utilisant éventuellement une autre stratégie pour le choix de W, peut-il obtenir par ce protocole, des informations qu'il ne pourrait pas obtenir sans la participation de Paula ?

D. Logarithme discret dans $\mathbb{F}_{128}$

19. – Soit $\mathcal{B}$ l'ensemble des polynômes irréductibles sur $\mathbb{F}_2$ de degré inférieur ou égal à 3. Déterminer $\mathcal{B}$.

20. – Montrer que le corps $\mathbb{F}_{128}$ est de la forme $\mathbb{F}_2[\alpha]$, où α vérifie la relation $\alpha^7 = \alpha + 1$.

21. – On donne l'expression de certaines puissances de α en polynômes u_i de degré $\leqslant 6$ en α :

$$\begin{cases} \alpha^{18} = u_1(\alpha) = \alpha^6 + \alpha^4 \\ \alpha^{45} = u_2(\alpha) = \alpha^5 + \alpha^2 + \alpha + 1 \\ \alpha^{72} = u_3(\alpha) = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 \\ \alpha^{105} = u_4(\alpha) = \alpha^6 + \alpha^5 + \alpha^4 + \alpha \\ \alpha^{121} = u_5(\alpha) = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1. \end{cases}$$

Factoriser (si possible) les polynômes $u_i(X)$ en produits d'éléments de $\mathcal{B}$.

22. – En déduire des relations faisant intervenir les logarithmes des éléments de $\mathcal{B}$ en base α.

23. – Expliquer comment en déduire les logarithmes des éléments de $\mathcal{B}$ en base α (le calcul explicite n'est pas demandé).

24. – Expliquer comment en déduire le logarithme en base α de $\beta = \alpha^6 + \alpha^5 + \alpha^3 + 1$.