DEVOIR MAISON
20 mai 2020

Exercice 1 – [LFSR]
Soit $s = (s_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite périodique de période 7 et dont les sept premiers termes sont 1 0 1 1 0 0 0.
1. Sans calcul, dire si cette suite est une MLS.
2. À l'aide de sa série génératrice, déterminer la relation de récurrence la plus courte vérifiée par s.
3. Soit $t = (t_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite définie par la relation

$$t_{i+7} = t_{i+3} + t_i \text{ pour tout } i \geq 0$$

et de graine 1 0 0 0 1 0 0. Sans calculer les termes suivants de la suite t, déterminer sa période.
4. Quelles sont la complexité linéaire et la période de la suite $s + t$?

Exercice 2 – [Goldwasser-Micali (2)*]
Alice utilise le chiffrement de Goldwasser-Micali : elle choisit deux grands premiers distincts p et q, calcule $n = pq$ et détermine un entier g (modulo n) qui n'est ni un carré modulo p, ni un carré modulo q. Sa clé publique est (n, g) et sa clé privée (p, q). Pour chiffrer un bit $m \in \{0, 1\}$, Bob tire au hasard $h \in (\mathbb{Z}/n\mathbb{Z})^\times$ et calcule $c = g^m h^2 \mod n$.
1. Montrer que

$$m = 0 \Leftrightarrow c \text{ est un carré modulo } p \Leftrightarrow c \text{ est un carré modulo } q$$

et en déduire l'algorithme de déchiffrement.
2. À quelle condition nécessaire et suffisante sur p et q peut-on prendre $g = n - 1$?
3. Exemple pédagogique. Alice choisit $p = 67$, $q = 83$ et donc $n = 5561$

(a) Montrer que 2 n'est pas un carré modulo p et que 19 n'est pas un carré modulo q.
(b) En déduire, à l'aide du théorème des restes chinois, une valeur de g différente de 5560 qui convient.
(c) Alice choisit ce g. Bob chiffre un bit m en $c = 4949$. Que vaut m ?

Exercice 3 – [Signature à la Rabin]
Alice utilise le cryptosystème de Rabin. Sa clé secrète est un couple de grands premiers distincts p et q vérifiant $p, q \equiv 3 \bmod 4$. Sa clé publique est $n = pq$. Pour signer un message M elle prend $U \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que UM soit un carré modulo n, extrait les racines carrées de UM, ce qu'elle sait faire efficacement grâce à sa connaissance de p et q. Elle en choisit une notée x et elle signe M par $S = (U, x)$. Pour simplifier, on supposera dans la suite que l'on est dans le cas générique $M \in (\mathbb{Z}/n\mathbb{Z})^\times$.
1. Quelle est la probabilité pour que U tiré au hasard dans $(\mathbb{Z}/n\mathbb{Z})^\times$ convienne ?
2. Supposons qu'Alice tire U au hasard dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Comment fait-elle pour déterminer si U convient ou non ?
3. Comment Alice peut-elle procéder pour trouver un U adéquat sans tirage aléatoire ?
4. Comment Bob procède-t-il pour vérifier la signature ?
5. Montrer comment un attaquant peut signer n'importe quel message M en se faisant passer pour Alice.
6. Hacher M à l'aide d'une fonction de hachage publique $h : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ et construire la signature à partir de $h(M)$ comme précédemment permet-il de résoudre ce problème ?
7. Si la réponse est non, proposer une autre solution, qui permette en outre d'empêcher toute falsification existentielle. Justifier.

Exercice 4 – [Partage de secret d'après Blakley]
Rappelons le principe d'un schéma à seuil. Soient des entiers $2 \leq k \leq n$. On veut partager un secret entre n personnes de telle sorte que k d'entre elles puissent retrouver ce secret, mais pas $k - 1$. Pour cela on donne à chacune des n personnes une information partielle sur ce secret. Intéressons-nous ici à un schéma à seuil inspiré de Blakley. Soit $\mathbb{F}_q$ un corps fini. Le secret est un élément s de $\mathbb{F}_q$. À la i-ème personne on donne l'équation d'un hyperplan de $\mathbb{F}_q^k$, d'inconnues $x_1, x_2, \ldots, x_k$:

* : (2) pour différencier cet exercice d'un autre proposé l'année dernière et qui portait sur le même cryptosystème.

$a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,k}x_k = b_i$ où $a_{i,1}, \ldots, a_{i,k}, b_i \in \mathbb{F}_q$. On suppose que ces hyperplans ont un et un seul point commun $(y_1, y_2, \ldots, y_k)$ dont la première coordonnée est $y_1 = s$. On suppose en outre que si $A = (a_{i,j})$ est la matrice $n \times k$ associée à ces équations, toute matrice $k \times k$ extraite de A est inversible et que toute matrice $(k-1) \times (k-1)$ extraite de la matrice A privée de sa première colonne est inversible.

1. Montrer que k personnes peuvent retrouver s.

2. Montrer que toutes les valeurs de s sont possibles pour $k-1$ personnes qui mettraient leurs informations en commun.

3. Donnons un exemple pédagogique avec $k = 3$ et $n = 5$. Soit $P(X) = X^2 + X + 2 \in \mathbb{F}_3[X]$.

(a) Montrer que $P(X)$ est irréductible dans $\mathbb{F}_3[X]$. On identifiera $\mathbb{F}_9$ à $\mathbb{F}_3[X]/\langle P(X)\rangle$ et on notera α la classe de X dans ce quotient.

(b) Quel est l'ordre de α dans $\mathbb{F}_9^\times$?

(c) On pose

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha^4 & 1 \\ 1 & \alpha^5 & \alpha^2 \\ 1 & \alpha^6 & \alpha^4 \\ 1 & \alpha^7 & \alpha^6 \end{pmatrix}.$$

Montrer que A vérifie les hypothèses de la construction faite plus haut.

Indication : sans faire du cas par cas, on pourra chercher à raisonner en termes de combinaisons linéaires de colonnes et faire apparaître des polynômes de degré 2 ayant 3 racines distinctes.

(d) Imaginons que les équations données aux 5 personnes soient

$$\begin{cases} x_1 + x_2 + x_3 &= 2\alpha + 1 \\ x_1 + \alpha^4 x_2 + x_3 &= \alpha + 2 \\ x_1 + \alpha^5 x_2 + \alpha^2 x_3 &= \alpha + 2 \\ x_1 + \alpha^6 x_2 + \alpha^4 x_3 &= 2\alpha \\ x_1 + \alpha^7 x_2 + \alpha^6 x_3 &= 1 \end{cases}$$

Retrouver le secret s.

(e) Montrer que cet exemple correspond en fait (à un détail non fondamental près) à un partage de secret de Shamir.

4. Prouver qu'un partage de secret de Shamir est un cas particulier de la construction donnée au départ.

Exercice 5 – [RSA ET DERNIER BIT]

Soit $n = pq$ un module RSA (p et q grands premiers distincts) et soit

$$E : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & x^e \end{array}$$

une fonction de chiffrement RSA ($\mathrm{pgcd}(e, \varphi(n)) = 1$). On identifie $\mathbb{Z}/n\mathbb{Z}$ et $\{0, 1, \ldots, n-1\}$. Soient $\mathcal{P}$ et $\mathcal{D} : \mathbb{Z}/n\mathbb{Z} \to \{0, 1\}$ les fonctions définies par :

- $\mathcal{P}(y) = 0$ si $E^{-1}(y)$ est pair et $\mathcal{P}(y) = 1$ sinon ;
- $\mathcal{D}(y) = 0$ si $0 \leq E^{-1}(y) < n/2$ et $\mathcal{D}(y) = 1$ sinon.

1. Pour tout $y \in \mathbb{Z}/n\mathbb{Z}$, montrer que

$$\mathcal{D}(y) = \mathcal{P}(yE(2)) \text{ et } \mathcal{P}(y) = \mathcal{D}(yE(2^{-1})).$$

2. Pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, montrer que

$$\begin{cases} \mathcal{D}(E(x)) = 0 & \Leftrightarrow & x \in [0, n/2[\\ \mathcal{D}(E(2x)) = 0 & \Leftrightarrow & x \in [0, n/4[\cup [n/2, 3n/4[. \end{cases}$$

3. Généraliser à $\mathcal{D}(E(2^k x))$ où k est un entier naturel.

4. En déduire que l'on peut transformer tout algorithme polynomial qui calculerait $\mathcal{D}(y)$ pour tout $y \in \mathbb{Z}/n\mathbb{Z}$ en un algorithme polynomial calculant $E^{-1}(y)$ pour tout y.

5. En déduire que si l'on dispose d'un algorithme polynomial permettant de déterminer le dernier bit d'un clair quelconque x connaissant son chiffré y, alors on dispose d'un algorithme polynomial permettant de déterminer x tout entier, et donc de casser RSA.