DS n°2

28 avril 2014

Corrigé

Exercice 1. Résoudre dans $\mathbb{Z}$ le système suivant.

$$\begin{cases} x &= 7 \mod 10 \\ 3x &= 9 \mod 21 \\ 5x &= 4 \mod 13 \end{cases}$$

On se ramène à un système qui permet d'utiliser le théorème chinois. La deuxième congruence est équivalente à $x = 3 \bmod 7$. En effet

$$\begin{aligned} 3x = 9 \bmod 21 &\iff \exists\, k \in \mathbb{Z} \text{ tel que } 3x - 9 = 21k \\ &\iff \exists\, k \in \mathbb{Z} \text{ tel que } x - 3 = 7k \\ &\iff x = 3 \bmod 7 \end{aligned}$$

Pour simplifier la troisième congruence, on détermine l'inverse de 5 modulo 13. Soit on utilise l'algorithme d'Euclide étendu, soit on voit que 8 convient. Alors

$$\begin{aligned} 5x = 4 \bmod 13 &\iff 8 \times 5x = 8 \times 4 \bmod 13 \\ &\iff x = 6 \bmod 13 \end{aligned}$$

La première équivalence est justifiée par le fait que si $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est inversible, alors pour tout β et tout γ de $\mathbb{Z}/n\mathbb{Z}$, on a

$$\beta = \gamma \iff \alpha\beta = \alpha\gamma.$$

Ainsi le système à résoudre est équivalent à

$$\begin{cases} x &= 7 \mod 10 \\ x &= 3 \mod 7 \\ x &= 6 \mod 13 \end{cases}$$

Les entiers 10, 7 et 13 sont premiers entre eux deux à deux et on peut utiliser le théorème chinois. Une relation de Bézout évidente entre 10 et 7 est : $(-2) \times 10 + 3 \times 7 = 1$. On en déduit que

$$\left.\begin{aligned} x &= 7 \mod 10 \\ x &= 3 \mod 7 \end{aligned}\right\} \iff x = 3 \times (-2) \times 10 + 7 \times 3 \times 7 \bmod 10 \times 7$$
$$\iff x = 17 \bmod 70$$

Le système à résoudre est donc équivalent à

$$\begin{cases} x &= 17 \mod 70 \\ x &= 6 \mod 13 \end{cases}$$

On cherche une relation de Bézout entre 70 et 13. On utilise l'algorithme d'Euclide étendu

r	q	u	v
70		1	0
13	5	0	1
5	2	1	-5
3	1	-2	11
2	1	3	-16
1		-5	27

qui donne $(-5) \times 70 + 27 \times 13 = 1$. On en déduit les solutions du système :

$$x = 6 \times (-5) \times 70 + 17 \times 27 \times 13 \bmod 70 \times 13,$$

ou encore

$$x = 227 \bmod 910.$$

Exercice 2. Alice et Bob communiquent en utilisant le protocole RSA. Bob choisit les deux premiers $p = 211$ et $q = 353$ et définit $N = pq = 74483$. Il lui reste à choisir l'exposant de chiffrement e.

1. Le choix $e = 123$ est-il pertinent ?
2. Finalement il opte pour $e = 139$. Montrer que c'est un choix correct et déterminer l'exposant de déchiffrement d qu'il va utiliser.
3. Préciser la clé publique et la clé secrète de Bob.

1. L'exposant e doit être inversible modulo $\phi(N)$. Or $\phi(N) = (p-1)(q-1) = 210 \times 352$. Trivialement 3 divise 123 est 210. L'exposant 123 n'est pas premier avec $\phi(N)$ et n'est donc pas inversible modulo $\phi(N)$. Ce choix est par conséquent incorrect.
2. Répondons aux deux questions en utilisant l'algorithme d'Euclide étendu. On a $\phi(N) = 73920$.

r	q	u	v
73920		1	0
139	531	0	1
111	1	1	-531
28	3	-1	532
27	1	4	-2127
1		-5	2659

Ceci prouve que $\text{pgcd}(73920, 139) = 1$ et fournit la relation de Bézout

$$(-5) \times 73920 + 2659 \times 139 = 1.$$

On en déduit que $e = 139$ convient et que son inverse modulo 73920 est 2659. Ainsi $d = 2659$.
3. La clé publique de Bob est $(74483, 139)$. Sa clé secrète est 2659.

Exercice 3. Un LFSR a engendré la suite périodique de période 15

$$S = (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}, 1, 0, 1, 0, 1, 1, 1, 1, \ldots)$$

1. Montrer que la longueur d'un tel LFSR est supérieure ou égale à 4.
2. Montrer qu'il existe un unique LFSR de longueur 4 engendrant S et le déterminer.
3. On a utilisé ce LFSR pour engendrer une clé destinée à être utilisée pour un chiffrement de Vernam. L'initialisation n'est pas la même que celle utilisée pour engendrer S. Les vingt-six lettres sont codées de 0 à 25 dans l'ordre alphabétique ; de plus, chaque entier de 0 à 25 est représenté par son écriture binaire sur cinq bits. Par exemple, A= 0 = 00000, D= 3 = 00011. Un message de quatorze lettres a été chiffré. Le message chiffré est
1 1 0 1 1 0 1 1 0 0 1 0 1 1 1 1 1 1 0 1 0 0 0 0 0 1 0 0 0 1 1 1 0 1 0 1 0 0 1 1 1 1 1 1 0 0 1 1 1 1
0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 0 0 0 0 0.
Le déchiffrer.

1. On sait que si un LFSR est de longueur k, la période d'une suite qu'il engendre est au plus égale à $2^k - 1$ (voir cours). Comme ici la période est 15, on a $15 \leq 2^k - 1$ ce qui implique $4 \leq k$.
2. Montrons d'abord l'unicité du LFSR cherché. Soit

$$x_{i+4} = a_3 x_{i+3} + a_2 x_{i+2} + a_1 x_{i+1} + a_0 x_i \quad \text{pour tout } i \geq 0$$

la relation de récurrence qui le définit, où $a_j \in \mathbb{Z}/2\mathbb{Z}$ pour tout j. En appliquant cette relation à S (avec $0 \leq i \leq 4$) on obtient le système

$$\begin{cases} 1 &= a_2 + a_0 \\ 1 &= a_3 + a_1 \\ 1 &= a_3 + a_2 + a_0 \\ 1 &= a_3 + a_2 + a_1 \end{cases}$$

que l'on résout facilement dans $\mathbb{Z}/2\mathbb{Z}$. On obtient finalement

$$a_0 = 1,\ a_1 = 1,\ a_2 = 0,\ a_3 = 0.$$

Si le LFSR existe, il est unique, défini par la relation de récurrence

$$x_{i+4} = x_{i+1} + x_i \quad \text{pour tout } i \geq 0.$$

Pour montrer l'existence, il suffit de vérifier que cette relation de récurrence fournit bien S, ce qui se fait sans peine en observant qu'elle est vérifiée par les termes de S jusqu'à $i = 14$ (voir pourquoi).
3. La clé est engendrée par le LFSR qui a défini S. L'initialisation est évidemment différente de $(0, 0, 0, 0)$ car le premier bloc ne correspond à aucune lettre. De plus, il n'y aurait pas de chiffrement ! Comme S est de période maximale $2^4 - 1 = 15$, il s'agit donc d'une décalée de S (voir cours) distincte de S, car il est précisé que l'initialisation est différente de celle de S.
Première hypothèse : la clé est $(x_{i+1})_{i \geq 0}$.

$$K = (0, 1, 0, 1, 1 \,|\, 1, 1, 0, 0, 0 \,|\, 1, 0, 0, 1, 1 \,|\, 0, 1, 0, 1, 1 \,|\, 1, 1, 0, 0, 0 \,|\, \ldots)$$

Si m est le message et c le chiffré, on a $m = c \oplus K$ d'où l'on tire

$$m = (1, 0, 0, 0, 0 \,|\, 1, 0, 1, 0, 0 \,|\, 0, 0, 1, 0, 0 \,|\, 1, 0, 1, 1, 0 \,|\, 1, 1, 0, 0, 0 \,|\, \ldots)$$

Ainsi $m =$ QUEWY.... Peu crédible.
Deuxième hypothèse : la clé est $(x_{i+2})_{i\geq 0}$.

$$K = (1,0,1,1,1\,|\,1,0,0,0,1\,|\,0,0,1,1,0\,|\,1,0,1,1,1\,|\,1,0,0,0,1\,|\,\ldots)$$

On obtient alors

$$m = (0,1,1,0,0\,|\,1,1,1,0,1\,|\,\ldots)$$

Mais le second bloc ne correspond à aucune lettre.
Troisième hypothèse : la clé est $(x_{i+3})_{i\geq 0}$.

$$K = (0,1,1,1,1\,|\,0,0,0,1,0\,|\,0,1,1,0,1\,|\,0,1,1,1,1\,|\,0,0,0,1,0\,|\,\ldots)$$

On obtient alors

$$m = (1,0,1,0,0\,|\,0,1,1,1,0\,|\,1,1,0,1,0\,|\,\ldots)$$

Mais le troisième bloc ne correspond à aucune lettre.
Quatrième hypothèse : la clé est $(x_{i+4})_{i\geq 0}$.

$$K = (1,1,1,1,0\,|\,0,0,1,0,0\,|\,1,1,0,1,0\,|\,1,1,1,1,0\,|\,0,0,1,0,0\,|\,\ldots)$$

On obtient alors

$$m = (0,0,1,0,1\,|\,0,1,0,0,0\,|\,0,1,1,0,1\,|\,0,0,1,0,0\,|\,\ldots),$$

qui correspond à FINDE. Comme c'est plausible on continue et on trouve

FINDELEXERCICE

Enfin, si l'on désire être complet, on vérifie avec patience que les dix autres décalées ne conviennent pas.