DS n°2

28 avril 2014

Durée : 1h20

Les documents sont interdits, les calculatrices autorisées.
La qualité de la rédaction sera un facteur d'appréciation important.

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

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

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.

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 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.