M1MI2016 Codes et Cryptologie

Corrigé du DS Terminal.

10 juin 2013, durée 3h

Documents interdits, calculatrices autorisées

EXERCICE 1 (6 points)

1.

$$\begin{aligned}
N &= 1111\\
x &= 0001000100010001\\
s &= 1000010010110011\\
c &= 1001010110100010
\end{aligned}$$

2. Soit y le bit manquant dans l'initialisation de s et soit $\overline{y} = 1 + y$.

$$\begin{aligned}
s &= 11y11\overline{y}0\overline{y}y10yyy\overline{y}y\\
c &= 1111110101010101\\
x &= 00\overline{y}00y0yy00\overline{y}y\overline{y}\overline{y}\overline{y}
\end{aligned}$$

soit

$$\begin{array}{lll}
y = 0 & x = 0010000000010111 & N = 2017\\
y = 1 & x = 0000010110001000 & N = 588
\end{array}$$

3. $N = 2017$
4. (a) Si l'initialisation de s est $s_0s_1s_2s_3s_4$, comme $c = 11111\dots$, x commence par $x = 1+s_0, 1+s_1, 1+s_2, 1+s_3, 1+s_4$. L'hypothèse $N < 3000$ se traduit par : x commence par 0000 ou 0001 ou 0010, soit les 5 premiers bits de x peuvent être :

$$00000 \quad 00001 \quad 00010 \quad 00011 \quad 00100 \quad 00101$$

ce qui correspond à 6 possibilités pour l'initialisation de s :

$$11111 \quad 11110 \quad 11101 \quad 11100 \quad 11011 \quad 11010.$$

(b) Car $\sum_{i=0}^{15} x_i = \sum_{i=0}^{15} c_1 = 1 \bmod 2$.

(c) On a déjà calculé N pour 11111 et 11011 dans la question 2. Il reste 4 possibilités à examiner. On trouve pour s :

1111000110111010
1110101000010010
1110001101110101
1101010000100101

Compte tenu de la condition de parité, il reste à examiner la première et la troisième. Le déchiffrement de c conduit dans le premier cas à 0000 1100 ... ce qui est impossible car le deuxième bloc de 4 bits correspond à 12 qui n'est pas un chiffre décimal. De même, dans l'autre cas, on trouve pour x, 0001 1110 ....

EXERCICE 2 (6 points)

1. Puisque $q = p + 2$, on a $N = p(p + 2) = p^2 + 2p$ donc $(p + 1)^2 = N + 1 = 5184 = 72^2$. Finalement, $p = 71$ et $q = 73$.
2. L'exposant de déchiffrement d est l'inverse de $e = 11$ modulo $(p-1)(q-1) = 70*72 = 5040$. On exécute l'algorithme d'Euclide étendu :

$$\begin{array}{rrrr} 5040 & 1 & 0 & \\ 11 & 0 & 1 & 458 \\ 2 & 1 & -458 & 2 \\ 1 & -5 & 2291 & \end{array} \qquad \begin{array}{r} \\ 5040 = 458 * 11 + 2 \\ 11 = 5 * 2 + 1 \\ \\ \end{array}$$

d'où la relation de Bezout $1 = 5040 * (-5) + 11 * 2291$ donc $d = 2291$.

3. $x = 3^{2291} \bmod 5183$
4.

$$\begin{array}{rrrr} 73 & 1 & 0 & \\ 71 & 0 & 1 & 1 \\ 2 & 1 & -1 & 35 \\ 1 & -35 & 36 & \end{array} \qquad \begin{array}{r} \\ 73 = 71 + 2 \\ 71 = 35 * 2 + 1 \\ \\ \end{array}$$

D'où $73 * (-35) + 71 * 36 = 1$.

5. Comme $2291 = 70 * 32 + 51$, $3^{2291} = 3^{51} \bmod 71$. Ensuite on calcule $3^{51} \bmod 71$ par exponentiation rapide. 51 s'écrit en binaire 110011.

$$\begin{array}{rr} & 1 \\ 1 & 3 \\ 1 & 27 \\ 0 & 19 \\ 0 & 6 \\ 1 & 37 \\ 1 & 60 \end{array}$$

Donc $3^{51} = 60 \bmod 71$.

De même, comme $2291 = 72 * 31 + 59$, $3^{2291} = 3^{59} \bmod 73$.

	1
1	3
1	27
1	70
0	9
1	24
1	49

Donc $3^{59} = 49 \bmod 73$.

6. Comme $x = 60 \bmod 71$ et $x = 49 \bmod 73$, par le théorème Chinois, on a $x = 60 * 73 * (-35) + 49 * 71 * 36 = 3042 \bmod 5183$.

EXERCICE 3 (8 points sur les questions 1 à 6 et 2 points bonus sur la 7)

1.
$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

2.
$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

3. $[n, k, d] = [8, 4, 4]$
4. $d - 1 = 3$ effacements, $\lfloor (d-1)/2 \rfloor = 1$ erreur.
5. (a) $x = 11101000$
   (b) $x = 11101000$ ou $x = 00000000$.
6. (a) $x = 1\mathbf{0}001110$
   (b) $x = \mathbf{0}001011\mathbf{1}$ ou $x = 1\mathbf{1}0101\mathbf{0}0$ ou $x = 10\mathbf{1}10\mathbf{0}10$ ou $x = 100\mathbf{01}110$