TELECOM

Contrôle des connaissances 2008/2009

CRYPTOGRAPHIE

22 octobre 2008

durée 2 heures

On sera attentif à la précision de la rédaction. Les résultats devront toujours être justifiés que ce soit par une démonstration, un algorithme ou une vérification numérique. Les protocoles seront décrits précisément.

Documents et calculettes non autorisés

Exercice 1

On considère le LSFR sur $\mathbb{F}_2$, défini par la relation de récurrence

$$u_{n+4} = u_{n+1} + u_n$$

et les conditions initiales $(k_0, k_1, k_2, k_3) \in \left(\mathbb{F}_2\right)^4$.

Question 1 Montrer que pour tout choix de conditions initiales la période de la suite récurrente linéaire $(u_n)_{n\in\mathbb{N}}$ est majorée par 15 (ne pas perdre de temps sur cette question).

Question 2 On code par XORisation à l'aide du LFSR précédent avec les conditions initiales $(k_0, k_1, k_2, k_3) = (1, 0, 0, 0)$. Chaque lettre de l'alphabet est codée par le quintuplet $(a_0, a_1, a_2, a_3, a_4)$ tel que $a_0+2a_1+4a_2+8a_3+16a_4)$ soit le rang de la lettre dans l'alphabet ordinaire compté entre 1 et 26, le quintuplet $(0, 0, 0, 0, 0)$ correspond à l'espace entre deux mots (exemples : A la première lettre de l'alphabet est codée $(1, 0, 0, 0, 0)$, M la treizième de l'alphabet lettre est codée $(1, 0, 1, 1, 0)$). Décoder le message page 10.

Exercice 2

On pose $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. Trouvez l'inverse multiplicatif de $X^3 + 3X - 1$ modulo $X^5 + X + 1$ considérés comme des polynômes de $\mathbb{F}_5[X]$.

Exercice 3

On considère le corps à 3 éléments $\mathbb{Z}_3/3\mathbb{Z}_3$ que l'on notera $\mathbb{F}_3$. On peut le représenter par les 3 entiers $\{0, 1, 2\}$ muni des lois d'addition et de multiplication modulo 3 données par les tables

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

table d'addition dans $\mathbb{F}_3$

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

table de multiplication dans $\mathbb{F}_3$

On admettra que le polynôme $P(X) = X^3 + 2X^2 + 1 \in \mathbb{F}_3[X]$ est irréductible et donc que $\mathbb{F}_3[X]/P(X)\mathbb{F}_3[X]$ est un corps.

Question 1 : Montrer que $\mathbb{F}_3[X]/P(X)\mathbb{F}_3[X]$ contient 27 éléments que l'on peut représenter par les polynômes de degré inférieur ou égal à 2 de $\mathbb{F}_3[X]$. On notera $\mathbb{F}_{27}$ l'ensemble $\mathbb{F}_3[X]/P(X)\mathbb{F}_3[X]$.

Question 2 : Montrer que

$$X^3 = X^2 + 2 \text{ dans } \mathbb{F}_{27}\big(\Leftrightarrow X^3 \equiv X^2 + 2 \mod (X^3 + 2X^2 + 1)\mathbb{F}_3[X]\big)$$
$$X^4 = X^3 + 2X = X^2 + 2X + 2 \text{ dans } \mathbb{F}_{27}$$
$$X^5 = x^3 + 2X^2 + 2X = 2X + 2 \text{ dans } \mathbb{F}_{27}$$

Question 3 : Écrire les puissances successives de X pour des exposants allant de 0 à 26. Déduisez-en que la suite $n \mapsto x^n$ est périodique de période 26 dans $\mathbb{F}_{27}$ et que tout élément non nul de $\mathbb{F}_{27}$ est représentable d'une et une seul manière par une puissance de x (autrement dit le groupe multiplicatif des éléments non nuls de $\mathbb{F}_{27}$ est cyclique).

Question 4 : Comme $\mathbb{F}_{27} - \{0\} = \mathbb{F}_{27}^*$ contient 26 éléments on peut coder les 26 lettres de l'alphabet par un élément et un seul de $\mathbb{F}_{27}^*$ de la manière suivante

$A \leftrightarrow 1$	$B \leftrightarrow 2$	$C \leftrightarrow x$	$D \leftrightarrow x+1$
$E \leftrightarrow x+2$	$F \leftrightarrow 2x$	$G \leftrightarrow 2x+1$	$H \leftrightarrow 2x+2$
$I \leftrightarrow x^2$	$J \leftrightarrow x^2+1$	$K \leftrightarrow x^2+2$	$L \leftrightarrow x^2+x$
$M \leftrightarrow x^2+x+1$	$N \leftrightarrow x^2+x+2$	$O \leftrightarrow x^2+2x$	$P \leftrightarrow x^2+2x+1$
$Q \leftrightarrow x^2+2x+2$	$R \leftrightarrow 2x^2$	$S \leftrightarrow 2x^2+1$	$T \leftrightarrow 2x^2+2$
$U \leftrightarrow 2x^2+x$	$V \leftrightarrow 2x^2+x+1$	$W \leftrightarrow 2x^2+x+2$	$X \leftrightarrow 2x^2+2x$
$Y \leftrightarrow 2x^2+2x+1$	$Z \leftrightarrow 2x^2+2x+2$		

Montrer que l'on peut alors utilser $\mathbb{F}_{27}^*$ pour construire un système El Gamal avec pour générateur $g = x$ et exposant $\alpha = 11$.

On code avec ce cryptosystème lettre à lettre : à quelles lettres correspondent les couples $(y_1, y_2) = (K, H)$ et $(y_1, y_2) = (F, A)$. Coder les lettres Z, et H.

Exercice 4

Alice et Bob veulent correspondre en employant un système RSA. Ils s'envoient des entiers entre 1 et 9 codés par blocs de 3.

Pour fabriquer sa clé Alice choisit comme nombres premiers :

$$p_a = 277 \quad q_a = 281$$

Elle veut choisir son exposant e_a dans la liste $9,\ 10,\ 11,\ 12$. Quels peuvent être ses choix. Elle choisit le plus grand. Quelle est sa clé publique, quelle est sa clef privée ?

Pour fabriquer sa clé Bob choisit comme nombres premiers

$$p_b = 223 \quad q_b = 233$$

Il choisit son exposant e_b dans la liste $5,\ 6,\ 7$. Quels sont ses choix possibles. Il choisit le plus petit. Quelle est sa clé privée, quelle est sa clé publique ?

Alice veut envoyer le message $M = 785$ crypté et signé à Bob. Qu'envoie Alice ?

Annexe 1 : Données numériques

Tables 1

Table des couples $[i,\ t_1(i) = 785^i \mod 77837]$ pour $1 \leq i \leq 100$

[1, 785], [2, 71366], [3, 57507], [4, 75372], [5, 10900], [6, 72267], [7, 64259], [8, 4939], [9, 63102], [10, 30738], [11, 77697], [12, 45774], [13, 49733], [14, 44068], [15, 33752], [16, 30740], [17, 1430], [18, 32832], [19, 9073], [20, 39138], [21, 55552], [22, 19600], [23, 52111], [24, 42710], [25, 57440], [26, 22777], [27, 55272], [28, 33311], [29, 73740], [30, 53009], [31, 47107], [32, 6420], [33, 58132], [34, 21138], [35, 14049], [36, 53448], [37, 2537], [38, 45620], [39, 6680], [40, 28721], [41, 51092], [42, 21165], [43, 35244], [44, 34405], [45, 76323], [46, 56902], [47, 67469], [48, 34005], [49, 73671], [50, 76681], [51, 26584], [52, 8124], [53, 72543], [54, 47408], [55, 9194], [56, 56286], [57, 50931], [58, 50454], [59, 65194], [60, 38381], [61, 6166], [62, 14416], [63, 30195], [64, 40627], [65, 56862], [66, 36069], [67, 59334], [68, 30664], [69, 19607], [70, 57606], [71, 75250], [72, 70804], [73, 5522], [74, 53735], [75, 72158], [76, 56531], [77, 9745], [78, 21799], [79, 65912], [80, 57152], [81, 30208], [82, 50832], [83, 50576], [84, 5290], [85, 27289], [86, 16690], [87, 25034], [88, 36766], [89, 61620], [90, 34923], [91, 15931], [92, 51915], [93, 44524], [94, 2527], [95, 37770], [96, 71390], [97, 76347], [98, 75742], [99, 67839], [100, 13107]

Tables 2

Table des couples $[i,\ t_8(i) = 785^i \mod 51959]$ pour $1 \leq i \leq 100$

[1, 785], [2, 44676], [3, 50294], [4, 43909], [5, 19748], [6, 18398], [7, 49787], [8, 9627], [9, 23140], [10, 31209], [11, 26376], [12, 25478], [13, 47974], [14, 41274], [15, 29633], [16, 36232], [17, 20547], [18, 22105], [19, 50078], [20, 30226], [21, 34106], [22, 14325], [23, 21981], [24, 4697], [25, 50015], [26, 32730], [27, 25304], [28, 15302], [29, 9541], [30, 7589], [31, 34039], [32, 13689], [33, 42311], [34, 12334], [35, 17816], [36, 8589], [37, 39654], [38, 4949], [39, 39999], [40, 15979], [41, 21396], [42, 13103], [43, 49932], [44, 19534], [45, 6285], [46, 49579], [47, 2224], [48, 31193], [49, 13816], [50, 38088], [51, 22655], [52, 14197], [53, 25419], [54, 1659], [55, 3340], [56, 23950], [57, 43551], [58, 50472], [59, 27762], [60, 22349], [61, 33782], [62, 19780], [63, 43518], [64, 24567], [65, 8306], [66, 25335], [67, 39637], [68, 43563], [69, 7933], [70, 44284], [71, 2369], [72, 41100], [73, 48920], [74, 4499], [75, 50462], [76, 19912], [77, 43220], [78, 50432], [79, 48321], [80, 1915], [81, 48423], [82, 30026], [83, 32983], [84, 16073], [85, 43227], [86, 3968], [87, 49299], [88, 42219], [89, 44032], [90, 12385], [91, 5892], [92, 869], [93, 6698], [94, 10071], [95, 7967], [96, 19015], [97, 14542], [98, 36449], [99, 35015], [100, 464]

Tables 3

Table des couples $[14000 + i,\ t_2(i) = 785^{14000+i} \mod 77837]$ pour $1 \leq i \leq 100$

[14001, 3876], [14002, 7017], [14003, 59755], [14004, 49801], [14005, 19611], [14006, 60746], [14007, 49366], [14008, 67321], [14009, 73499], [14010, 19498], [14011, 49878], [14012, 2219], [14013, 29501], [14014, 40696], [14015, 33190], [14016, 56592], [14017, 57630], [14018, 16253], [14019, 71174], [14020, 62461], [14021, 72412], [14022, 22410], [14023, 688], [14024, 73058], [14025, 62498], [14026, 23620], [14027, 16494], [14028, 26848], [14029, 59690], [14030, 76613], [14031, 51041], [14032, 58967], [14033, 53917], [14034, 59354], [14035, 46364], [14036, 45861], [14037, 40191], [14038, 25950], [14039, 55293], [14040, 49796], [14041, 15686], [14042, 15264], [14043, 73179], [14044, 1809], [14045, 18999], [14046, 47348], [14047, 39931], [14048, 55361], [14049, 25339], [14050, 42680], [14051, 33890], [14052, 61233], [14053, 42476], [14054, 29424], [14055, 58088], [14056, 64435], [14057, 65262], [14058, 13924], [14059, 33160], [14060, 33042], [14061, 18249], [14062, 3457], [14063, 67287], [14064, 46809], [14065, 6001], [14066, 40565], [14067, 8192], [14068, 48086], [14069, 74402], [14070, 27820], [14071, 44340], [14072, 13761], [14073, 60879], [14074, 75934], [14075, 62885], [14076, 16067], [14077, 3001], [14078, 20675], [14079, 39779], [14080, 13878], [14081, 74887], [14082, 19360], [14083, 19385], [14084, 39010], [14085, 32909], [14086, 69518], [14087, 7893], [14088, 46882], [14089, 63306], [14090, 35204], [14091, 3005], [14092, 23815], [14093, 13895], [14094, 10395], [14095, 65027], [14096, 62960], [14097, 74942], [14098, 62535], [14099, 52665], [14100, 10578]

Tables 4

Table des couples $[t_2(i),\ t_4(i) = t_2(i)^5 \mod 51959]$ pour $1 \leq i \leq 100$

[3876, 29484], [7017, 19873], [59755, 20562], [49801, 33825], [19611, 3570], [60746, 8072], [49366, 1201], [67321, 6681], [73499, 41419], [19498, 45999], [49878, 38055], [2219, 1516], [29501, 2224], [40696, 36432], [33190, 24876], [56592, 46765], [57630, 43953], [16253, 13667], [71174, 2999], [62461, 13236], [72412, 5110], [22410, 35317], [688, 24883], [73058, 24986], [62498, 2875], [23620, 30016], [16494, 32125], [26848, 15248], [59690, 15978], [76613, 32398], [51041, 10545], [58967, 41645], [53917, 47465], [59354, 34291], [46364, 1388], [45861, 43809], [40191, 18829], [25950, 22094], [55293, 6645], [49796, 49880], [15686, 7348], [15264, 1634], [73179, 22323], [1809, 4246], [18999, 4602], [47348, 49658], [39931, 6638], [55361, 3046], [25339, 38716], [42680, 26076], [33890, 48866], [61233, 41644], [42476, 46069], [29424, 11632], [58088, 45810], [64435, 1597], [65262, 46039], [13924, 13353], [33160, 3863], [33042, 29136], [18249, 20862], [3457, 676], [67287, 31987], [46809, 46751], [6001, 2949], [40565, 51211], [8192, 51388], [48086, 33433], [74402, 21095], [27820, 28409], [44340, 25099], [13761, 40369], [60879, 21185], [75934, 49081], [62885, 23637], [16067, 22791], [3001, 21613], [20675, 45769], [39779, 1163], [13878, 26050], [74887, 19505], [19360, 5902], [19385, 3092], [39010, 47439], [32909, 23694], [69518, 50422], [7893, 307], [46882, 50357], [63306, 36413], [35204, 310], [3005, 51644], [23815, 21232], [13895, 10145], [10395, 44164], [65027, 19550], [62960, 13681], [74942, 32060], [62535, 16892], [52665, 38010], [10578, 22584]

Tables 5

Table des couples $[10300 + i,\ t_5(i) = 785^{10300+i} \mod 51959]$ pour $1 \leq i \leq 100$

[10301, 3669], [10302, 22420], [10303, 37558], [10304, 22277], [10305, 29221], [10306, 24566], [10307, 7521], [10308, 32618], [10309, 41302], [10310, 51613], [10311, 40144], [10312, 25886], [10313, 4541], [10314, 31473], [10315, 25780], [10316, 25249], [10317, 24086], [10318, 46393], [10319, 47205], [10320, 9158], [10321, 18688], [10322, 17642], [10323, 27876], [10324, 7921], [10325, 34864], [10326, 37806], [10327, 9121], [10328, 41602], [10329, 27318], [10330, 37522], [10331, 45976], [10332, 31614], [10333, 32547], [10334, 37526], [10335, 49116], [10336, 2482], [10337, 25887], [10338, 5326], [10339, 24190], [10340, 24115], [10341, 17199], [10342, 43834], [10343, 12832], [10344, 45033], [10345, 18785], [10346, 41828], [10347, 48851], [10348, 2293], [10349, 33399], [10350, 30879], [10351, 27121], [10352, 38754], [10353, 25875], [10354, 47865], [10355, 7668], [10356, 44095], [10357, 9881], [10358, 14694], [10359, 51851], [10360, 19138], [10361, 7179], [10362, 23943], [10363, 38056], [10364, 49494], [10365, 39417], [10366, 26740], [10367, 51423], [10368, 46871], [10369, 6763], [10370, 9137], [10371, 2203], [10372, 14708], [10373, 10882], [10374, 21094], [10375, 35828], [10376, 15161], [10377, 2774], [10378, 47271], [10379, 9009], [10380, 5641], [10381, 11670], [10382, 16166], [10383, 12314], [10384, 2116], [10385, 50331], [10386, 20995], [10387, 10072], [10388, 8752], [10389, 11732], [10390, 12877], [10391, 28399], [10392, 2804], [10393, 18862], [10394, 50314], [10395, 7650], [10396, 29965], [10397, 37057], [10398, 44664], [10399, 40874], [10400, 27387]

Tables 6

Table des couples $[t_5(i),\ t_7(i) = t_5(i)^{11} \mod 77837]$ pour $1 \leq i \leq 100$

[3669, 40067], [22420, 57384], [37558, 44123], [22277, 33124], [29221, 49494], [24566, 22702], [7521, 20637], [32618, 39432], [41302, 11487], [51613, 76531], [40144, 9959], [25886, 24981], [4541, 66799], [31473, 64912], [25780, 75063], [25249, 2909], [24086, 49747], [46393, 12325], [47205, 71974], [9158, 27932], [18688, 71847], [17642, 57665], [27876, 807], [7921, 26748], [34864, 10931], [37806, 3461], [9121, 57797], [41602, 73331], [27318, 49677], [37522, 50614], [45976, 64798], [31614, 14804], [32547, 56482], [37526, 37374], [49116, 70647], [2482, 19276], [25887, 26298], [5326, 14239], [24190, 10605], [24115, 45559], [17199, 14671], [43834, 34250], [12832, 27013], [45033, 25003], [18785, 35588], [41828, 32133], [48851, 48130], [2293, 4698], [33399, 1458], [30879, 67974], [27121, 10], [38754, 71728], [25875, 30667], [47865, 28709], [7668, 35803], [44095, 40091], [9881, 46457], [14694, 52189], [51851, 70007], [19138, 21319], [7179, 8893], [23943, 33217], [38056, 6783], [49494, 37566], [39417, 29177], [26740, 17624], [51423, 4777], [46871, 50142], [6763, 21283], [9137, 44127], [2203, 64428], [14708, 2523], [10882, 52313], [21094, 14820], [35828, 3012], [15161, 40653], [2774, 35372], [47271, 56381], [9009, 14295], [5641, 56809], [11670, 64664], [16166, 17737], [12314, 11340], [2116, 55391], [50331, 17082], [20995, 28672], [10072, 29371], [8752, 37274], [11732, 49234], [12877, 28101], [28399, 3215], [2804, 48143], [18862, 28546], [50314, 30461], [7650, 71274], [29965, 20011], [37057, 9108], [44664, 44004], [40874, 68194], [27387, 45582]

Message à déchiffrer

1	1	0	0	0	1	0	0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0	1	0	1	1	1	0	0
1	0	0	0	1	0	0	0	1	0	0	0	0	1	1
0	0	1	1	1	1	0	1	1	0	0	0	1	0	1
1	1	1	1	1	0	0	1	1	0	0	0	0	0	1
0	0	0	1	1	0	0	0	1	0	0	0	1	0	1
1	0	0	0	1	0	1	0	1	1	0	0	1	0	1

1	0	1	1	1	0	0	0	0	0	0	0	0	1	1
1	0	1	0	0	1	0	1	1	0	1	1	0	0	1
0	0	1	0	1	1	0	0	1	1	0	1	1	1	0
0	0	1	0	1	0	0	1	1	0	1	0	1	1	1