Enseignement libre
Introduction à la Cryptographie
2012/2013

UNIVERSITÉ de Cergy-Pontoise

Examen, durée 3 heures maximum

Tous documents autorisés mais les communications avec d'autres personnes sont interdites.
Toute note supérieure à 20 sera ramenée à 20.

Exercice 1 : (sur 10 points) L'objectif de cet exercice est d'étudier ce qui se passe dans le protocole RSA lorsque le message est multiple de p ou q.
On se donne donc deux nombres premiers distincts p et q, de 300 chiffres en écriture décimale. On appelle message un nombre entier m de $[0; \ldots ; pq-1]$. On a vu dans le cours que

$$m^{(p-1)(q-1)} \equiv 1 \ [pq]$$

lorsque m n'est ni multiple de p, ni multiple de q. Cette relation est évidemment fausse lorsque $m = 0$, néanmoins on va montrer que pour tout m de $[0; \ldots ; pq-1]$, on a :

$$m^{1+(p-1)(q-1)} \equiv m \ [pq]$$

1. Montrer que cette relation est vraie lorsque m n'est ni multiple de p, ni multiple de q. (2 points)
2. Supposons m multiple de p et non multiple de q,
   (a) Montrer que $p | \left(m^{1+(p-1)(q-1)} - m\right)$. (2 points)
   (b) Montrer que $q | \left(m^{(p-1)(q-1)} - 1\right)$ (2 points)
   (c) En déduire que $m^{1+(p-1)(q-1)} \equiv m \ [pq]$. (2 points)
3. Traitez les autres cas. (2 points)

Exercice 2 : (13 points) On appelle courbe elliptique une courbe E de $\mathbb{K}^2$ avec $\mathbb{K}$ corps, dont l'équation est $y^2 = x^3 + ax + b$ avec a et b tels que $\Delta = -16(4a^3 + 27b^2) \neq \bar{0}$. Pour être plus précis, on a

$$E = \{(x, y) \in \mathbb{K}^2 \mid y^2 = x^3 + ax + b\}.$$

Pour $\mathbb{K}$, on prendra $\mathbb{Z}/p\mathbb{Z}$ avec p premier strictement supérieur à 3.

1. Parmi les courbes suivantes, lesquelles sont des courbes elliptiques ? (3 points)
   (a) $y^2 = x^3 + 2x + 1$ sur $\mathbb{Z}/5\mathbb{Z}$.
   (b) $y^2 = x^3 + 4x + 5$ sur $\mathbb{Z}/7\mathbb{Z}$.
   (c) $y^2 = x^3 + x + 1$ sur $\mathbb{Z}/11\mathbb{Z}$.
2. Soit p un nombre premier strictement supérieur à 2.
   (a) Montrer que pour tout $c \in \mathbb{Z}/p\mathbb{Z}$ non nul, l'équation d'inconnue $y \in \mathbb{Z}/p\mathbb{Z}$:
   $$y^2 = c$$
   a soit deux solutions, soit aucune solution. (2 points)
   (b) Que se passe-t-il dans les autres cas ($p = 2$, $c = 0$) ? (2 points)
   (c) En déduire que le cardinal d'une courbe elliptique est forcément impair lorsque $b = 0$. (2 points)
3. Programmation Le nombre de points d'une courbe elliptique est donnée par le cardinal de E plus 1 car on rajoute un point à l'infini, noté $\mathcal{O}$.
   Écrire une procédure dans votre langage favori qui donne le nombre de points d'une courbe sur $\mathbb{Z}/p\mathbb{Z}$ en fonction de a, b et p. On vérifiera que la courbe d'équation
   $$y^2 = x^3 + 3x$$
   a 26 points exactement pour $p = 17$. (4 points)

Exercice 3 : Déchiffrements classique : César, affine et Vigénère. (6 points)

1. Le texte suivant a été chiffré à l'aide d'un chiffrement par décalage (du type de celui de César). Retrouvez le texte original. (1 point)

   abhfsrebafynthreerrafrzoyrrgabhfsrebafyncnvkrafrzoyr

2. Le texte suivant a été chiffré à l'aide d'un chiffrement affine. Retrouvez le texte original. (2 points)

   qbptdabqtunqevqenbqknqdprpiviudrpviivtbptfdinqvdbpeidqzv

3. Le texte suivant a été chiffré à l'aide d'un chiffrement de Vigénère. Retrouvez la clé et remarquez ce que le texte a d'extraordinaire. (3 points)

   lbndyjinwbugcwppthjpdrigxwlxwofafauhzbdpkaugbiuxeaccfwnktbaitzjdfgmpfb
   jgzticogijawlhlgmxerucdgicwwnhldjjjohidilhzbjdwcwwzbcaafcifbldxohxwzijgfci
   tzfjeauxdwfcjguxdwmhlwnffihxxpldrzcdnchufgcaminpthndfhccdhucegogfbgderi
   cewfxrbiglwnalgcvywzxnonxzb

Exercice 4 : (3 points) Trouvez le nom propre de 6 lettres caché dans le texte suivant :
Le Patna franchit les détroits, traversa le golfe, suivit le passage du premier degré. Il piqua droit vers la mer rouge, sous un ciel serein, sous un ciel torride et sans nuage, sous un éclaboussement de soleil qui tuait toute pensée, serrait le cœur, desséchait toute impulsion de force et d'énergie.

Exercice 5 : Programmation (6 points) En 1931, Lester S. Hill publie un système de chiffrement par groupement de lettres. Au lieu de chiffrer les lettres une par une, on chiffre les lettres par groupe de n où $n \geq 2$. On va juste programmer ici le chiffrement de Hill dans le cas $n = 2$.
Exemple : je donne ici un exemple de chiffrement de Hill afin de faciliter la compréhension. On pose $k_1 = 15$, $k_2 = 8$, $k_3 = 25$ et $k_4 = 5$, et $A = \begin{pmatrix} 15 & 8 \\ 25 & 5 \end{pmatrix}$. On veut chiffrer la chaîne de caractères "cout". On commence par l'écrire sous forme de suite de nombres : $(2, 14, 20, 19)$, puis on calcule

$$A\begin{pmatrix} 2 \\ 14 \end{pmatrix} = \begin{pmatrix} 15 \times 2 + 8 \times 14 \\ 25 \times 2 + 5 \times 14 \end{pmatrix} = \begin{pmatrix} 142 \\ 120 \end{pmatrix} \overset{\text{mod}(26)}{\longrightarrow} \begin{pmatrix} 12 \\ 16 \end{pmatrix}$$

$$A\begin{pmatrix} 20 \\ 19 \end{pmatrix} = \begin{pmatrix} 15 \times 20 + 8 \times 19 \\ 25 \times 20 + 5 \times 19 \end{pmatrix} = \begin{pmatrix} 452 \\ 595 \end{pmatrix} \overset{\text{mod}(26)}{\longrightarrow} \begin{pmatrix} 10 \\ 23 \end{pmatrix}$$

Puis, on transforme la suite de nombres obtenue : $(12, 16, 10, 23)$ par les caractères correspondants, ce qui donne "mqkx".

La clé est donc constituée de 4 entiers (k_1, k_2, k_3, k_4) de $\{0; \ldots; 25\}$, pour que la clé soit valide il faut que $\Delta = k_1k_4 - k_2k_3$ soit premier avec 26, c'est à dire ni multiple de 2, ni de 13. Si la clé n'est pas valide, on ne pourra pas inverser le chiffrement.

1. Écrire une procédure `valide(k1,k2,k3,k4)`, qui renvoie `True` si la clé est valide, et `False` sinon. (1 point)
2. Écrire une procédure `hill1(k1,k2,k3,k4,c1,c2)` qui renvoie (k1×c1+k2×c2 mod(26), k3×c1+k4×c2 mod(26)) (1 point) Cette procédure chiffre deux entiers (c_1, c_2) de $\{0; \ldots; 25\}$ représentant des lettres, par deux autres entiers de $\{0; \ldots; 25\}$.
3. Écrire une procédure `hill(k1,k2,k3,k4,m)` où `m` est une chaîne avec un nombre pair de caractères, qui chiffre deux par deux les caractères de `m` et fabrique la chaîne de caractères correspondant aux nombres chiffrés (voir exemple). (4 points)

Projet : Nombre de personnes sur le projet : 2 ou 3 si un site internet est fait.
Date limite de dépôt : première semaine de janvier.
Écrire une procédure qui transforme un texte (suite de lettres d'un alphabet déterminé à l'avance) en une partie d'échecs. On pourra s'appuyer sur des programmes d'échecs existants. L'idée est la suivante : on numérise le texte, puis on cache les chiffres un par un dans les coups successifs. Lorsqu'un joueur a plus que 10 possibilités de coups, le chiffre correspond à l'unité du numéro du coup. Par exemple, si le chiffre à cacher est 2, on choisit le coup numéro 2 ou le 12 ou le 22 etc. Il faut donc ordonner les coups de chaque joueur, mais il y a des programmes qui font déjà cela.

Correction

Exercice 1 :

1. Si m n'est ni multiple de p, ni de q, d'après le cours on a $m^{(p-1)(q-1)} \equiv 1\ [pq]$, donc pq divise $m^{(p-1)(q-1)} - 1$, forcément pq divise tous les multiples de ce nombre, et en particulier $m \times (m^{(p-1)(q-1)} - 1)$. D'où $m^{1+(p-1)(q-1)} \equiv m\ [pq]$
2. (a) m est multiple de p, donc $m^{1+(p-1)(q-1)}$ également et leur différence aussi.
   (b) D'après Fermat, comme q est premier et m non multiple de q, on a $m^{q-1} \equiv 1\ [q]$, d'où $(m^{q-1})^{p-1} \equiv 1^{p-1}\ [q]$ et finalement on a $m^{(p-1)(q-1)} - 1$ multiple de q.
   (c) de la question précédente, on déduit immédiatement que q divise $m^{1+(p-1)(q-1)} - m$ qui est égal à pk pour un certain entier k d'après le (a). Comme p est premier avec q, d'après Gauss, q divise k et donc $m^{1+(p-1)(q-1)} - m$ est égal à pqk' pour un certain entier k'.
3. Lorsque m est multiple de q et non multiple de p, on procède de la même manière en inversant le rôle de p et de q. Lorsque m est à la fois multiple de p et q, m est forcément nul et la relation est évidement vérifiée.

Exercice 2 :

1. (a) $\Delta = \bar{1}$ donc c'est une courbe elliptique.
   (b) $\Delta = \bar{0}$ donc ce n'est pas une courbe elliptique.
   (c) $\Delta = 1\bar{0}$ donc c'est une courbe elliptique.
2. (a) Supposons que l'équation $y^2 = c$ d'inconnue y admette une solution y_1, alors cette équation équivaut à ${y^2} = {y_1}^2$ donc à $(y - y_1)(y + y_1) = \bar{0}$. Or dans $\mathbb{Z}/p\mathbb{Z}$, un produit est nul ssi un des facteurs est nul puisque p est premier. En effet si un nombre premier divise un produit, il divise forcément un des facteurs. Donc $y^2 = c$ équivaut finalement à $y = y_1$ ou $y = -y1$. D'autre part $y_1 \neq -y1$ car $2y_1 \neq 0$ (2 n'est pas nul car $p \neq 2$ et y_1 n'est pas nul car autrement on aurait $c = 0$).
   (b) Lorsque $p = 2$, il n'y a que deux valeurs possibles 0 et 1. Si c est non nul, $c = 1$ et $y = 1$ est solution unique. Si c est nul (et toujours $p = 2$) alors $y = 0$ est l'unique solution.
   Lorsque $c = 0$, la seule solution est $y = 0$ parce que p est premier.
   (c) Si $b = 0$ alors $x^3 + ax = 0$ admet comme solution $x = 0$ plus les solutions de $x^2 + a = 0$ qui sont au nombre de 0 ou 2. On aura alors 1 ou 3 points dont l'ordonnée est nulle. Avec la première question, il est évident que le nombre de points d'ordonnée non nulle est pair (ils vont par deux). Donc en tout, une courbe elliptique d'équation $y^2 = x^3 + ax$ a un nombre de points impair (si on ne compte pas le point à l'infini).
3.
```
def nombre_de_points(a,b,p):
 n=1
 for x in range(p):
   for y in range(p):
     if ((y**2 - x**3+a*x+b)%p == 0):
       n += 1
 return n
```

Exercice 3 :

1. Décalage de 13 lettres, il s'agit d'une partie d'une déclaration de guerre historique. Le message original était codé à l'aide d'un dictionnaire.

   Nous ferons la guerre ensemble et nous ferons la paix ensemble.

2. Un autre extrait du même texte. La clé est $a = 11$ et $b = 3$. On trouve le texte suivant :

   Nous avons l'intention d'inaugurer la guerre sous-marine à outrance.

3. La clé est "loup" et le texte est extrait de la disparition de Pérec, il ne comporte aucun "e" !

Exercice 4 : Les lettres sont écrites dans deux tailles différentes. On note les 6 changements de taille de caractères, qui correspondent aux lettres CONRAD (auteur du texte)

Exercice 5 : Voir fichier examen.py