Examen Partiel – Cryptographie
jeudi 1er décembre 2005
Correction

Exercice 1 (12pts)
Soit p un nombre premier. Donner une formule simple pour

$$\left(\frac{21}{p}\right)$$

Indication : on distinguera les trois cas : 1) $p = 2$; 2) $p = 3$ ou $p = 7$; 3) p impair et $p \neq 5, 7$.

Solution. 1) Pour $p = 2$, on a $\left(\frac{21}{2}\right) = \left(\frac{21 \mod 2}{2}\right) = \left(\frac{1}{2}\right) = 1$ puisque 1 n'est pas divisible par 2 et est un carré modulo 2.
2) Pour $p = 3$ et $p = 7$, puisque p divise 21, on a par définition $\left(\frac{21}{p}\right) = 0$.
3) Pour p impair, p différent de 3 et 7, on utilise les propriétés du symbole de Jacobi

$$\left(\frac{21}{p}\right) = (-1)^{\frac{(21-1)(p-1)}{4}}\left(\frac{p}{21}\right) = (-1)^{5(p-1)}\left(\frac{p}{3\times 7}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{7}\right)$$

Les classes inversibles modulo 3 sont 1 et 2, et 1 est un carré modulo 3 (c'est le carré de 1), alors que 2 n'est pas un carré modulo 3. Donc on a

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv 2 \pmod 3 \end{cases}$$

Les classes inversibles modulo 7 sont $1, 2, 3, 4, 5$ et 6. Parmi celles-ci les carrés sont 1 (carré de 1), 2 (carré de 3) et 4 (carré de 2). Ainsi on a

$$\left(\frac{p}{7}\right) = \begin{cases} 1 & \text{si } p \equiv 1, 2, 4 \pmod 7 \\ -1 & \text{si } p \equiv 3, 5, 6 \pmod 7 \end{cases}$$

On trouve donc que $\left(\frac{p}{21}\right) = 1$ si et seulement si on est dans un des deux cas suivants : a) $p \equiv 1 \pmod 3$ et $p \equiv 1, 2, 4 \pmod 7$, ou b) $p \equiv 2 \pmod 3$ et $p \equiv 3, 5, 6 \pmod 7$. Pour obtenir des congruences modulo 21, on utilise le théorème des restes chinois. Notons que $(-2)\cdot 3 + 1\cdot 7 = 1$ et donc les deux congruences

$$\begin{cases} x \equiv a \pmod 3 \\ x \equiv b \pmod 7 \end{cases}$$

sont équivalentes à la congruence $x \equiv c \pmod{21}$ où $c = 7a - 6b \mod 21$. On trouve ainsi que

$$\left(\frac{p}{21}\right) = 1 \text{ si et seulement si } p \equiv 1, 4, 5, 16, 17, 20$$

Les classes possibles pour p modulo 21 sont $1, 2, 4, 5, 7, 8, 10, 11, 13, 16, 17, 19, 20$. En effet, les classes 3, 6, 9, 12, 15, 18 ne sont pas possibles car elles impliquent que p est divisible par 3,

de même si $p \equiv 7, 14 \pmod{21}$ alors p est divisible par 7. Puisque $\left(\frac{p}{21}\right)$ vaut 1 pour les 6 classes listés ci-dessus, on a $\left(\frac{p}{21}\right) = -1$ pour les 6 classes restantes : $2, 8, 10, 11, 13$ et 19

Exercice 2 (6pts)
On considère un diagramme de Feistel à deux rondes où les fonctions f_1 et f_2 sont constantes, c'est-à-dire il existe deux chaînes binaires c_1 et c_2 telles que $f_1(w) = c_1$ et $f_2(w) = c_2$ pour tout w.

1. Donner les expressions des chaînes w_1'' et w_2'' renvoyées par le diagramme.
2. Montrer comment un attaquant, qui ne connaît pas les valeurs de c_1 et c_2, peut quand même retrouver w_1 et w_2 à partir de w_1'' et w_2'' à l'aide d'une *seule* attaque à texte clair choisi.

Solution. 1. Les chaînes renvoyés par le diagramme sont $w_1'' = f_2(f_1(w_1) \oplus w_2) \oplus w_1$ et $w_2'' = f_1(w_1) \oplus w_2$. Puisque les fonctions sont constantes, on a donc $w_1'' = c_2 \oplus w_1$ et $w_2'' = c_1 \oplus w_2$.
2. Un attaquant qui intercepte w_1'' et w_2'' pour faire une attaque à texte clair choisi en demandant le cryptage de la chaîne $w_1'' \cdot w_2''$. Il reçoit en réponse les chaînes $c_2 \oplus w_1'' = c_2 \oplus c_2 \oplus w_1 = w_1$ et $c_1 \oplus w_2'' = c_1 \oplus c_1 \oplus w_2 = w_2$. Il retrouve ainsi le message clair initial.

Exercice 3 (10pts)
Décoder le message suivant encodé par le procotole de Vigenère avec une clé de longueur 2

`OSFFBDWCJFDAPSGSYWJSQSUSQSVHSZXGFCQ`
`GLRHFHRHBRGMCXFVQRAPSXBSFRHRQRZHGXF`

(Note : les espaces et signes de ponctuation ont été supprimés.)

Solution. On considère les deux sous-messages extraits : `OFBWJDPGYJQUQVSXFQLHHHRMXVRPXSRRRHX` et `SFDCFASSWSSSSHZGCGRFRBGCFQASBFHQZGF`. Dans le premier sous-message, la lettre la plus fréquente est `R` avec 5 occurences. Après, on trouve `H` et `X` avec chacune 4 occurences. Dans le deuxième sous-message, la lettre la plus fréquente est `S` avec 7 occurences, ensuite on a `F` avec 6 occurences. En posant `R` comme codage de `E` par la première lettre `C1` de la clé et `S` comme codage de `E` par la deuxième lettre `C2`, on obtient que `C1 = R - E = N` et `C2 = S - E = O`. On essait de décoder le début du message, on obtient

`BESROP...`

Ce qui ne semble pas à un texte en français. On essaie d'autre possibilités. Par exemple, en supposant que le codage de `E + C1 = H`. On trouve alors que `C1 = H - E = D`. Le décodage du début du message avec la clé `DO` donne

`LECRYPTOGRAMMEDEVIGENERE...`

donc est correct.

Exercice 4 (18pts)
Soit G un groupe cyclique d'ordre $N = p^2q$ avec p et q deux nombres premiers distincts.
Notons γ un générateur de G et soit $\alpha \in G$.
On cherche à déterminer le logarithme discret de α en base γ, c'est-à-dire à trouver x tel que $0 \leq x < N$ et $\gamma^x = \alpha$.

1. On pose $y := x \mod p^2$.
   (a) Montrer qu'on peut écrire
   $$y = y_0 + y_1 \cdot p$$
   avec $0 \leq y_0 \leq p-1$ et $0 \leq y_1 \leq p-1$.
   (b) Calculer α^{pq} en tant que puissance de γ. En déduire que y_0 est l'unique solution (entre 0 et $p-1$) de
   $$\beta^{y_0} = \alpha^{pq}$$
   où $\beta = \gamma^{pq}$.
   (c) On pose $\alpha_1 = \alpha \cdot \gamma^{-y_0}$. Montrer que y_1 est l'unique solution (entre 0 et $p-1$) de
   $$\beta^{y_1} = \alpha_1^q$$
2. On pose $z := x \mod q$.
   (a) Montrer que z est l'unique solution (entre 0 et $q-1$) de
   $$\eta^z = \alpha^{p^2}$$
   où $\eta = \gamma^{p^2}$.
3. Expliquer comment on peut retrouver x à partir de y et z.
4. Que peut-on en conclure sur la complexité du problème du logarithme discret dans le groupe G ?

Solution. 1.(a) Puisque y est le reste la division euclidienne de x par p^2, on a $0 \leq y < p^2$. On pose
$$y = qp + r$$
la division euclidienne de y par p. On a par construction $0 \leq r < p$ et aussi $q = (y-r)/p \leq y/p < p^2/p = p$. Donc on peut prendre $y_1 = q$ et $y_0 = r$.
1.(b) Posons $x = kp^2 + y = kp^2 + y_0 + y_1 p$. On calcule
$$\alpha^{pq} = \left(\gamma^x\right)^{pq} = \gamma^{xpq} = \gamma^{kp^3q + y_0pq + y_1p^2q} = \left(\gamma^{p^2q}\right)^{kp} \left(\gamma^{pq}\right)^{y_0} \left(\gamma^{p^2q}\right)^{y_1} = \left(\gamma^{pq}\right)^{y_0}$$
puisque γ^{p^2q} est l'identité de G. Ainsi, on trouve que
$$\alpha^{pq} = \beta^{y_0}$$

Puisque $\beta = \alpha^{pq}$, on sait que β est d'ordre $N/pq = p$ et y_0 est l'unique solution de l'équation ci-dessus entre 0 et $p-1$.
1.(c) On calcule

$$\alpha_1^q = \left(\alpha \cdot \gamma^{-y_0}\right)^q = \alpha^q \cdot \gamma^{-qy_0} = \gamma^{q(kp^2+y_0+y_1p)-qy_0} = \left(\gamma^{p^2q}\right)^k \left(\gamma^{pq}\right)^{y_1} = \beta^{y_1}$$

Et de même manière, y_1 est l'unique solution entre 0 et $p-1$ de cette équation.
2.(a) On écrit $x = lq + z$ avec $0 \leq z < q$. On calcule

$$\alpha^{p^2} = \left(\gamma^x\right)^{p^2} = \gamma^{p^2(lq+z)} = \left(\gamma^{p^2q}\right)^l \left(\gamma^{p^2}\right)^z = \eta^z$$

De plus η est d'ordre $N/p^2 = q$ et donc z est l'unique solution entre 0 et $q-1$ de cette équation.
3. Une fois déterminer y et z, on a le système suivant

$$\begin{cases} x \equiv y \pmod{p^2} \\ x \equiv z \pmod{q} \end{cases}$$

En utilisant le théorème des reste chinois, on en déduit la valeur de x.
4. Pour résoudre le problème du logarithme discret dans G, il suffit de savoir résoudre successivement les trois problèmes de logarithme discret donné ci-dessus avec des éléments d'ordre respectivement p, p et q. Donc la complexité du problème du logarithme discret dépend juste de la taille du plus grand des nombres premiers p et q, et non pas de la taille de N.