Examen Partiel – Cryptographie

jeudi 1er décembre 2005

Exercice 1

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 $p \neq 5, 7$.

Exercice 2

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.

Exercice 3

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.)

Exercice 4

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 ?