Licence Informatique 3ème année
(Ens-Lyon, Université Lyon-I)

Calcul formel et cryptographie
Contrôle du vendredi 20 mai 2005 . Durée 3h.

La qualité de la rédaction et de la présentation seront des facteurs importants d'appréciation.

Exercice 1

Soit $f = X^3 - 2\,X + 3$. Montrer que

1. $f(X) \equiv 0 \pmod 3$ admet une unique solution modulo 3.
2. $f(X) \equiv 0 \pmod 9$ admet une unique solution modulo 9 et l'expliciter.
3. $f(X) \equiv 0 \pmod{3^n}$ admet une unique solution modulo 3^n, pour tout $n \geq 1$.

Exercice 2

Alice utilise RSA, et sa clef publique est (N, e), avec $N = pq$, p et q premiers. On dit que le message clair x est non dissimulé si $x^e \bmod N = x$.

1. Quel est le nombre de solutions de l'équation $u^e = u$ dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$? Indication : vous pourrez considérer un générateur g du groupe multiplicatif $\mathbb{F}_p^\times$. Le résultat s'exprime simplement en fonction de $\mathrm{pgcd}(e-1, p-1)$.
2. En déduire que le nombre de messages clairs non dissimulés est

$$(1 + \mathrm{pgcd}(e-1, p-1))(1 + \mathrm{pgcd}(e-1, q-1)).$$

Exercice 3

Si $a \in \mathbb{Z}$ est un carré, a est un carré modulo p pour tout premiep p. On se propose de démontrer la réciproque : *si $a \in \mathbb{Z}$ est un carré modulo p pour tout premier p, alors a est un carré de $\mathbb{Z}$*. Par contraposition, il suffit de démontrer que si a n'est pas un carré, il existe un nombre premier p tel que $\left(\frac{a}{p}\right) = -1$. Soit donc a un entier non carré.

1. Démontrer que l'une des assertions suivantes est vraie.
   (a) a est l'opposé d'un carré, $a = -b^2$, $b > 0$.
   (b) $a = \pm\, 2^{2k+1} q$, avec q impair.

(c) $a = \pm\, 2^{2k} q^{2t+1} b$ avec b et q impairs, q premier ne divisant pas b.

2. Dans le premier cas $a = -b^2$, $b > 0$, montrer qu'il existe $m \in \mathbb{Z}$, avec $m \equiv 3 \pmod 4$, et $(m, b) = 1$. Montrer que $\left(\frac{a}{m}\right) = -1$, où $\left(\frac{a}{m}\right)$ est le symbole de Jacobi.
3. Soit $a = \pm 2^{2k+1} q$ avec q impair. Si $q = 1$ montrer que $\left(\frac{a}{5}\right) = -1$. Si $q > 1$ montrer qu'il existe $m > 0$, $m \equiv 5 \pmod 8$ et $m \equiv 1 \pmod q$. Prouver que $\left(\frac{a}{m}\right) = -1$.
4. Soit $a = \pm 2^{2k} q^{2t+1} b$ avec b et q impairs, q premier ne divisant pas b. Montrer qu'il existe $m > 0$, avec $m \equiv 1 \pmod{4b}$, $\left(\frac{m}{q}\right) = -1$. Montrer que $\left(\frac{a}{m}\right) = -1$.
5. Déduire des questions précédentes que, dans tous les cas, il existe un nombre premier p tel que a ne soit pas un carré modulo p.

Problème

Soit $\mathbb{K}$ un corps commutatif, et f, g deux polynômes de $\mathbb{K}[X, Y]$. Le résultant $R_X(f, g)$ est un polynôme de $\mathbb{K}[Y]$ dont les racines sont les valeurs de y pour lesquelles $f(X, y)$ et $g(X, y)$ ont une racine commune x dans une cloture algébrique de $\mathbb{K}$. On admettra qu'on sait calculer $R_X(f, g)$ et que le degré de $\mathrm{Res}_X(f, g)$ est au plus $\deg_X(f) \deg_X(g)$. De plus si f et g appartiennent à $\mathbb{Z}[X, Y]$, il en est de même de $R_X(f, g)$ calculé dans $\mathbb{C}[X]$, et le résultant de f et g considérés comme des polynômes de $\mathbb{F}_p[X, Y]$ se déduit du résultant calculé dans $\mathbb{C}[X]$ en réduisant ses coefficients modulo p, pout tout premier p.

Une entreprise utilise RSA pour le chiffrement de ses communications. Pour accéler le chiffrement l'exposant e utilisé pour le chiffrement est toujours $e = 3$.

1) Alice envoie le message clair m à trois correspondants Bob_1, Bob_2 et Bob_3, dont les clefs publiques sont $(N_1, 3)$, $(N_2, 3)$ et $(N_3, 3)$. Eve intercepte les trois messages chiffrés $C_1 = m^3 \bmod N_1$, $C_2 = m^3 \bmod N_2$, et $C_3 = m^3 \bmod N_3$. Expliquez le calcul qu'elle fait pour retrouver m.

Le responsable réseau décide de se protéger contre cette attaque de la manière suivante : Il choisit une fois pour toutes un entier k. Avant d'envoyer le message m à Alice, dont la clef publique est $(N, 3)$ ($N = pq$, p et q premiers) Bob choisit au hasard une chaine de bits r_1, de longueur k, puis il calcule $M_1 = 2^k m + r_1$, et envoie le message chiffré $C_1 = M_1^3 \bmod N$.

Eve intercepte et bloque le message chiffré C_1. Alice, ne recevant pas le message attendu, demande à Bob de le lui faire parvenir à nouveau. Bob calcule un nouveau masque aléatoire r_2, puis $M_2 = 2^k m + r_2$ et envoie à Alice le message chiffré $C_2 = M_2^3 \bmod N$.

Eve connait C_1, C_2, N, k et se propose de retrouver m. Notons $\delta = r_2 - r_1 = M_2 - M_1$.

2) Vérifier que $M_1(C_2 - C_1 + 2\delta^3) \equiv \delta(C_2 + 2C_1 - \delta^3) \bmod N$. Comment Eve peut-elle retrouver m si elle connait δ ?

3) Soit $f(X, Y) = X^3 - C_1$, et $g(X, Y) = (X + Y)^3 - C_2$. Montrer que, pour $y = \delta$, les deux polynômes en X, $f(X, y)$ et $g(X, y)$ ont une racine commune modulo N.

4) Eve connait C_2 et C_1, donc f et g. Elle calcule le résultant $h(Y) = \mathrm{Res}_X(f, g)$. Que peut on dire de $h(\delta) \bmod N$?

5) On suppose que $2^k < \frac{1}{3} N^{1/9}$. Par quelle méthode Eve peut-elle calculer δ, (et donc m, par la question 2) ?