Magistère Informatique et Modélisation
(Ens-Lyon, Université Lyon-I)

Calcul formel et cryptographie
Contrôle du vendredi 14 mai 2004 . Durée 3h.

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

Exercice 1 : Question de cours

Soit $F = X^4 + 1$.

1. Quelle est la factorisation de F modulo 2, c'est à dire dans $\mathbb{F}_2[X]$?
2. Soit p un nombre premier, $p \equiv 1 \pmod 8$. Montrer que F n'a pas de facteurs multiples dans $\mathbb{F}_p[X]$. Expliciter la matrice de Berlekamp de F, et en déduire le nombre de facteurs de la factorisation de F dans $\mathbb{F}_p[X]$.
3. Même question avec $p \equiv 3 \pmod 8$.

Exercice 2 : Un autre point de vus sur le paradoxe des anniversaires

N et n sont deux entiers > 0. On dispose d'une urne contenant N boules numérotées de 1 à N. On tire n fois de suite une boule dans l'urne, avec remise après chaque tirage. On note x_i le numéro de la boule obtenue au tirage numéro i. On obtient ainsi une suite $(x_1, x_2, \cdots, x_n)$ d'entiers de l'ensemble $\{1, 2, \ldots, N\}$. Soit X le nombre des couples $(i, j), 1 \leq i < j \leq n$ tels que $x_i = x_j$. On se propose d'étudier la variable aléatoire X. On utilisera pour cela les variables aléatoires $X_{i,j}$, définies pour $1 \leq i < j \leq n$, par

$$X_{i,j} = \begin{cases} 1 & \text{si } x_i = x_j \\ 0 & \text{sinon.} \end{cases}$$

1. Exprimer X en fonction des $X_{i,j}$.
2. (a) En déduire l'espérance de X.
   (b) Combien vaut cette espérance lorsque $n = N$? Lorsque $N = 365$ et $n = 40$?
   (c) Comment choisir n (en fonction de N) pour que $E(X) \geq 1$?
3. (a) Les variables $(X_{i,j})_{1 \leq i < j \leq n}$ sont elles indépendantes dans leur ensemble ?
   (b) Démontrer qu'elles sont deux à deux indépendantes.

(c) En admettant que la variance d'une somme de variables 2 à 2 indépendantes est la somme de leurs variances, exprimer simplement la variance de X en fonction de n et N.

4. On rappelle la formule de Tchebychev : $P(|Y - E(Y)| \geq \lambda) \leq \frac{V(Y)}{\lambda^2}$, où Y est une variable aléatoire d'espérance finie $E(Y)$, de variance finie $V(Y)$, et λ un réel positif quelconque.

   Montrer que
   $$P(X = 0) \leq \frac{V(X)}{E(X)^2}.$$
   En déduire que si $n(n-1) \geq 4(N-1)$ soit, approximativent, $n \geq 2\sqrt{N}$, la probabilité de l'évènement $X > 0$ est plus grande que $1/2$.

5. **Une application du paradoxe des anniversaires.** Une *fonction de hachage cryptographique* est une fonction définie sur un ensemble E de grand cardinal, éventuellement infini, à valeurs dans un ensemble de plus petit cardinal K.

   La fonction f est *fortement résistante aux collisions* si la construction d'un couple $(x, y) \in E \times E$ tel que $x \neq y$ et $f(x) = f(y)$ est pratiquement impossible en temps raisonnable (un tel couple est appelé une collision de f). Cette propriété est nécessaire dans les problèmes de signature par exemple.

   Soit f une fonction de hachage prenant ses valeurs dans l'ensemble $\{1, 2, \ldots, 2^{64}\}$. Expliquer comment fabriquer en un temps raisonnable un couple (x, y) qui est une collision de f, en occupant un espace dont l'ordre de grandeur est quelques dizaines de giga-octets.

Problème

Partie I $N = pq$ est le produit de deux nombres premiers distincts p et q. Soit m un entier. On dira que m *est un bon exposant modulo* N si, pour tout entier x premier avec N, on a $x^m \equiv 1 \pmod{N}$.

1. Montrer que m est un bon exposant si et seulement si c'est un multiple de $p - 1$ et de $q - 1$.
2. Montrer que si m n'est pas un bon exposant modulo N, alors $x^m \not\equiv 1 \pmod{N}$ pour au moins la moitié des éléments x de $(\mathbb{Z}/N\mathbb{Z})^\times$.
3. En déduire un algorithme probabiliste

   `booleen BonExposant(entiers m,N,k)`

   qui recevant les entiers m, N **produit de deux premiers**, et k, renvoie vrai ou faux. Quand il renvoie faux, m n'est pas un bon exposant modulo N . Sachant que m n'est pas un bon exposant, la probabilité qu'il renvoie vrai est inférieure à 2^{-k}.

Partie II Dans cette partie m est un bon exposant modulo N. L'objet de cette partie est l'élaboration d'un algorithme probabiliste, qui factorise N à partir de la donnée du couple (N, m).

1. Montrer que m est un entier pair. Si $m/2$ est encore un bon exposant modulo N, expliquer comment construire, à partir de m un autre entier pair qui est un bon exposant, mais dont la moitié n'est plus un bon exposant. A partir de cette question on supposera donc que m est un bon exposant mais pas $m/2$. Alors
   – ou bien $m/2$ est multiple de l'un des deux nombres $p-1, q-1$ et pas de l'autre.
   – ou bien $m/2$ n'est divisible ni par $p-1$, ni pas $q-1$.
2. Dans le premier cas, supposons par exemple que $m/2$ est multiple de $p-1$ et non multiple de $q-1$. Montrer que la moitié exactement des entiers x dans $(\mathbb{Z}/N\mathbb{Z})^\times$ sont tels que
$$x^{m/2} \equiv 1 \pmod{p}, \qquad x^{m/2} \equiv -1 \pmod{q}.$$
3. Dans le deuxième cas, $m/2$ non multiple de $p-1$ et non multiple de $q-1$, montrer que pour chacun des quatre couples $(\varepsilon_1, \varepsilon_2)$ de $\{-1, 1\}^2$, exactement le quart des entiers x dans $(\mathbb{Z}/N\mathbb{Z})^\times$ sont tels que
$$x^{m/2} \equiv \varepsilon_1 \pmod{p}, \qquad x^{m/2} \equiv \varepsilon_2 \pmod{q}.$$
4. Déduire des question précédentes un algorithme probabiliste
   `procedure Factorise(entiers N,m)`
   qui factorise N à partir de la donnée du couple (N, m) où m est un bon exposant modulo N. Rédiger le dans un pseudo langage de programmation raisonnable.

Partie III Soit (N, e) une clef publique pour le protocole RSA. N est le produit de 2 grands nombres premiers p et q, et e un entier premier avec $\varphi(N)$. La clef secrète correspondant à cette clef publique est le couple (N, d) avec d inverse de e modulo $\varphi(n)$.

1. Montrer que la connaissance du triplet (N, e, d) permet de factoriser N.
2. Que pouvez vous en déduire à propos de la difficulté du calcul de l'exposant de déchiffrage d à partir de la donnée de la clef publique (N, e) ?
3. Cela prouve t-il que le problème du décryptage du code RSA est aussi difficile que le problème de la factorisation ?