TD Cryptographie à Clé Publique

Quelques pré-requis mathématiques

Sebastien.Varrette@imag.fr

Exercice 1. [Algorithme d'Euclide Etendu] On demande de trouver les coefficients de bezout pour les nombres entiers suivants :
- $(a, b) = (17, 50)$
- $(a, b) = (11, 280)$
- $(a, b) = (35, 50)$

Exercice 2. [Calcul modulaire] Résoudre les équations suivantes :

1. $17x \equiv 10 \mod 50$
2. $35x \equiv 10 \mod 50$
3. $35y \equiv 11 \mod 50$

Exercice 3. [Théorème des restes chinois] Soient $(n_1, \ldots, n_k)$ k entiers premiers deux à deux et $N = \prod_{i=1}^{k} n_i$. On considère l'applications suivante :

$$\begin{array}{rccll} \Psi : & \mathbb{Z}_N & \longrightarrow & \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k} & \\ & a & \longrightarrow & (a_1, \ldots, a_k) & \forall i \in [1, k],\ a \equiv a_i \mod n_i \end{array}$$

1. Montrer que Ψ est un isomorphisme d'anneau
2. Caractériser la fonction Ψ^{-1}
   Indice : on posera $N_i = \frac{N}{n_i}$ et on remarquera que $pgcd(N_i, n_i) = 1$.
3. En déduire l'unique solution modulo N au système :

$$\begin{cases} x \equiv a_1 \mod n_1 \\ \vdots \\ x \equiv a_k \mod n_k \end{cases}$$

Exercice 4. [Application : le problème des restes chinois :-)]
Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Survient alors un naufrage et seuls 6 pirates, le trésor et le cuisinier sont sauvés. Le partage laisserait 5 pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer ce dernier s'il décide d'empoisonner le reste des pirates ?

Note : on utilisera les résultats suivants :
- $17 \times 11 \times 6 = 1122$ et $66 = 3 \times 17 + 15$
- $8 \times 66 \times 3 = 1584$ et $16 \times 102 = 1632$
- $4151 = 3 \times 1122 + 785$

Exercice 5. [Indicatrice d'Euler et inversion modulaire] On étudie ici la fonction $\varphi(n)$, introduite par Euler, et dont les propriétés sont à la base de la méthode RSA.
On pose $\varphi(1) = 1$ et pour $n > 1$, $\varphi(n)$ est le nombre d'entiers $m \in \{1, \ldots, n-1\}$ premiers avec n (i.e. $\gcd(m, n) = 1$).

1. Pour $n = p^k$ où p est premier et $k \in \mathbb{N}^*$, montrer que $\varphi(n) = \left(1 - \frac{1}{p}\right).n$.
2. Montrer que si n_1 et n_2 sont premiers entre eux : $\varphi(n_1.n_2) = \varphi(n_1).\varphi(n_2)$.
   Indication : on utilisera la fonctions Ψ du théorème des restes chinois.
3. En déduire que, dans $\mathbb{Z}/n\mathbb{Z}$, le cardinal du groupe des éléments inversibles est
   $$\varphi(n) = n.\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$
   où les p_i $(i = 1, \ldots, k)$ sont les k facteurs premiers distincts de n.
4. On rappelle[1] que dans un groupe fini commutatif $(G, \times, e)$ de cardinal c, on a $\forall x \in G \ : x^c = e$. En déduire que pour tout x inversible dans $\mathbb{Z}/n\mathbb{Z}$: $x^{\varphi(n)} = 1 \mod n$ et proposer un algorithme de calcul de l'inverse dans $\mathbb{Z}/n\mathbb{Z}$.
   Application : calculer (le plus vite possible) $22^{-1} \mod 63$ et $5^{2001} \mod 24$.
   On pourra utiliser : $22^2 \mod 63 = 43; 22^4 \mod 63 = 22$.
5. Donner trois algorithmes différents pour calculer l'inverse de y modulo $N = p_1^{\delta_1}.p_2^{\delta_2}.\ldots.p_k^{\delta_k}$, où les p_i sont des entiers premiers distincts.

[1] **Propriété** *Dans un groupe fini commutatif $(G, \times, e)$ de cardinal c, $\forall x \in G \ : x^c = e$.*
Preuve. Soit a un élément quelconque de G. Comme G est un groupe, a est inversible. Donc, l'application f_a de G dans G définie par $f_a : x \mapsto a \times x$ est une bijection. On a donc $Im(f_a) = G$; d'où $\prod_{y \in Im(f_a)} y = \prod_{x \in G} x$.
Or $\prod_{y \in Im(f_a)} y = \prod_{x \in G} a \times x = a^n \prod_{x \in G} x$ (commutativité de $\times$). Ainsi $a^n \prod_{x \in G} x = \prod_{x \in G} x$, d'où $a^n = e$.