Rappels et Compléments d'Arithmétique pour la Cryptographie

INSA CVL

28 septembre 2020

Les notions d'arithmétique suivantes vous seront utiles pour le TD 3 :

Définition 1. On dira de deux entiers a et b qu'ils sont *premiers entre eux* lorsque $\mathsf{pgcd}(a, b) = 1$

Définition 2. L'indicatrice d'Euler est la fonction $\phi : \mathbb{N}^+ \to \mathbb{N}$ qui à tout entier naturel N non nul associe le nombre d'entiers compris entre 1 et N (inclus) et premiers avec N. En particulier, pour n'importe quelle paire de nombres premiers (p, q), on aura $\phi(pq) = (p-1)(q-1)$.

Théorème 1. *(de Bézout).* deux entiers a et b sont *premiers entre eux* si et seulement si il existe un couple $(u, v) \in \mathbb{Z}$ tel que $au + bv = 1$.

Théorème 2. *(de Fermat).* Si p est premier, alors pour tout entier a non divisible par p, on a $a^{p-1} \equiv 1 \mod p$.

Le calcul du PGCD peut être réalisé à l'aide de l'algorithme d'Euclide :

```
fonction euclide(a, b)
    tant que (b != 0)
        tmp := b;
        b := a modulo b;
        a := tmp;
    retourner a
```

Le calcul des coefficients de Bézout (u et v tel que $au+bv = 1$) peut être réalisé à l'aide d'une généralisation de cet algorithme, qu'on appelle l'algorithme d'Euclide étendu :

```
fonction euclideEtendu(a, b)
    r := a; r' := b; u := 1; v := 0; u' := 0; v' := 1;
    tant que (r' != 0)
        q := r/r';
        rs := r; us := u; vs := v;
        r := r'; u := u'; v := v';
        r' := rs - q*r'; u' = us - q*u'; v' = vs - q*v';
    retourner (u, v)
```

Enfin, le chiffrement RSA est un système de chiffrement à clé publique défini comme suit :

Génération des clés publique et privée : Choisir deux grands nombres premiers p et q au hasard.
Poser $N = pq$ (on aura donc $\phi(N) = (p-1)(q-1)$).
Choisir un entier e au hasard tel que $0 \leq e \leq \phi(N) - 1$, et tel que e et $\phi(N)$ soient premiers entre eux (on vérifie qu'ils sont premiers entre eux avec l'algorithme d'Euclide).
Calculer d tel que $ed \equiv 1 \mod \phi(N)$ (à l'aide de l'algorithme d'Euclide étendu).
La clé secrète est d, la clé publique est (N, e).

Chiffrement de M avec la clé publique (e, N) : Calculer $C = M^e \mod N$.

Déchiffrement de C avec la clé secrète d : Calculer $M = C^d \mod N$.