R3.09 - Cryptographie et sécurité
Cours 2 - Compléments pour la cryptographie asymétrique

A. Ridard

Vannes
iut
Université Bretagne Sud

A propos de ce document

- Pour naviguer dans le document, vous pouvez utiliser :
  - le menu (en haut à gauche)
  - l'icône en dessous du logo IUT
  - les différents liens
- Pour signaler une erreur, vous pouvez envoyer un message à l'adresse suivante : anthony.ridard@univ-ubs.fr

Plan du cours

Sauf mention contraire, n désigne un entier supérieur ou égal à 1.

Propriété (théorème des restes chinois)

Soit m, n deux entiers premiers entre eux et u, v des entiers [a] tels que $um+vn=1$. Alors, pour tout entier a, b, x, on a :

$$\Big(x \equiv a \mod m \quad \text{et} \quad x \equiv b \mod n\Big) \Longleftrightarrow x \equiv avn+bum \mod mn$$

a. Ce sont les coefficients de Bézout

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Définition

La fonction φ d'Euler est définie par :

$$\varphi(n) = Card\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)$$

Comme a est inversible modulo n si et seulement si $pgcd(a,n) = 1$, $\varphi(n)$ compte le nombre d'entiers premiers avec n et compris (au sens large) entre 1 et $n-1$.

Propriété

La fonction φ d'Euler vérifie :

- $\varphi(1) = 1$
- Pour tout p premier et tout $k \geq 1$, $\varphi\left(p^k\right) = p^k - p^{k-1}$
- Pour tout m, n premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$

- Si p est premier, alors $\varphi(p) = p - 1$
- Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, alors $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$

Démontrer cette propriété.

Propriété (théorème d'Euler)

Si a est un entier premier avec n, alors $a^{\varphi(n)} \equiv 1 \mod n$.

- Lorsque $n = p$ avec p premier, on a tout simplement [a] :
  Si a est un entier, alors $a^{p-1} \equiv 1 \mod p$
- Lorsque $n = pq$ avec p, q premiers, cela devient [b] :
  Si a est un entier premier avec n, alors $a^{(p-1)(q-1)} \equiv 1 \mod n$

---

a. Il s'agit du *petit théorème de Fermat* qui est à la source d'un test de non-primalité

b. Ce cas particulier est utilisé pour le déchiffrement RSA

Démontrer ce théorème.

Vérifier le petit théorème de Fermat pour $n = 7$.

Calcul d'une puissance modulo n à l'aide du petit théorème de Fermat

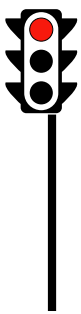
1. Montrer que $153^{100} \equiv 23 \mod 29$.
2. Montrer que $17^{1717} \equiv 7 \mod 10$.

Calcul d'une puissance modulo n par exponentiation rapide

1. Décomposer [a] 11 en base 2 puis montrer que $5^{11} \equiv 3 \mod 14$.
2. Décomposer 154 en base 2 puis montrer que $17^{154} \equiv 29 \mod 100$.

---

a. La méthode la plus efficace pour convertir un entier en base p est la méthode du bit de poids faible qui consiste à calculer le dernier chiffre de la représentation du nombre en base p par une division euclidienne.



L'objectif de cette partie est de présenter le lemme du déchiffrement RSA et de proposer un exercice détaillé, faisable à la main, pour bien comprendre les étapes de chiffrement et déchiffrement.
Des informations complémentaires seront fournies dans le TP4...

Propriété (lemme du déchiffrement RSA)

Soit d l'inverse de e modulo $\varphi(n)$.
Si $c \equiv m^e \mod n$, alors $m \equiv c^d \mod n$.

Démontrer [a] ce lemme.

---

a. Par une disjonction de cas :

- 1er cas : $pgcd(m,n) = 1$
  Il suffit d'utiliser le théorème d'Euler
- 2e cas (EXPERT) : $pgcd(m,n) \neq 1$
  On pourra supposer, sans perdre de généralité, $pgcd(m,n) = p$ et $pgcd(m,q) = 1$.
  On montrera $(m^e)^d \equiv m \mod p$ et $(m^e)^d \equiv m \mod q$.
  On conclura en utilisant le lemme de Gauss !

RSA

Alice souhaite envoyer le message $m = 10$ à Bob qui a défini sa clé $\left(k_B^{pub}, k_B^{priv}\right)$ de la manière suivante :

- il a choisi deux nombres premiers[a] distincts : $p = 5$ et $q = 17$
- il a calculé $n = pq = 85$ et $\varphi(n) = (p-1)(q-1) = 64$
- il a choisi un entier $e = 5$ premier avec $\varphi(n)$
- il a calculé l'inverse d de e modulo $\varphi(n)$
- il a ainsi obtenu :

$$k_B^{pub} = (n, e) \quad \text{et} \quad k_B^{priv} = (n, d)$$

a. Dans la pratique, ce sont de très grands nombres d'une centaine de chiffres

RSA (suite)

1. Déterminer d.
2. Alice utilise la fonction de chiffrement définie par :

$$E_{k_B^{pub}}(m) = m^e \mod n$$

   Calculer le chiffré c reçu par Bob.
3. Bob utilise la fonction de déchiffrement définie par :

$$D_{k_B^{priv}}(c) = c^d \mod n$$

   Retrouver le message m envoyé par Alice.