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

L. Naert, T. Godin, T. Ferragut

Merci à A. Ridard pour ce cours !

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

1. Théorème d'Euler
2. Cryptographie asymétrique et RSA

1 Théorème d'Euler

2 Cryptographie asymétrique et RSA

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

Propriété (théorème des restes chinois)

Soit m_1, m_2, ..., m_k, des entiers deux à deux premiers entre eux.
Alors, pour tous entiers a_1, a_2, ..., a_k, le système d'équations :

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \dots \\ x \equiv a_k \mod m_k \end{cases}$$

admet une solution x unique modulo $M = m_1 m_2 ... m_k$ donnée par :

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_k M_k y_k$$

où $M_i = \frac{M}{m_i}$ et $y_i \equiv M_i^{-1} \mod m_i$ pour i entre 1 et k.

Le problème de Sun Zi

Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?

Le problème des pirates

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. 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

L'indicatrice 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 $n-1$.
- Si p est premier, alors $\varphi(p) = p-1$

Donner $\varphi(26)$ et $\varphi(17)$.

Propriétés

L'indicatrice d'Euler vérifie :

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

En utilisant les propriétés, donner $\varphi(25)$, $\varphi(49)$, $\varphi(64)$ et $\varphi(60)$

Démontrer les propriétés (1) et (2).

Avec ces propriétés, il est possible de trouver l'indicatrice d'Euler de n'importe quel nombre ... **à condition de trouver sa décomposition en facteurs premiers !**.

Par exemple :

- $\varphi(240) = \varphi(2^4 \times 3 \times 5) = \varphi(2^4) \times \varphi(3) \times \varphi(5) = (2^4 - 2^3) \times 2 \times 4 = 8 \times 2 \times 4 = 64$
- mais $\varphi(221)$?
- ou $\varphi(33741)$?

La décomposition en facteurs premiers n'est pas si évidente et le chiffrement RSA se base sur cette difficulté !

Propriété (théorème d'Euler)

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

- **Petit théorème de Fermat** : Lorsque $n = p$ avec p premier, le théorème d'Euler donne :
  Si a est un entier premier avec p, alors $a^{p-1} \equiv 1 \mod p$
- **Cas particulier utilisé pour le déchiffrement RSA** : Lorsque $n = pq$ avec p, q premiers, cela devient :
  Si a est un entier premier avec n, alors $a^{(p-1)(q-1)} \equiv 1 \mod n$

Vérifier le petit théorème de Fermat pour $n = 5$.

Calcul d'une puissance modulo n à l'aide du théorème d'Euler

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

Exponentiation rapide

L'exponentation rapide est une technique utilisée pour calculer rapidement de grandes puissances de nombres entiers. Elle est particulièrement utile pour l'exponentiation modulaire dans laquelle les nombres manipulés reste limités par le modulo. Étant donné les entiers a et e, et l'entier non nul m, cette technique vise donc à calculer b dans l'expression suivante :
$a^e \equiv b \mod m$

Description de la méthode :

Tout d'abord, il s'agit de donner la décomposition binaire de e : $e = \sum_{i=0}^{n-1} c_i 2^i$ avec n la longueur de e en bits, et $c_i = 0$ ou 1 pour tout i compris entre 0 et $n-1$.

Ainsi, a^e peut s'écrire comme le produit des a^{2^i} pour les c_i non nuls.

Il suffit donc ensuite de réaliser les carrés successifs de a (modulo m) puis de faire le produit (modulo m) pour obtenir b.

Exemple : Calculons b dans que $7^{18} \equiv b \mod 10$

1. Décomposition binaire de l'exposant : $18 = 16 + 2 = 2^4 + 2^1$
2. On a donc $7^{18} = 7^{2^4} \times 7^{2^1}$
3. Calcul des carrés successifs modulo 10 :
   $7^{2^1} \equiv 7^2 \equiv 49 \equiv 9 \mod 10$
   $7^{2^2} \equiv 9^2 \equiv 81 \equiv 1 \mod 10$
   $7^{2^3} \equiv 1^2 \equiv 1 \equiv 1 \mod 10$
   $7^{2^4} \equiv 1^2 \equiv 1 \equiv 1 \mod 10$
4. Produit et conclusion :

$$\begin{aligned} 7^{18} &\equiv 7^{2^4} \times 7^{2^1} \mod 10 \\ &\equiv 1 \times 9 \mod 10 \\ &\equiv 9 \mod 10 \end{aligned}$$

Refaire le même exemple en utilisant le théorème d'Euler.

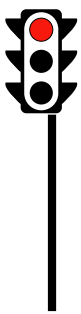
Vannes
IUT
Université Bretagne Sud

Calcul d'une puissance modulo n par exponentiation rapide

1. Décomposer 11 en base 2 puis montrer que $5^{11} \equiv 3 \mod 14$.
2. Décomposer 154 en base 2 puis montrer que $3^{154} \equiv 4 \mod 5$.

1 Théorème d'Euler

2 Cryptographie asymétrique et RSA



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...

Principe de la cryptographie asymétrique

Les interlocuteurs possèdent chacun une clef composée d'une partie publique connue de tous et d'une partie privée connue uniquement du propriétaire de la clef :

- clef d'Alice : $k_A = (k_A^{pub}, k_A^{priv})$
- clef de Bob : $k_B = (k_B^{pub}, k_B^{priv})$

Chiffrement du message
La fonction de chiffrement E est paramétrée par la partie **publique** de la clef du destinataire :

- Si Alice souhaite envoyer un message à Bob, elle chiffre son message m en utilisant la partie publique de la clef de Bob : $c = E_{k_B^{pub}}(m)$

Déchiffrement du message
La fonction de déchiffrement D est paramétrée par la partie **privée** de la clef du destinataire :

- Bob déchiffrera le message c en utilisant la partie privée de sa clef : $m = D_{k_B^{priv}}(c)$

Vannes iut Université Bretagne Sud

Pour que ce système fonctionne, il faut que la partie publique et la partie privée de la clef permettent de définir des opérations E et D réciproques ($D_{k^{priv}} = E^{-1}_{k^{pub}}$) et que le calcul de la clef privée de quelqu'un connaissant sa clef publique soit infaisable dans des temps raisonnables.

Ce principe de la cryptographie asymétrique a été formalisé par Diffie et Hellmann en 1976 mais aucune solution concrète n'avait été proposée à ce moment. Il a fallu attendre le chiffrement **RSA**, proposé par Rivest, Shamir et Adleman un an plus tard pour pouvoir implémenter le chiffrement asymétrique.

Principe du chiffrement RSA

RSA propose une application concrète du principe du chiffrement asymétrique en se basant sur la difficulté à factoriser des entiers de grande taille.

Une clef RSA $k = (k^{pub}, k^{priv})$ est définie à partie des paramètres suivants :

- p et q sont deux grands nombres premiers distincts
- $n = pq$
- e et d sont des entiers tels que $ed \equiv 1 \mod \varphi(n)$ $(d \equiv e^{-1} \mod \varphi(n))$

Alors $k^{pub} = (n, e)$ et $k^{priv} = (n, d)$

Propriété (lemme du déchiffrement RSA)

Soit $n = pq$, le produit de deux nombres premiers distincts.
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** : $pgcd(m,n) = 1$
  En utilisant le théorème d'Euler
- **2e cas** : $pgcd(m,n) \neq 1$ (plus difficile !)
  En utilisant le lemme de Gauss

RSA

Alice souhaite envoyer le message $m = 10$ à Bob.
Ce dernier, pour définir sa clef $\left(k_B^{pub}, k_B^{priv}\right)$ a choisi deux nombres premiers [a] distincts : $p = 5$ et $q = 17$

1. Déterminer n et $\varphi(n)$.

Bob a ensuite choisi un entier $e = 5$ premier avec $\varphi(n)$

2. Déterminer k_B^{pub} et k_B^{priv}

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

RSA (suite)

3. Alice utilise la fonction de chiffrement définie par :

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

   Calculer le chiffré c reçu par Bob.

4. Bob utilise la fonction de déchiffrement définie par :

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

   Retrouver le message m envoyé par Alice.