Eléments mathématiques pour la cryptographie à clé publique

Troisième séance

Venir avec des calculatrices si possible

0. Rappel $(R_n, \odot)$

Définition 1.

Soit un entier n, on désigne par R_n ***l'ensemble des éléments inversibles de l'anneau*** $(Z/nZ, \oplus, \odot)$

Théorème 2. ***Soit un entier*** $n>1$

1. $(R_n, \odot)$ ***est un groupe de cardinal*** $\varphi(n)$

2. $\forall \bar{a} \in R_n, \bar{a}^{\varphi(n)} = \bar{1}$ ***(théorème d'Euler)***

3. Si p est premier, $\forall \bar{a} \in R_p, \bar{a}^{p-1} = \bar{1}$ ***; c'est à dire Si p est premier,*** $\forall a, a \wedge p = 1 \Longrightarrow a^{p-1} \equiv 1[p]$(th de Fermat)**.**

Théorème 3.

Soit un entier premier p

1. $\forall \bar{a} \in R_p, \bar{a}^{p-1} = \bar{1}$ ***; c'est à dire Si p est premier,*** $\forall a, a \wedge p = 1 \Longrightarrow a^{p-1} \equiv 1[p]$(th de Fermat)**.**

Mieux encore

2. Le groupe $(R_p, \odot)$ ***est cyclique.***

1. Cryptographie à clé publique, RSA

l'objectif est de réaliser le schéma suivant

- Texte clair M $\xrightarrow[\mathcal{E}_K]{\text{chiffrement}}$ Texte crypté $M' = \mathcal{E}_K(M)$ $\xrightarrow[\mathcal{D}_{K'}]{\text{déchiffrement}}$ $\mathcal{D}_{K'}(M') = \mathcal{D}_{K'} \circ \mathcal{E}_K(M) = M$

Il existe des systèmes de cryptage à « clé secrète » (ou systèmes symétriques) dans lesquels l'algorithme de chiffrement et l'algorithme de déchiffrement sont facilement dérivées l'un de l'autre; par suite celui qui connait l'un connait l'autre, ce qui impose d'une part de conserver le secret, d'autre part de commmuniquer (avec prudence) entre l'émetteur et le destinataire, qui ont besoin de partager le secret de la méthode.

Depuis quelques dizaines d'années existent des systèmes de cryptage à « clé publique », dans lesquels il n'est besoin d'aucune communication privée entre l'émetteur et le destinataire, parce qu'il n ' y a plus de symétrie, la connaissance de l'algorithme de chiffrement ne permet en aucun cas de connaître l'algorithme de déchiffrement.

C'est le cas de l'algorithme RSA (bien connu mais ce n'est pas le seul). 1978

1.1 l'idée c'est Euler + Bezout...

Soit un entier n>1 et $\varphi(n)$ **le cardinal du groupe** $(R_n, \odot)$ **alors** $\forall \bar{a} \in R_n, \bar{a}^{\varphi(n)} = \bar{1}$**; si on considère un entier e, premier avec** $\varphi(n)$ **alors on sait trouver deux entiers relatifs (u,d) tels que** $u\varphi(n) + \mathrm{de} = 1$

alors $\bar{a}^{u\varphi(n)+\mathrm{de}} = \bar{a}^{1} = \bar{a}$**, mais par ailleurs** $\bar{a}^{u\varphi(n)+\mathrm{de}} = \bar{a}^{u\varphi(n)}\bar{a}^{\mathrm{de}} = \bar{1}\,\bar{a}^{\mathrm{de}} = \bar{a}^{\mathrm{de}}$**;**

en conclusion, $\bar{a}^{\mathrm{de}} = \bar{a}$**.**

Supposons que le message à coder soit: $\bar{a}$

l'émetteur le chiffre comme suit: $\bar{a} \longrightarrow \bar{b} = \bar{a}^{e}$**; c'est à dire il envoie** $\bar{b}$

le destinataire reçoit $\bar{b}$ **et, pour déchiffrer, il opère comme suit:** $\bar{b} \longrightarrow \bar{b}^{d}$ **qui vaut** $(\bar{a}^{e})^{d} = \bar{a}^{\mathrm{de}} = \bar{a}$**.**

donc

on chiffre en élevant à la puissance e, on déchiffre en élevant à la puissance d.

1.2 Mais qui sait quoi ?

1. **L'émetteur sait qu'on calcule modulo n et qu'il élève à la puissance e.**

Il n'a pas besoin de connaître ni $\varphi(n)$**, ni d.**

2. **Le destinataire a besoin de savoir qu'on calcule modulo n et de connaître d et, bien sûr, d doit être secret, sinon toute personne qui met la main sur le message crypté (qui vaut b) pourrait le déchiffrer.**

3. **Donc le destinataire doit être le seul à connaître d, tandis que le même e peut être utilisé et connu par tout le monde.**

4. **Comment faire ?**

En fait le chef d'orchestre c'est le destinataire; il dit en public

« toute personne qui veut m'écrire, on se placera modulo n, et vous élèverez le message $\bar{a}$ **à la puissance e ».**

5. Comment faire pour que, même si tout le monde connaît n et e, il leur soit difficile de trouver tous seuls d ?

Il faut que la connaissance de n ne permette pas facilement de trouver $\varphi(n)$; or, dès qu'est connue la factorisation de n en produit de puissances de premiers, on est en en mesure de trouver $\varphi(n)$.

Donc la clé c'est n. Comment rendre difficile de trouver sa factorisation ?

6. Pour que la recherche des diviseurs de n soit difficile il faut qu'ils soient grands; on prendra n=pq, deux facteurs premiers tous les deux grands, plus ou moins proches.

1.3 Cryptage et authentification

Soient donc Alice et Bob.

Supposons que Alice a publié son n, noté n_A et l'entier e_A qu'elle a choisi premier avec $\varphi(n_A)$ qu'elle seule connaît; Alice a déterminé d_A mais ne le rend surtout pas public.

De même Bob a publié son n, noté n_B et l'entier e_B qu'il a choisi premier avec $\varphi(n_B)$; Bob a déterminé d_B, mais ne le rend surtout pas public.

1.3.A

Si Bob veut envoyer le message x à Alice, où $x \wedge n_A = 1$, il envoie $\bar{x'} = \bar{x}^{\,e_A}$ et Alice calcule $\bar{x'}^{d_A}$ ce qui lui donne $\bar{x}$.

1.3.B

Si Alice veut envoyer le message y à Bob, où $y \wedge n_B = 1$, elle envoie $\bar{y'} = \bar{y}^{\,e_B}$ et Bob calcule $\bar{y'}^{d_B}$ ce qui lui donne $\bar{y}$.

1.3.AA Et si Bob veut prouver à Alice qu'il est bien Bob

Soit la signature bob de Bob, Bob envoie à Alice le message $\bar{z'} = \overline{\text{bob}}^{d_B e_A}$, elle l'élève à la puissance $d_A e_B$; si Bob est Bob alors le message qu'elle a déchiffré est la signature de Bob, sinon elle n'obtient pas la signature de Bob.

1.3. BB De même si Alice veut prouver à Bob qu'elle est bien Alice

Soit la signature ali d'Alice, Alice envoie à Bob le message $\overline{w'} = \overline{\text{ali}}^{d_A e_B}$, il l'élève à la puissance $d_B e_A$; si Alice est Alice alors le message qu'il a déchiffré est la signature d'Alice, sinon il n'obtient pas la signature d'Alice.

Exercice 1. Un message simple

Alice attend un message de Bob; elle chosit n_A=55 et déclare que $e_A = 3$

1. Bob veut lui envoyer le message 7, que doit-il lui envoyer ?

(réponse 13)

2. Si Alice reçoit le message crypté 13, que doit-elle faire pour le décrypter ?

(réponse élever à la puissance 27, dans $\mathbb{Z}/55\mathbb{Z}$)

Exercice 2. Toujours dans $\mathbb{Z}/55\mathbb{Z}$

1. Alice reçoit le message crypté 12, décryptez-le

2. Caroline se joint à ce groupe elle conserve n_C=55 et déclare que $e_C = 9$

Bob lui envoie le message crypté 31, décryptez-le pour Caroline

2. Un outil utile : l'exponentiation rapide

Vous venez de constater que le cryptage comme le décryptage conduisent facilement à de grandes exponentiations, voici une méthode qui permet 1) d'aller plus vite 2) d'éviter des nombres inutilement grands.

Théorème 4. ***Ecriture binaire d'un entier***

Tout entier m>0 se décompose sous la forme $\mathbf{m}=m_0+2m_1+2^2m_2+....+2^pm_p$

où $\mathbf{m}_p=1$ ***et*** $(m_0,m_1,m_2,....,m_{p-1})\in\{0,1\}^p$

(nb p est Log$_2$***(m))***

on écrira $\mathbf{m}=\overline{m_pm_{p-1}....m_2m_1m_0}$

Exemple 5. $\mathbf{52}=\mathbf{2}^2+\mathbf{2}^4+\mathbf{2}^5=\overline{11010}$

Théorème 6. ***Exponentiation rapide***

Soit $\mathbf{m}=m_pm_{p-1}....m_2m_1m_0$ ***(comme au-dessus) et a un nombre (réel, entier ou modulo n, peu importe)***

Pour calculer a^m

1) On calcule successivement a^2 **,** $\mathbf{a}^4$ (qui vaut $(a^2)^2$)**,** $\mathbf{a}^8$ (qui vaut $(a^4)^2$)**, etc... ,** $\mathbf{a}^{2^p}$ $\left(\text{qui vaut } \left(a^{2^{p-1}}\right)^2\right)$ ***(donc chaque fois ce sont des élévations toutes simples au carré)***

2) On multiplie $a^m=\prod_{k,m_k=1}\mathbf{a}^{2^k}$

Exemple 7. Calcul de $\bar{7}^{52}$ **dans** $\mathbb{Z}/13\mathbb{Z}$

Comme $\mathbf{52}=\mathbf{2}^2+\mathbf{2}^4+\mathbf{2}^5$

On calcule $\bar{7}^2=\bar{10}$, $\bar{7}^4=(\bar{10})^2=\bar{9}$, $\bar{7}^8=(\bar{9})^2=\bar{6}$, $\bar{7}^{16}=(\bar{6})^2=\bar{10}$, $\bar{7}^{32}=(\bar{10})^2=\bar{9}$

D'où $\bar{7}^{52}=\bar{9}\odot\bar{10}\odot\bar{9}=(\bar{9}\odot\bar{10})\odot\bar{9}=\bar{12}\odot\bar{9}=\bar{4}$**.**

Problème 1.

Calcul de $\bar{8}^{67}$ **dans** $\mathbb{Z}/11\mathbb{Z}$

Problème 2. Alice attend un message de Bob; elle choisit $\mathbf{n}_A$**=14 et déclare que** $e_A=5$

1. Bob veut lui envoyer le message 6, que doit-il lui envoyer ?

2. Si Alice reçoit le message crypté 13, quel était le message ?

Travaux Dirigés

Exercice 3. Exponentiation rapide

a. Soit n=323

Vérifer que le calcul de 201^{99} pose un problème technique

Proposer une méthode de calcul de 201^{99} mod(323)

b. Ecrire 99 en base 2

Montrer qu'au moyen de calculs succesifs de carrés on peut trouver rapidement 201^{64} mod(323)

Exploiter l'écriture de 99 en base 2 pour trouver une méthode de calcul rapide et réaliste de 201^{99} mod(323)

Exercice 4.

i. Factoriser 323 en produit de facteurs premiers

ii. Déterminer la valeur de $\varphi(323)$

iii. Déterminer (u,v) dans Z tels que 288u+227v=1

iv. Calculer a=$2^{227} \bmod (323)$

Si nécessaire appliquer l'algorithme d'exponentiation rapide

v. Vérifer que $a^v = 2 \bmod (323)$

Exercice 5. Simuler le cryptage et le décryptage d'un message numérique

n=323

e=49

i. Déterminer la clé d de décryptage

ii. Crypter le message « 11 »

iii. Décrypter le message et vérifier que vous retrouvez « 11 »

Exercice 6. avec Maxima

n=12743417, e=15997

1. Crypter le message x=2160

2. Décrypter le message y=34571