CRYPTANALYSE DE RSA

Abderrahmane NITAJ

Université de Caen, France

Oujda, 20-21 mai 2009

وَجدَة، المَغرِب

عبدالرحمان نتاج

CONTENU

CONTENU

Le cryptosystème RSA

- Rivest, Shamir, Adleman (1977).
- Le cryptosystème le plus utilisé dans le monde.
- Sa sécurité est basée sur le problème de la factorisation.

La factorisation

- $77 = 7 \times 11$.
- $15629010403 = ?$
- Etant donné $N = pq$, comment trouver p et q rapidement ?
- Problème difficile si p et q sont grands...

Le cryptosystème RSA

- Rivest, Shamir, Adleman (1977).
- Le cryptosystème le plus utilisé dans le monde.
- Sa sécurité est basée sur le problème de la factorisation.

La factorisation

- $77 = 7 \times 11$.
- $1562900109403 = ? \times ?$
- Etant donné $N = pq$, comment trouver p et q ou calculer $(p-1)(q-1)$.
- Problème difficile si p et q sont grands.

Le cryptosystème RSA

- Rivest, Shamir, Adleman (1977).
- Le cryptosystème le plus utilisé dans le monde.
- Sa sécurité est basée sur le problème de la factorisation.

La factorisation

- $77 = 7 \times 11$.
- $1562900109403 = ? \times ?$
- Etant donné $N = pq$, comment trouver p et q ou calculer $(p-1)(q-1)$.
- Problème difficile si p et q sont grands.

Le cryptosystème RSA

- Rivest, Shamir, Adleman (1977).
- Le cryptosystème le plus utilisé dans le monde.
- Sa sécurité est basée sur le problème de la factorisation.

La factorisation

- $77 = 7 \times 11$.
- $1562900109403 = ? \times ?$
- Etant donné $N = pq$, comment trouver p et q ou calculer $(p-1)(q-1)$.
- Problème difficile si p et q sont grands.

Le cryptosystème RSA

- Rivest, Shamir, Adleman (1977).
- Le cryptosystème le plus utilisé dans le monde.
- Sa sécurité est basée sur le problème de la factorisation.

La factorisation

- $77 = 7 \times 11$.
- $1562900109403 = ? \times ?$
- Etant donné $N = pq$, comment trouver p et q ou calculer $(p-1)(q-1)$.
- Problème difficile si p et q sont grands.

Le cryptosystème RSA

- Rivest, Shamir, Adleman (1977).
- Le cryptosystème le plus utilisé dans le monde.
- Sa sécurité est basée sur le problème de la factorisation.

La factorisation

- $77 = 7 \times 11$.
- $1562900109403 = ? \times ?$
- Etant donné $N = pq$, comment trouver p et q ou calculer $(p-1)(q-1)$.
- Problème difficile si p et q sont grands.

Principe de RSA

BUT

Une pesronne **A** veut envoyer un message M à une personne **B** en utilisant le cryptosystème RSA.

Principe de RSA

Préparations du destinataire B

- Choisir deux nombres premiers p et q assez grand.
- Calculer $N = pq$.
- Calculer $\phi(N) = (p-1)(q-1)$.
- Choisir une entier $e \in \mathbb{N}$, $1 < e < \phi(N)$ tel que $\text{pgcd}(e, \phi(N)) = 1$.
- Calculer $d \in \mathbb{N}$, $1 < d < \phi(N)$, $ed \equiv 1 \pmod{\phi(N)}$.
- Publier la clé publique (N, e).
- Garder la clé secrète (N, d).

Principe de RSA

Chiffrement par l'expéditeur A

- Prendre la clé publique (N, e) de **B**.
- Transformer le message en un nombre entier M de l'intervalle $[2, N]$.
- Calculer $C \equiv M^e \pmod{N}$.
- Envoyer le message C à **B**.

Principe de RSA

Déchiffrement par le destinataire B

- Prendre la clé privée (N, d).
- Calculer $M \equiv C^d \pmod{N}$.

Preuve.

Puisque $ed \equiv 1 \pmod{\phi(N)}$, alors $ed = 1 + k\phi(N)$. Donc

$$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\phi(N)} \equiv M\left(M^{\phi(N)}\right)^k \equiv M \pmod{N}.$$

□

Principe de RSA

Déchiffrement par le destinataire B

- Prendre la clé privée (N, d).
- Calculer $M \equiv C^d \pmod{N}$.

Preuve.

Puisque $ed \equiv 1 \pmod{\phi(N)}$, alors $ed = 1 + k\phi(N)$. Donc

$$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\phi(N)} \equiv M\left(M^{\phi(N)}\right)^k \equiv M \pmod{N}.$$

□

Principe de RSA

L'indicateur d'Euler

- $\phi(N) = \#\{a \mid 0 \leq a \leq N-1,\ \text{pgcd}(a,N) = 1\}$
- $\phi(p) = p-1$, si p est premier.
- $\phi(pq) = (p-1)(q-1)$, si p et q sont premiers et $p \neq q$.
- $$\phi\left(\prod_{i=1}^{s} p_i^{n_i}\right) = \prod_{i=1}^{s} p_i^{n_i-1}(p_i-1).$$

Theorem (Euler)

Si pgcd$(a,N) = 1$ alors

$$a^{\phi(N)} \equiv 1 \pmod{N}.$$

Principe de RSA

L'indicateur d'Euler

- $\phi(N) = \#\{a \mid 0 \leq a \leq N-1,\ \text{pgcd}(a,N) = 1\}$
- $\phi(p) = p - 1$, si p est premier.
- $\phi(pq) = (p-1)(q-1)$, si p et q sont premiers et $p \neq q$.
- $$\phi\left(\prod_{i=1}^{s} p_i^{n_i}\right) = \prod_{i=1}^{s} p_i^{n_i-1}(p_i - 1).$$

Theorem (Euler)

Si $\text{pgcd}(a,N) = 1$ *alors*

$$a^{\phi(N)} \equiv 1 \pmod{N}.$$

Principe de RSA

preuve.

$$\begin{aligned} & \{a \mid 0 \leq a < N,\ \text{pgcd}(a, N) = 1\} \\ = & \left\{a_1, a_2, \cdots, a_{\phi(N)},\ a_1 < a_2 < \cdots < a_{\phi(N)} < N\right\} \\ = & \left\{\overline{aa_1}, \overline{aa_2}, \cdots, \overline{aa_{\phi(N)}}\right\}. \end{aligned}$$

En formant les produits

$$\prod_{i=1}^{\phi(N)} a_i = \prod_{i=1}^{\phi(N)} \overline{aa_i} \equiv a^{\phi(N)} \prod_{i=1}^{\phi(N)} a_i \pmod{N}.$$

En simplifiant, on obtient $a^{\phi(N)} \equiv 1 \pmod{N}$. □

Cryptanalyses élémentaires

Cryptanalyse de RSA connaissant $\phi(N)$

Proposition (1)

Soit $N = pq$. Si on connait $\phi(N)$, alors on peut factoriser N.

preuve.

Si

$$\begin{cases} pq = N, \\ p + q = N + 1 - \phi(N), \end{cases}$$

alors $p^2 - (N + 1 - \phi(N))p + N = 0$, et on peut calculer p.

□

Cryptanalyses élémentaires

Cryptanalyse de RSA connaissant $\phi(N)$

Proposition (1)

Soit $N = pq$. Si on connait $\phi(N)$, alors on peut factoriser N.

preuve.

Si

$$\begin{cases} pq & = N, \\ p+q & = N+1-\phi(N), \end{cases}$$

alors $p^2 - (N+1-\phi(N))p + N = 0$, et on peut calculer p.

Cryptanalyses élémentaires

Utilisation du même module et deux exposants différents

Proposition (2)

Si un message clair M est chiffré avec (N, e_1) et (N, e_2) avec pgcd$(e_1, e_2) = 1$, alors on peut calculer M.

preuve.

Si pgcd$(e_1, e_2) = 1$, alors $e_1 x_1 - e_2 x_2 = 1$. Supposons

$$\begin{aligned} C_1 &\equiv M^{e_1} \pmod N, \\ C_2 &\equiv M^{e_2} \pmod N, \end{aligned}$$

Alors $C_1^{x_1} C_2^{-x_2} \equiv M^{e_1 x_1} M^{-e_2 x_2} \equiv M^{e_1 x_1 - e_2 x_2} \equiv M \pmod N$, □

Cryptanalyses élémentaires

Utilisation du même module et deux exposants différents

Proposition (2)

Si un message clair M est chiffré avec (N, e_1) et (N, e_2) avec pgcd$(e_1, e_2) = 1$, alors on peut calculer M.

preuve.

Si pgcd$(e_1, e_2) = 1$, alors $e_1 x_1 - e_2 x_2 = 1$. Supposons

$$\begin{aligned} C_1 &\equiv M^{e_1} \pmod N, \\ C_2 &\equiv M^{e_2} \pmod N, \end{aligned}$$

Alors $C_1^{x_1} C_2^{-x_2} \equiv M^{e_1 x_1} M^{-e_2 x_2} \equiv M^{e_1 x_1 - e_2 x_2} \equiv M \pmod N$, □

Cryptanalyses élémentaires

Utilisation de modules différentes pour le même message

Proposition (3)

Soient $k \geq 2$ et k modules RSA N_i avec $1 \leq i \leq k$. Soient C_i, $1 \leq i \leq k$, des messages chiffrés du même message clair M à l'aide du même exposant e. Si

$$M^e < N = \prod_{i=1}^{k} N_i$$

alors on peut déterminer le message clair M sans factoriser les modules.

Cryptanalyses élémentaires

Utilisation de modules différentes pour le même message

preuve.

On applique le Théorème des Restes Chinois pour résoudre le système formé des k équations

$$x \equiv C_i \pmod{N_i},$$

avec $x < N$. Si on suppose que $M^e < N$, alors $x = M^e$ en tant que nombres entiers. Ainsi

$$M = x^{\frac{1}{e}},$$

Cryptanalyses élémentaires

Utilisation de modules différentes pour le même message

preuve.

On applique le Théorème des Restes Chinois pour résoudre le système formé des k équations

$$x \equiv C_i \pmod{N_i},$$

avec $x < N$. Si on suppose que $M^e < N$, alors $x = M^e$ en tant que nombres entiers. Ainsi

$$M = x^{\frac{1}{e}},$$

□

Cryptanalyses élémentaires

Théorème (Chinois)

Si les entiers $N_1, N_1, \cdots, N_k$ sont deux à deux premiers entre eux, alors le système

$$\begin{cases} x = a_1 \pmod{N_1}, \\ x = a_1 \pmod{N_1}, \\ \vdots = \quad \vdots \\ x = a_k \pmod{N_k}, \end{cases}$$

admet une solution unique modulo $N = \prod_{i=1}^{k} N_i$. Cette solution est

$$x \equiv \sum_{i=1}^{k} a_i p_i M_i \pmod{N},$$

avec $p_i = \frac{N}{N_i}$ et $M_i \equiv p_i^{-1} \pmod{N_i}$.

Cryptanalyses élémentaires

Cryptanalyse de RSA si $|p-q| < cN^{1/4}$: Méthode de Fermat

Proposition (4)

Si $N = pq$ avec $|p-q| < cN^{1/4}$, alors alors on peut factoriser N.

preuve.

On écrivant

$$4N = 4pq = x^2 - y^2 = (x+y)(x-y), \quad p = \frac{x+y}{2},$$

on peut tester si les valeurs $x_k = \left[2\sqrt{N}\right] + k$ vérifient $x_k^2 - 4N = y^2$. On peut montrer alors que si $|p-q| < cN^{1/4}$, alors $k < \frac{c^2}{2} + 1$. □

Cryptanalyses élémentaires

Cryptanalyse de RSA si $|p-q| < cN^{1/4}$: Méthode de Fermat

Proposition (4)

Si $N = pq$ avec $|p-q| < cN^{1/4}$, alors alors on peut factoriser N.

preuve.

On écrivant

$$4N = 4pq = x^2 - y^2 = (x+y)(x-y), \quad p = \frac{x+y}{2},$$

on peut tester si les valeurs $x_k = \left[2\sqrt{N}\right] + k$ vérifient $x_k^2 - 4N = y^2$. On peut montrer alors que si $|p-q| < cN^{1/4}$, alors $k < \frac{c^2}{2} + 1$. □

CONTENU

L'algorithme des fraction continues

Théorème

Tout nombre réel positif x a une écriture unique comme fraction continue :

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} = [a_0, a_1, a_2, \cdots],$$

où les a_i sont des entiers positifs. De plus, la fraction continue est finie si et seulement si le nombre x est rationnel.

Les nombres entiers a_i s'appellent les quotients partiels.

L'algorithme des fraction continues

Théorème

Tout nombre réel positif x a une écriture unique comme fraction continue :

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} = [a_0, a_1, a_2, \cdots],$$

où les a_i sont des entiers positifs. De plus, la fraction continue est finie si et seulement si le nombre x est rationnel.

Les nombres entiers a_i s'appellent les quotients partiels.

Les fractions continues

Les nombres $[a_0, a_1, a_2, \cdots, a_k]$ s'appellent les réduites de x.

Proposition

Soit $[a_0, a_1, a_2, \cdots]$ la fraction continue de x. Pour tout $n \geq 0$, on définit les nombres p_n et q_n par,

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}, \end{aligned}$$

avec la convention

$$p_{-2} = 0, \quad q_{-2} = 1, \quad p_{-1} = 1, \quad q_{-1} = 0.$$

Alors tout $n \geq 0$, on a $\frac{p_n}{q_n} = [a_0, a_1, a_2, \cdots, a_n]$.

Les fractions continues

Les nombres $[a_0, a_1, a_2, \cdots, a_k]$ s'appellent les réduites de x.

Proposition

Soit $[a_0, a_1, a_2, \cdots]$ la fraction continue de x. Pour tout $n \geq 0$, on définit les nombres p_n et q_n par,

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}, \end{aligned}$$

avec la convention

$$p_{-2} = 0, \quad q_{-2} = 1, \quad p_{-1} = 1, \quad q_{-1} = 0.$$

Alors tout $n \geq 0$, on a $\frac{p_n}{q_n} = [a_0, a_1, a_2, \cdots, a_n]$.

Les fractions continues

Proposition

Soit $[a_0, a_1, a_2, \cdots]$ *la fraction continue d'un nombre* x*. Alors les convergentes* $\frac{p_n}{q_n}$ *de* x *vérifient pour tout* $n \geq -2$

$$p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1}.$$

Les fractions continues

Proposition

Les convergentes $\frac{p_n}{q_n}$ *d'un nombre réel* x *vérifient* $pgcd(p_n, q_n) = 1$ *pour tout* $n \geq 0$.

Les fractions continues

Proposition

Si x est un nombre réel. Si $\frac{p}{q}$ est un nombre rationnel qui vérifie

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2},$$

alors $\frac{p}{q}$ est une convergente de x.

L'attaque de Wiener

Théorème

Si $N = pq$ avec $q < p < 2q$ et $e < \phi(N)$ avec $ed \equiv 1 \pmod{\phi(N)}$ et $d < \frac{1}{3}N^{\frac{1}{4}}$, alors on peut calculer d et factoriser N.

preuve.

En utilisant $ed - k\phi(N) = 1$, $p + q < 3\sqrt{N}$ et $k < d < \frac{1}{3}N^{\frac{1}{4}}$, on a

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{|ed - kN|}{Nd} = \frac{|ed - k\phi(N) - kN + k\phi(N)|}{Nd}$$
$$\leq \cdots$$
$$< \frac{1}{2d^2}.$$

Donc $\frac{k}{d}$ est une convergente de $\frac{e}{N}$. □

L'attaque de Wiener

Théorème

Si $N = pq$ *avec* $q < p < 2q$ *et* $e < \phi(N)$ *avec* $ed \equiv 1 \pmod{\phi(N)}$ *et* $d < \frac{1}{3}N^{\frac{1}{4}}$, *alors on peut calculer* d *et factoriser* N.

preuve.

En utilisant $ed - k\phi(N) = 1$, $p + q < 3\sqrt{N}$ et $k < d < \frac{1}{3}N^{\frac{1}{4}}$, on a

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{|ed - kN|}{Nd} = \frac{|ed - k\phi(N) - kN + k\phi(N)|}{Nd}$$
$$\leq \cdots$$
$$< \frac{1}{2d^2}.$$

Donc $\frac{k}{d}$ est une convergente de $\frac{e}{N}$. □

CONTENU

Les réseaux

Définition

Soit n et d deux un entiers positifs. Soit L une partie non vide de $\mathbb{R}^n$. On dit que L est un réseau s'il existe une famille libre $(b_1 \cdots, b_d)$ de $\mathbb{R}^n$ telle que

$$L = \sum_{i=1}^{d} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{d} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

L'entier d est la dimension du réseau, et $(b_1 \cdots, b_d)$ est une base de ce réseau.

Les réseaux

Définition

Soit L un réseau de dimension n et $(b_1 \cdots, b_n)$ une base de L. Le déterminant de L est

$$\det(L) = |\det(b_1 \cdots, b_n)|.$$

Proposition

Soit L un réseau de dimension n. Le déterminant de L est indépendant de la base.

Les réseaux

Définition

Soit L un réseau de dimension n et $(b_1 \cdots, b_n)$ une base de L. Le déterminant de L est

$$\det(L) = |\det(b_1 \cdots, b_n)|.$$

Proposition

Soit L un réseau de dimension n. Le déterminant de L est indépendant de la base.

Les réseaux

Définition

Soient $x = (x_1 \cdots, x_n)$ *et* $y = (y_1 \cdots, y_n)$ *deux vecteurs de* $\mathbb{R}^n$.

1. *Le produit scalaire de* x *et* y *est*

$$\langle x, y \rangle = x^T y = \sum_{i=1}^{n} x_i y_i.$$

2. *La norme de* x *est*

$$\|x\| = (\langle x, x \rangle)^{\frac{1}{2}} = \left(\sum_{i=1}^{n} x_i^2 \right)^{\frac{1}{2}}.$$

Bases orthogonales

Théorème (Gram-Schmidt)

Soit V un sous-espace vectoiel de dimension n et $(b_1 \cdots, b_n)$ une base de V. On considère la famille de vecteurs $(b_1^* \cdots, b_n^*)$ définie par

$$b_1^* = b_1, \quad b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

avec pour $j < i$

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}.$$

Alors $(b_1^* \cdots, b_n^*)$ est une base orthogonale de V.

Bases orthogonales

Matrice de passage entre $(b_1^* \cdots, b_n^*)$ et $(b_1 \cdots, b_n)$

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ \mu_{2,1} & 1 & 0 & 0 & \cdots & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n_1,1} & \mu_{n-1,2} & \mu_{n-1,3} & \cdots & 1 & 0 \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \cdots & \mu_{n,n-1} & 1 \end{bmatrix} \begin{bmatrix} b_1^* \\ b_2^* \\ b_3^* \\ \vdots \\ b_{n-1}^* \\ b_n^* \end{bmatrix}.$$

Les réseaux

Théorème (Hadamard)

Soit L un réseau de dimension n, $(b_1 \cdots, b_n)$ une base de L et $(b_1^* \cdots, b_n^*)$ la famille orthogonale au sens de Gram-Schmidt. Alors

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\|.$$

Les réseaux

SVP : Problème du plus court vecteur du réseau

Etant donné un réseau L. Déterminer un vecteur non nul v qui minimise la nome $\|v\|$.

CVP : Problème du vecteur le plus proche

Etant donné un réseau L et un vecteur v_0. Déterminer un vecteur $v \neq v_0$ qui minimise la nome $\|v - v_0\|$.

Théorème (Hermitte)

Soit L un réseau de dimension n. Alors il existe un vecteur v non nul de L tel que

$$\|v\| \leq \sqrt{n} \det(L)^{\frac{1}{n}}.$$

Les réseaux

SVP : Problème du plus court vecteur du réseau

Etant donné un réseau L. Déterminer un vecteur non nul v qui minimise la nome $\|v\|$.

CVP : Problème du vecteur le plus proche

Etant donné un réseau L et un vecteur v_0. Déterminer un vecteur $v \neq v_0$ qui minimise la nome $\|v - v_0\|$.

Théorème (Hermitte)

Soit L un réseau de dimension n. Alors il existe un vecteur v non nul de L tel que

$$\|v\| \leq \sqrt{n} \det(L)^{\frac{1}{n}}.$$

Les réseaux

SVP : Problème du plus court vecteur du réseau

Etant donné un réseau L. Déterminer un vecteur non nul v qui minimise la nome $\|v\|$.

CVP : Problème du vecteur le plus proche

Etant donné un réseau L et un vecteur v_0. Déterminer un vecteur $v \neq v_0$ qui minimise la nome $\|v - v_0\|$.

Théorème (Hermitte)

Soit L un réseau de dimension n. Alors il existe un vecteur v non nul de L tel que

$$\|v\| \leq \sqrt{n} \det(L)^{\frac{1}{n}}.$$

L'algorithme LLL

LLL

A.K. Lenstra, H.W. Lenstra et L. Lovász, 1982

Définition

Une base $(b_1 \cdots, b_n)$ *est LLL-réduite si la base* $(b_1^* \cdots, b_n^*)$ *produite par Gram-Schmidt vérifie*

$$|\mu_{i,j}| \leq \frac{1}{2}, \quad \textit{pour} \quad 1 \leq j < i \leq n, \tag{1}$$

$$\frac{3}{4}\|b_{i-1}^*\|^2 \leq \|b_i^* + \mu_{i,i-1}b_{i-1}^*\|^2, \quad \textit{pour} \quad 1 < i \leq n, \tag{2}$$

avec

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}.$$

L'algorithme LLL

Théorème

Soit $(b_1 \cdots, b_n)$ une base LLL-réduite et $(b_1^*, \cdots, b_n^*)$ la base orthogonale associée par la méthode de Gram-Schmidt. Alors

$$\|b_j^*\| \leq 2^{\frac{i-j}{2}} \|b_i^*\|, \quad 1 \leq j \leq i \leq n. \tag{3}$$

$$\prod_{i=1}^{n} \|b_i\| \leq 2^{\frac{n(n-1)}{4}} \det(L). \tag{4}$$

$$\|b_j\| \leq 2^{\frac{i-1}{2}} \|b_i^*\|, \quad 1 \leq j \leq i \leq n. \tag{5}$$

$$\|b_1\| \leq 2^{\frac{n-1}{4}} (\det(L))^{\frac{1}{n}}. \tag{6}$$

$$\|b_1\| \leq 2^{\frac{n-1}{2}} \|v\|, \quad v \in L^*. \tag{7}$$

Polynômes à une variable

Données

- $N \in \mathbb{N}$, sans facteurs connus.
- L'existence d'un facteur inconnu b de N avec $b > N^{\beta}$.
- $f_b(x) = \sum_{i=1}^{\delta} a_i x^i \in \mathbb{Z}[x]$.
- Une borne X pour laquelle $f_b(x_0) \equiv 0 \pmod{b}$ avec $|x_0| < X$.

BUT

Déterminer x_0.

Polynômes à une variable

Données

- $N \in \mathbb{N}$, sans facteurs connus.
- L'existence d'un facteur inconnu b de N avec $b > N^{\beta}$.
- $f_b(x) = \sum_{i=1}^{\delta} a_i x^i \in \mathbb{Z}[x]$.
- Une borne X pour laquelle $f_b(x_0) \equiv 0 \pmod{b}$ avec $|x_0| < X$.

BUT

Déterminer x_0.

Polynômes à une variable

Theorem (Howgrave-Graham)

Soit $h(x) \in \mathbb{Z}[x]$ un polynôme de degré d ayant au plus ω monômes et X un nombre positif. Si x_0 est un entier et M un nombre positif tels que :

- $|x_0| < X$,
- $h(x_0) \equiv 0 \pmod{M}$,
- $\|h(xX)\| < \frac{M}{\sqrt{\omega}}$,

alors $h(x_0) = 0$ en tant qu'équation sur $\mathbb{Z}$.

Polynômes à une variable

Données

- $N \in \mathbb{N}$, sans facteurs connus.
- L'existence d'un facteur inconnu b de N avec $b > N^{\beta}$.
- $f_b(x) = \sum_{i=1}^{\delta} a_i x^i \in \mathbb{Z}[x]$.
- Une borne X pour laquelle $f_b(x_0) \equiv 0 \pmod{b}$ avec $|x_0| < X$.

Réseau

Pour des paramètres entiers m et t fixés, on considère le réseau formé par les vecteurs colonnes de la matrice définie par les polynômes :

$$\begin{aligned} g_{i,j}(x) &= x^j N^i (f_b(x))^{m-i}, \quad j = 0, \cdots, \delta - 1, \quad i = m, \cdots, 1, \\ h_i(x) &= x^i (f_b(x))^m, \quad i = 0, \cdots, t-1, \end{aligned}$$

Polynômes à une variable

Données

- $N \in \mathbb{N}$, sans facteurs connus.
- L'existence d'un facteur inconnu b de N avec $b > N^{\beta}$.
- $f_b(x) = \sum_{i=1}^{\delta} a_i x^i \in \mathbb{Z}[x]$.
- Une borne X pour laquelle $f_b(x_0) \equiv 0 \pmod{b}$ avec $|x_0| < X$.

Réseau

Pour des paramètres entiers m et t fixés, on considère le réseau formé par les vecteurs colonnes de la matrice définie par les polynômes :

$$\begin{aligned} g_{i,j}(x) &= x^j N^i (f_b(x))^{m-i}, \quad j = 0, \cdots, \delta - 1, \quad i = m, \cdots, 1, \\ h_i(x) &= x^i (f_b(x))^m, \quad i = 0, \cdots, t - 1, \end{aligned}$$

Polynômes à une variable

Formation de la matrice

	$j=0$ $\downarrow$	$j=1$ $\downarrow$	$j=2$ $\downarrow$	$\cdots$ $\downarrow$	$j=\delta-1$ $\downarrow$
$i=m \rightarrow$	$N^m,$	$N^m x,$	$N^m x^2,$	$\cdots$	$N^m x^{\delta-1},$
$i=m-1 \rightarrow$	$N^{m-1} f$	$N^{m-1} xf$	$N^{m-1} x^2 f$	$\cdots$	$N^{m-1} x^{\delta-1} f$
$i=m-2 \rightarrow$	$N^{m-2} f^2$	$N^{m-2} xf^2$	$N^{m-2} x^2 f^2$	$\cdots$	$N^{m-2} x^{\delta-1} f^2$
$\vdots \rightarrow$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i=2 \rightarrow$	$N^2 f^{m-2}$	$N^2 xf^{m-2}$	$N^2 x^2 f^{m-2}$	$\cdots$	$N^2 x^{\delta-1} f^{m-2}$
$i=1 \rightarrow$	Nf^{m-1}	Nxf^{m-1}	$Nx^2 f^{m-1}$	$\cdots$	$Nx^{\delta-1} f^{m-1}$

Polynômes à une variable

La ligne $i = m$

$$= \begin{bmatrix} N^m & & & \\ & N^m X & & \\ & & \ddots & \\ & & & N^m X^{\delta-1} \end{bmatrix}.$$

Polynômes à une variable

La ligne $i = m - 1$

$$\begin{bmatrix} - & - & - & - & N^{m-1}X^{\delta} & & & \\ - & - & - & - & - & N^{m-1}X^{\delta+1} & & \\ - & - & - & - & - & - & \ddots & \\ - & - & - & - & - & - & - & N^{m-1}X^{2\delta-1} \end{bmatrix}.$$

Polynômes à une variable

La ligne $i = 1$

$$\begin{bmatrix} — & \dots & — & NX^{(m-1)\delta} & & & \\ — & \dots & — & — & NX^{(m-1)\delta+1} & & \\ — & \dots & — & — & — & \ddots & \\ — & \dots & — & — & — & — & NX^{(m-1)\delta+\delta-1} \end{bmatrix}.$$

Polynômes à une variable

La ligne $i = 0$

$$\begin{bmatrix} - & - & \cdots & - & X^{m\delta} & & & \\ - & - & \cdots & - & - & X^{m\delta+1} & & \\ - & - & \cdots & - & - & - & \ddots & \\ - & - & \cdots & - & - & - & - & X^{m\delta+t-1} \end{bmatrix}.$$

Polynômes à une variable

Forme de la matrice finale

$$\begin{bmatrix}
1 & x & & & \cdots & & x^{m\delta+t} \\
\downarrow & \downarrow & & & & & \downarrow \\
N^m & & & & & & \\
 & N^m X & & & & & \\
 & & \ddots & & & & \\
 & & & N^m X^{\delta-1} & & & \\
- & - & - & - & N^{m-1}X^{\delta} & & \\
- & - & - & - & \ddots & & \\
- & - & - & - & \cdots & X^{m\delta} & \\
- & - & - & - & - & - \cdots & \ddots \\
- & - & - & - & - & - & \cdots \quad X^{m\delta+t-1}
\end{bmatrix}.$$

Polynômes à une variable

Théorème (Coppersmith)

Pour tout $\varepsilon > 0$, il existe un entier N_0 qui vérifie la propriété : Soit $N > N_0$ un entier de factorisation inconnue qui a un diviseur $b > N^{\beta}$. Soit $f_b(x)$ un polynôme de degrés δ. Toutes les solutions x_0 de la congruence $f_b(x) \equiv 0 \pmod{b}$ vérifiant

$$|x_0| < 2^{-\frac{1}{2}} N^{\frac{\beta^2}{\delta} - \varepsilon}$$

peuvent être déterminées en temps polynômial en $\log N$.

Polynômes à une variable

Théorème (Coppersmith)

Soit $N = pq$ un module RSA dont les facteurs premiers p et q sont inconnus et tels que $q < p$. Si on connait une valeur $\tilde{p}$ telle que

$$|\tilde{p} - p| < N^{\frac{1}{4}},$$

alors on peut factoriser N en temps polynômial en $\log N$.

Applications

1

Si $ex - y\phi(N) = z$ et x, y, z petits, alors on peut factoriser N.

2

Si $ex - y(N - pu) = z$ et u, x, y, z petits, alors on peut factoriser N.

3

Si $ex - y(N - (pu - qv)) = z$ et u, v, x, y, z petits, alors on peut factoriser N.

4

Si $ex - y\phi(N) = Nz$ et u, v, x, y, z petits, alors on peut factoriser N.

Applications

1

Si $ex - y\phi(N) = z$ et x, y, z petits, alors on peut factoriser N.

2

Si $ex - y(N - pu) = z$ et u, x, y, z petits, alors on peut factoriser N.

3

Si $ex - y(N - (pu - qv)) = z$ et u, v, x, y, z petits, alors on peut factoriser N.

4

Si $ex - y\phi(N) = Nz$ et u, v, x, y, z petits, alors on peut factoriser N.

Applications

1

Si $ex - y\phi(N) = z$ et x, y, z petits, alors on peut factoriser N.

2

Si $ex - y(N - pu) = z$ et u, x, y, z petits, alors on peut factoriser N.

3

Si $ex - y(N - (pu - qv)) = z$ et u, v, x, y, z petits, alors on peut factoriser N.

4

Si $ex - y\phi(N) = Nz$ et u, v, x, y, z petits, alors on peut factoriser N.

Applications

1

Si $ex - y\phi(N) = z$ et x, y, z petits, alors on peut factoriser N.

2

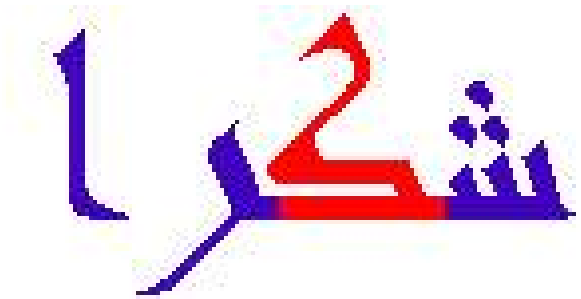
Si $ex - y(N - pu) = z$ et u, x, y, z petits, alors on peut factoriser N.

3

Si $ex - y(N - (pu - qv)) = z$ et u, v, x, y, z petits, alors on peut factoriser N.

4

Si $ex - y\phi(N) = Nz$ et u, v, x, y, z petits, alors on peut factoriser N.



Mais

Ce n'est pas fini

شِعر

لَا يَنَالُ العُلَا مَن طَبعُهُ الغَضَبُ وَ لَا يَحمِلُ الحِقدَ مَن تَعلُوا بِهِ الرُّتَبُ

شِعر

عَنتَرَة إِبنُ شَدَّاد العَبسي

شِعر

لَا يَنَالُ العُلَا مَن طَبعُهُ الغَضَبُ وَ لَا يَحمِلُ الحِقدَ مَن تَعلُوا بِهِ الرُّتَبُ

شِعر

عَنتَرَة إِبنُ شَدَّاد العَبسي

شِعر

وَ مَن لَا يُحِبُّ صُعُودَ الجِبَالِ يَعشُ أَبَدَ الدَّهرِ بَينَ الحُفَرِ.

شِعر

ابُو القَاسِم الشَابِّي

شِعر

وَ مَن لَا يُحِبُّ صُعُودَ الجِبَالِ يَعشُ أَبَدَ الدَّهرِ بَينَ الحُفَرِ.

شِعر

ابُو القَاسِم الشَابِّي

شِعر

وَمَا نَيلُ المَطَالِبِ بِالتَّمَنّي وَ لَاكِن تُؤخَذُ الدُّنيَا غَلَابَا

شِعر

ابُو العَلَاءِ المَعَرّي

شِعر

وَمَا نَيلُ المَطَالِبِ بِالتَّمَنّي وَ لَاكِن تُؤخَذُ الدُّنيَا غَلَابَا

شِعر

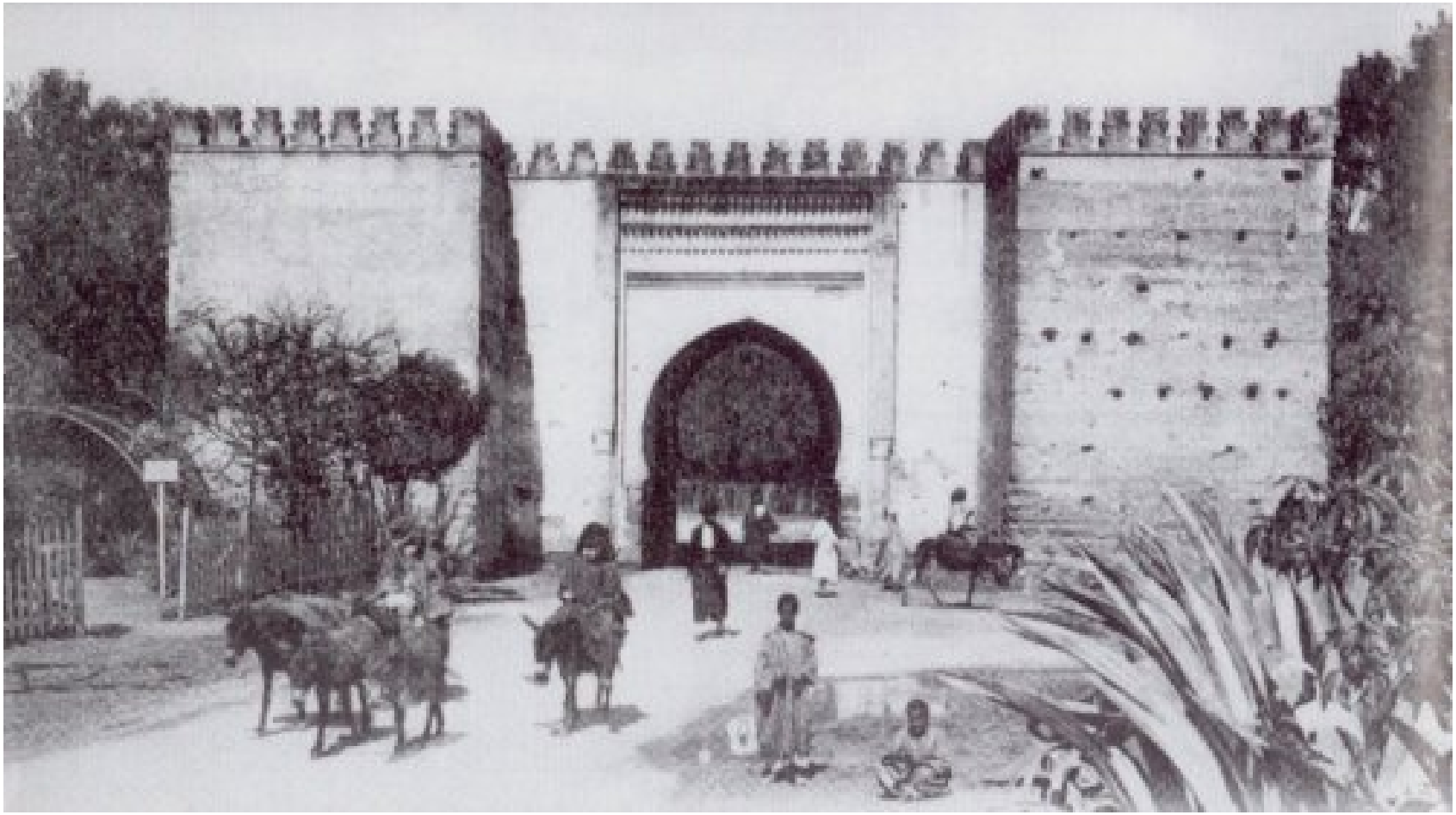
ابُو العَلَاءِ المَعَرّي

AFRICACRYPT 2009

Des tarifs préférentiels sont réservés aux étudiants africains.
Contacter Sami Omar

Oujda 2000

Oujda 1900



Hommage à toutes les participantes

إِذَا علَّمتَ رَجُلًا فَقَد علَّمتَ فَردًا، أَمَّا إِذَا علَّمتَ إِمرأَةً فَقَد علَّمتَ عَائِلةً.