CRYPTANALYSE DE CERTAINS RSA PAR LES FRACTIONS CONTINUES ET L'ALGORITHME LLL

Abderrahmane Nitaj

13 Janvier 2005

Contenu

- Le cryptosystème RSA
- Les fractions continues
- Le théorème de Legendre
- Les réseaux
- L'algorithme LLL
- Le théorème de Coppersmith
- Le théorème de May
- L'attaque de Wiener
- L'attaque de de Weger
- Les modules de sécurité
- Généralisation de l'attaque de de Weger
- L'attaque de Blömer-May
- Généralisation de l'attaque de Blömer-May

Le cryptosystème RSA

Brigitte veut envoyer un message secret à Ali.

- Ali construit son initialisation :
  - Choisit p et q premiers.
  - Calcule $n = pq$.
  - Choisit e, $\gcd(e, \phi(n)) = 1$.
  - Calcule $d \equiv 1/e \pmod{\phi(n)}$.
  - p, q et d sont privés, n et e sont publics.
- Brigitte envoie le message :
  - prend $m \in \{2, 3, \cdots, n-1\}$.
  - Calcule $c \equiv m^e \pmod{n}$.
  - envoie le message c.
  - m est secret, c est public.
- Ali procède au décodage :
  - Calcule $m \equiv c^d \pmod{n}$.
- Equation : $\boxed{ed - k\phi(n) = 1.}$

Les fractions continues

- Données :
  - $n \in \mathbb{N}$.
  - $e \in \mathbb{N}$, $\qquad e < n$.
- On cherche :
  - $a \in \mathbb{N}$.
  - $b \in \mathbb{N}$.
  - $\frac{a}{b} \approx \frac{e}{n}$.

$\Longrightarrow$

- Divisions Euclidiennes successives.
- Algorithme des fractions continues.
  - Calcule $\frac{e}{n} = [a_0, a_1, \cdots, a_s] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_s}}}$.
  - $a = NUMER([a_0, a_1, \cdots, a_i])$.
  - $b = DENOM([a_0, a_1, \cdots, a_i])$.

Le théorème de Legendre?Lagrange?

- Données :
  - $n \in \mathbb{N}$.
  - $e \in \mathbb{N}, \qquad e < n$.
  - $a, b \in \mathbb{N}, \qquad \frac{a}{b} \approx \frac{e}{n}$.
- Problème :
  - $\frac{a}{b}$ est-il une réduite de $\frac{e}{n}$?

$\Longrightarrow$

- Théorème.
  - Si $\left|\frac{a}{b} - \frac{e}{n}\right| < \frac{1}{2b^2}$, alors $\frac{a}{b}$ est une réduite de $\frac{e}{n}$.

Les réseaux

- Données :
  - $v_1, v_2, \cdots v_m \in \mathbb{R}^l$, $l \geq m$, linéairement indépendants.
  - $L = \mathbb{Z}.v_1 \oplus \mathbb{Z}.v_2 \oplus \cdots \oplus \mathbb{Z}.v_m$.
- Caractéristiques
  - dim$(L) = m$.
  - det$(L) = \prod_{i=1}^{m} ||v_i^*||$ (après une orthogonalisation de Gram-Schmidt).
  - Théorème de Minkowski: $\exists v \in L$ tel que $||v|| \leq \sqrt{m}\text{det}(L)^{\frac{1}{m}}$.
- Problème : $\boxed{\text{Trouver un vecteur court.}}$

L'algorithme LLL

- Données :
  - $v_1, v_2, \cdots v_m \in \mathbb{R}^l$, linéairement indépendants.
  - $L = \mathbb{Z}.v_1 \oplus \mathbb{Z}.v_2 \oplus \cdots \oplus \mathbb{Z}.v_m$.
- Problème : Déterminer un vecteur v
  - $v \in L$.
  - $||v||$ est assez petite.

$\Longrightarrow$

- L'algorithme LLL (Lenstra-Lenstra-Lovasz) :
  - Produit un vecteur v, $||v|| \leq 2^{\frac{m-1}{4}} \det(L)^{\frac{1}{m}}$.
  - En temps polynomial en m.

Le théorème de Coppersmith

- Données :
  - $n = pq$.
  - $\tilde{p}$, tel que $|p - \tilde{p}| \leq n^{1/4}$.
- Problème : Déterminer p et q

$\Longrightarrow$

- Le théorème de Coppersmith :
  - Produit p et q.
  - En temps polynomial en $\log(n)$.

Le théorème de May

- Données :
  - $n = pq$.
  - $\tilde{P}$, tel que $|up - \tilde{P}| \leq n^{1/4}$.
- Problème : Déterminer p, q et u

$\Longrightarrow$

- Le théorème de May :
  - Utiliser Coppersmith pour produire up.
  - $p = \gcd(up, n)$.
  - En temps polynomial en $\log(n)$.

L'attaque de Wiener

Les fractions continues.

- Données :.
  - $n = pq$.
  - $e \qquad (e < n)$.
- But :
  - Trouver d, k, $\phi(n)$, p, q
  - En utilisant l'équation $ed - k\phi(n) = 1$.

$\Longrightarrow$

- L'attaque de Wiener
  - Si $d < \frac{1}{3}n^{\frac{1}{4}}$, alors d est le dénominateur d'une réduite de $\frac{e}{n}$.
- L'idée
  - $\left|\frac{k}{d} - \frac{e}{\phi(n)}\right|$ est petit.
  - $\phi(n) = n + 1 - p - q \approx n$.
  - Les réduites de $\frac{e}{n}$.

La généralisation de de Weger

Les fractions continues.

- Données :
  - $n = pq, \qquad (p \approx q)$.
  - $e, \qquad (e < n)$.
- But :
  - Trouver d, k, $\phi(n)$, p, q.
  - En utilisant l'équation $ed - k\phi(n) = 1$.

$\Longrightarrow$

- L'attaque de de Weger
  - Si $d < \frac{n^{\frac{3}{4}}}{|p-q|}$, alors d est le dénominateur d'une réduite de $\frac{e}{n+1-2\sqrt{n}}$.
- L'idée :
  - $\left|\frac{k}{d} - \frac{e}{\phi(n)}\right|$ est petit.
  - $\phi(n) = n + 1 - p - q \approx n + 1 - 2\sqrt{n}$.
  - Les réduites de $\frac{e}{n+1-2\sqrt{n}}$.

Les modules de sécurité

p et q ont le même nombre de bits.

- Données :
  - $n = pq, \qquad (q < p < 2q) \Longleftrightarrow n$ est un module de sécurité.
- Conséquences :
  - $\frac{\sqrt{2}}{2}\sqrt{n} < q < \sqrt{n} < p < \sqrt{2}\sqrt{n}$.
  - $\frac{p}{q} = 1 + x_0, \qquad (0 < x_0 < 1)$.
  - $\phi(n) = n + 1 - \frac{2+x_0}{\sqrt{1+x_0}}\sqrt{n}$.

$\Longrightarrow$

- Deux exemples.
  - $q \approx \sqrt{n} \approx p \Longleftrightarrow x_0 \approx 0 \Longleftrightarrow$ l'attaque de de Weger avec $\phi(n) \approx n + 1 - 2\sqrt{n}$.
  - $q \approx \frac{\sqrt{2}}{2}\sqrt{n}, p \approx \sqrt{2}\sqrt{n} \Longleftrightarrow x_0 \approx 1 \Longleftrightarrow$ une attaque avec $\phi(n) \approx n + 1 - \frac{3}{\sqrt{2}}\sqrt{n}$.

Généralisation de l'attaque de de Weger

- Données :
  - $n = pq$, module de sécurité $\quad (q < p < 2q)$, $\left[\frac{p}{q} \approx 1 + \frac{a}{b}\right]$
  - $e, \quad (e < n)$.
- But :
  - Trouver d, k, $\phi(n)$, p, q.
  - En utilisant l'équation $ed - k\phi(n) = 1$.
- Théorème :
  - $x = \frac{a}{b}, \quad F(x) = n + 1 - \frac{2+x}{\sqrt{1+x}}\sqrt{n}$.
  - $\left|\frac{p}{q} - 1 - x\right| = n^{-\gamma}$
  - Si $d < n^{\frac{1}{4}+\frac{\gamma}{2}}$, alors d est le dénominateur d'une réduite de $\frac{e}{F(x)}$.
- L'idée
  - $\left|\frac{k}{d} - \frac{e}{\phi(n)}\right|$ est petit.
  - $\phi(n) = n + 1 - p - q \approx F(x)$.
  - Les réduites de $\frac{e}{F(x)}$.

Généralisation de l'attaque de de Weger: L'algorithme

- Données :
  - $n = pq$, module de sécurité $\quad (q < p < 2q)$.
  - $e, \quad (e < n)$.
  - $\left[\frac{p}{q} \approx 1 + \frac{a}{b}\right]$,
  - $0 \leq a < b \leq B$.
- Algorithme 1:
  - $0 \leq a \leq B$
  - $0 \leq b \leq B$
  - $x = \frac{a}{b}$.
  - $F(x) := n + 1 - \frac{2+x}{\sqrt{1+x}}$.
  - Calculer les réduites $\frac{X}{Y}$ de $\frac{e}{F(x)}$ avec $Y < e$.
  - Pour chaque réduite $\frac{X}{Y}$, calculer $T \equiv eY - 1 \pmod{X}$.
  - Si $T = 0$, prendre $\phi(n) = \frac{eY-1}{X}$ et calculer p et q.
  - Stoper si $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$.

Généralisation de l'attaque de de Weger: un exemple

- Données :
  - $n = pq = 8133876630876764379064472085871019680113623317877$.
  - $e = 6055258312152372605476785266317750951108834153931$.
- Résultats :
  - $B = 300$, $a = 152$, $b = 273$, $x = \frac{152}{273}$.
  - La 49ème réduite $\frac{X}{Y} = \frac{894685072338790067428 52}{1201808019863653564738 43}$,
  - $p = 3558458718976746753830603$, $q = 2285786424189769091284159$.
  - $d \approx n^{0.47}$.

- Pourquoi?
  - Avec l'algorithme 1: Une solution car
    - $d\sqrt{|p/q - 1 - a/b|} \approx n^{0.47-0,46/2} \approx n^{0.24} < n^{0.25}$.
    - $\frac{p}{q} \approx 1 + \left[0, 1, \frac{1}{2}, \frac{4}{7}, \frac{5}{9}, \frac{49}{88}, \frac{103}{185}, \frac{152}{273}, \cdots\right]$.
  - Pas de solution avec l'attaque de Wiener : $d \approx n^{0.47} >> n^{0.25}$.
  - Pas de solution avec l'attaque de de Weger : $(p-q)d \approx n^{0.49+0.47} \approx n^{0.96} >> n^{0.75}$.

L'attaque de Blömer-May

Les fractions continues+LLL.

- Données :
  - $n = pq$, module de sécurité $\quad (q < p < 2q)$.
  - $e, \quad (e < n)$.
- But :
  - Trouver p, q.
  - En utilisant l'équation $eY - X\phi(n) = Z$.
- Théorème :
  - Si $0 < Y \leq \frac{1}{3}n^{\frac{1}{4}}$ et $|Z| \leq n^{-\frac{3}{4}}eY$, alors n peut être factorisé en temps polynomial.
- L'idée
  - $\left|\frac{X}{Y} - \frac{e}{\phi(n)}\right|$ est petit.
  - $\phi(n) = n + 1 - p - q \approx n \Longrightarrow$ les réduites de $\frac{e}{n} \Longrightarrow X$ et Y.
  - $p + q \approx n + 1 - e\frac{Y}{X}$, $pq = n \Longrightarrow$ approximation de $p \Longrightarrow$ Coppersmith-LLL $\Longrightarrow p$.

Généralisation de l'attaque de Blömer-May (1/2)

- Données :
  - $n = pq$, module de sécurité $\quad (q < p < 2q)$.
  - $e, \quad (e < n)$.
- But :
  - Trouver p, q.
  - En utilisant l'équation $eY - XF = Z$.
  - Conditions :
    - $F \approx n$,
    - de F on peut extraire un multiple de p ou de q,
- L'idée
  - $\left|\frac{X}{Y} - \frac{e}{F}\right|$ est petit.
  - $F \approx n \Longrightarrow$ les fractions continues de $\frac{e}{n} \Longrightarrow X$ et Y.
  - $F \approx e\frac{Y}{X} \Longrightarrow$ approximation d'un multiple pu ou $qu \Longrightarrow$ Coppersmith-LLL-May $\Longrightarrow p$ ou q.

Généralisation de l'attaque de Blömer-May (2/2)

- Données :
  - $n = pq$, module de sécurité $\quad (q < p < 2q)$.
  - $e, \quad (e < n)$.
- But :
  - Trouver p, q.
  - En utilisant l'équation $eY - XF = Z$.
- Théorème :
  - Si $0 < Y \leq \frac{1}{\sqrt{2e}} \frac{n}{\sqrt{|F-n|}}$ et $|Z| \leq n^{-\frac{3}{4}} eY$, alors n peut être factorisé en temps polynomial.

Généralisation de l'attaque de Blömer-May : $F = p(q-u)$

- Données :
  - $n = pq$, module de sécurité $\quad (q < p < 2q)$.
  - $e, \quad (e < n)$.
- But :
  - Trouver p, q.
  - $F = F(u) = p(q-u)$, $u \in \mathbb{Z}$, inconnu.
  - En utilisant l'équation $eY - XF = Z$.
- Algorithme 2:
  - Calculer les réduites $\frac{X}{Y}$ de $\frac{e}{n}$ avec $Y < e$.
  - Pour chaque réduite $\frac{X}{Y}$, calculer $\tilde{P} = n - \frac{eY}{X}$.
  - Calculer pu par l'algorithme de Coppersmith.
  - Stoper si $\gcd(pu, n) \neq 1, n$.

Généralisation de l'attaque Blömer-May : un exemple

- Données :
  - $n = pq = 94109625208978446256481635828331078768267327552 3$.
  - $e = 847441242103359735969302036883150331348431432 7$.
- Résultats :
  - La 12ème réduite $\frac{X}{Y} = \frac{36482}{4051381}$,
  - Coppersmith-LLL-May avec $\tilde{P} = n - \frac{eY}{X}$.
  - $p = 1321110693270343633073777$,
  - $q = 712352308465649934350899$,
  - $u = 1215417$.
  - $F = p(q-u)$, $Z = eY - FX$.
- Pourquoi?
  - Avec l'algorithme 2: Une solution car
    - Y et Z vérifient le théorème.
  - Pas de solution avec l'attaque de Blömer-May car:
    - Pour toutes les réduites $\frac{x}{y}$, $\left|p + q - \left(n + 1 - \frac{ey}{x}\right)\right| >> n^{1/4}$.

Généralisation de l'attaque de Blömer-May :Autres F

- Données :
  - $n = pq$, module de sécurité $\quad (q < p < 2q)$.
  - $e, \quad (e < n)$.
- But :
  - Trouver p, q.
  - En utilisant l'équation $eY - XF = Z$.
  - Conditions :
    - $F \approx n$,
    - de F on peut extraire un multiple de p ou de q,
- Exemples :
  - $F = p(q - u)$, $u \in \mathbb{Z}$.
  - $F = q(p - u)$, $u \in \mathbb{Z}$.
  - $F = (p - 1)(p - u)$, $u \in \mathbb{Z}$ (généralise $\phi(n) = (p - 1)(q - 1)$).
  - $F = (p - u)(q - 1/u)$, $u \in \mathbb{Z}$.