# Another Generalization of Wiener’s Attack on RSA

Abderrahmane NITAJ

Université de Caen, France

Casablanca, June 12, 2008

الدار البيضاء، المغرب

# Colour conventions

**Red**

Secret parameters.

**Blue or Black**

Public parameters.

# Colour conventions

**Red**

Secret parameters.

**Blue or Black**

Public parameters.

## RSA cryptosystem

- Rivest, Shamir and Adleman (1977).
- The most successful public key encryption algorithm.
- The security of RSA is based on the problem of factoring large integers.

## The RSA modulus

- $p$, $q$ large primes with the same bit-size.
- $N = pq$.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$.
- $e \in \mathbb{N}$, $1 < e < \phi(N)$, the public exponent.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given $N$, $e$, find $p$, $q$.

## The RSA modulus

- $p$, $q$ large primes with the same bit-size.
- $N = pq$.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$.
- $e \in \mathbb{N}$, $1 < e < \phi(N)$, the public exponent.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given $N$, $e$, find $p$, $q$.

## The RSA modulus

- $p$, $q$ large primes with the same bit-size.
- $N = pq$.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$.
- $e \in \mathbb{N}$, $1 < e < \phi(N)$, the public exponent.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given $N$, $e$, find $p$, $q$.

## The RSA modulus

- $p$, $q$ large primes with the same bit-size.
- $N = pq$.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$.
- $e \in \mathbb{N}$, $1 < e < \phi(N)$, the public exponent.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given $N$, $e$, find $p$, $q$.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Wiener's attack, 1990

If $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

## The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Wiener's attack, 1990

If $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

## The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Wiener's attack, 1990

If $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

## The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Boneh-Durfee's attack, 2000

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

## The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p + q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Boneh-Durfee's attack, 2000

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

## The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p+q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Boneh-Durfee's attack, 2000

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

## The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p+q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

## The variant RSA equation

$$ex - (p-1)(q-1)k = y.$$

## Blömer-May's attack, 2004

If $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = O\left(N^{-\frac{3}{4}}ex\right)$ then the factorization of $N = pq$ can be found.

## The method

- $\frac{k}{x} \approx \frac{e}{N}$.
- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

## The variant RSA equation

$$ex - (p-1)(q-1)k = y.$$

## Blömer-May's attack, 2004

If $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = O\left(N^{-\frac{3}{4}}ex\right)$ then the factorization of $N = pq$ can be found.

## The method

- $\frac{k}{x} \approx \frac{e}{N}$.
- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

## The variant RSA equation

$$ex - (p-1)(q-1)k = y.$$

## Blömer-May's attack, 2004

If $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = O\left(N^{-\frac{3}{4}}ex\right)$ then the factorization of $N = pq$ can be found.

## The method

- $\frac{k}{x} \approx \frac{e}{N}$.
- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

# The new attack

## The variant RSA equation

$$eX - (p-u)(q-v)Y = 1.$$

$u = v = 1$ implies the RSA equation $ed - (p-1)(q-1)k = 1$.

## The new attack

If $1 \le Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$, $|u| < N^{\frac{1}{4}}$, $v = \left[ -\frac{qu}{p-u} \right]$, and all prime factors of $p-u$ or $q-v$ are less than $10^{50}$, then the factorization of $N = pq$ can be found.

## The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

# The new attack

## The variant RSA equation

$$eX - (p-u)(q-v)Y = 1.$$

$u = v = 1$ implies the RSA equation $ed - (p-1)(q-1)k = 1$.

## The new attack

If $1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$, $|u| < N^{\frac{1}{4}}$, $v = \left[-\frac{qu}{p-u}\right]$, and all prime factors of $p-u$ or $q-v$ are less than $10^{50}$, then the factorization of $N = pq$ can be found.

## The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

# The new attack

## The variant RSA equation

$$eX - (p-u)(q-v)Y = 1.$$

$u = v = 1$ implies the RSA equation $ed - (p-1)(q-1)k = 1$.

## The new attack

If $1 \leq Y < X < 2^{-\frac{1}{4}}N^{\frac{1}{4}}$, $|u| < N^{\frac{1}{4}}$, $v = \left[-\frac{qu}{p-u}\right]$, and all prime factors of $p-u$ or $q-v$ are less than $10^{50}$, then the factorization of $N = pq$ can be found.

## The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

## The Continued fraction alorithm

- $e$ and $N$ are coprime positive integers.
- $$\frac{e}{N} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}.$$
- $\frac{e}{N} = [a_0, a_1, a_2, \cdots]$ where $a_i$ are positive integers.
- $\frac{r_i}{s_i} = [a_0, a_1, a_2, \cdots, a_i]$ are called the convergents.

## The convergent theorem

If $\left|\frac{e}{N} - \frac{x}{y}\right| < \frac{1}{2y^2}$, then $\frac{x}{y}$ is one of the convergents of the continued fraction expansion of $\frac{e}{N}$.

## The Continued fraction alorithm

- $e$ and $N$ are coprime positive integers.
- $\frac{e}{N} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}.$
- $\frac{e}{N} = [a_0, a_1, a_2, \cdots]$ where $a_i$ are positive integers.
- $\frac{r_i}{s_i} = [a_0, a_1, a_2, \cdots, a_i]$ are called the convergents.

## The convergent theorem

If $\left|\frac{e}{N} - \frac{x}{y}\right| < \frac{1}{2y^2}$, then $\frac{x}{y}$ is one of the convergents of the continued fraction expansion of $\frac{e}{N}$.

## Coppermith's theorem

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Given an approximation $\tilde{p}$ of $p$ with $|p - \tilde{p}| < N^{\frac{1}{4}}$, then $N = pq$ can be factored in time polynomial in $\log N$.

## Smooth numbers

Let $y$ be a positive constant. A positive number $n$ is $y$-smooth if all prime factors of $n$ are less than $y$.

## The Elliptic Curve Method (ECM)

- H.W. Lenstra, 1985, phase 1.
- Brent, Montgomery, 1986-87, phase 2.
- ECM is very efficient to factor $B_{\text{ecm}}$-smooth integers where

$$B_{\text{ecm}} = 10^{50}$$

## Smooth numbers

Let $y$ be a positive constant. A positive number $n$ is $y$-smooth if all prime factors of $n$ are less than $y$.

## The Elliptic Curve Method (ECM)

- H.W. Lenstra, 1985, phase 1.
- Brent, Montgomery, 1986-87, phase 2.
- ECM is very efficient to factor $B_{\text{ecm}}$-smooth integers where

$$B_{\text{ecm}} = 10^{50}$$

## The counting function

$$\Psi(x,y) = \#\{n : 1 \le n \le x,\ n \text{ is } y\text{-smooth}\}.$$

## Theorem (Hildebrand)

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

holds in the range $x = y^u$ and $y > \exp\left\{(\log\log x)^{5/3+\varepsilon}\right\}$ where $\rho(u)$ be the Dickman-de Bruijn function.

## Theorem (Friedlander and Granville)

$$\Psi(x+z,y) - \Psi(x,y) \ge c\frac{z}{x}\Psi(x,y)$$

in the range $x \ge z \ge x^{\frac{1}{2}+\delta}$, $x \ge y \ge x^{1/\gamma}$, $\delta > 0$, $\gamma > 0$, $c = c(\delta,\gamma) > 0$.

## The counting function

$$\Psi(x,y) = \#\{n : 1 \le n \le x,\ n \text{ is } y\text{-smooth}\}.$$

## Theorem (Hildebrand)

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

holds in the range $x = y^u$ and $y > \exp\left\{(\log\log x)^{5/3+\varepsilon}\right\}$ where $\rho(u)$ be the Dickman-de Bruijn function.

## Theorem (Friedlander and Granville)

$$\Psi(x+z,y) - \Psi(x,y) \ge c\frac{z}{x}\Psi(x,y)$$

in the range $x \ge z \ge x^{\frac{1}{2}+\delta}$, $x \ge y \ge x^{1/\gamma}$, $\delta > 0$, $\gamma > 0$, $c = c(\delta,\gamma) > 0$.

## The counting function

$$\Psi(x,y) = \#\left\{n : 1 \le n \le x,\ n \text{ is } y\text{-smooth}\right\}.$$

## Theorem (Hildebrand)

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

holds in the range $x = y^u$ and $y > \exp\left\{(\log\log x)^{5/3+\varepsilon}\right\}$ where $\rho(u)$ be the Dickman-de Bruijn function.

## Theorem (Friedlander and Granville)

$$\Psi(x+z,y) - \Psi(x,y) \ge c\frac{z}{x}\Psi(x,y)$$

in the range $x \ge z \ge x^{\frac{1}{2}+\delta}$, $x \ge y \ge x^{1/\gamma}$, $\delta > 0$, $\gamma > 0$, $c = c(\delta,\gamma) > 0$.

# The proof

## Setting

- $eX - (p-u)(q-v)Y = 1$.
- $1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$.
- $|u| < N^{\frac{1}{4}}, \quad v = \left[ -\frac{qu}{p-u} \right]$.
- Without loss of generality, suppose $p - u$ is $B_{\text{ecm}}$-smooth.

- Write $eX - NY = 1 - (N - (p-u)(q-v))Y$. Then

$$\frac{e}{N} \approx \frac{Y}{X}.$$

- Compute $X$ and $Y$ via **the continued fraction expansion** of $\frac{e}{N}$.
- Compute $(p-u)(q-v) = \frac{eX-1}{Y}$.
- Apply **ECM** to write $\frac{eX-1}{Y} = M_1 M_2$ where $M_1$ is $B_{\text{ecm}}$-smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \le B_{\text{ecm}}, \qquad a_i \ge 1.$$

- Write $eX - NY = 1 - (N - (p-u)(q-v))Y$. Then

$$\frac{e}{N} \approx \frac{Y}{X}.$$

- Compute $X$ and $Y$ via **the continued fraction expansion** of $\frac{e}{N}$.
- Compute $(p-u)(q-v) = \frac{eX-1}{Y}$.
- Apply **ECM** to write $\frac{eX-1}{Y} = M_1 M_2$ where $M_1$ is $B_{\text{ecm}}$-smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \leq B_{\text{ecm}}, \qquad a_i \geq 1.$$

- Write $eX - NY = 1 - (N - (p-u)(q-v))Y$. Then

$$\frac{e}{N} \approx \frac{Y}{X}.$$

- Compute $X$ and $Y$ via **the continued fraction expansion** of $\frac{e}{N}$.
- Compute $(p-u)(q-v) = \frac{eX-1}{Y}$.
- Apply **ECM** to write $\frac{eX-1}{Y} = M_1 M_2$ where $M_1$ is $B_{\text{ecm}}$-smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \leq B_{\text{ecm}}, \qquad a_i \geq 1.$$

- Write $eX - NY = 1 - (N - (p-u)(q-v))Y$. Then

$$\frac{e}{N} \approx \frac{Y}{X}.$$

- Compute $X$ and $Y$ via **the continued fraction expansion** of $\frac{e}{N}$.
- Compute $(p-u)(q-v) = \frac{eX-1}{Y}$.
- Apply **ECM** to write $\frac{eX-1}{Y} = M_1 M_2$ where $M_1$ is $B_{\text{ecm}}$-smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \leq B_{\text{ecm}}, \qquad a_i \geq 1.$$

- Since $p-u$ is $B_{\text{ecm}}$-smooth, then

$$p-u=\prod_{i=1}^{\omega(M_1)} p_i^{x_i}, \qquad x_i\geq 0.$$

- Since $N^{\frac{1}{2}}<p-u<\sqrt{2}N^{\frac{1}{2}}$, then

$$0<\sum_{i=1}^{\omega(M_1)} x_i\log p_i-\frac{1}{2}\log N<\frac{1}{2}\log 2.$$

- To solve this
  - The Lenstra-Lenstra-Lovasz LLL algorithm.
  - The Ferguson PSLQ algorithm.
  - Exhaustive search since $\omega(M_1)\sim\log\log M_1$.

- Since $p-u$ is $B_{\text{ecm}}$-smooth, then

$$p-u=\prod_{i=1}^{\omega(M_1)} {p_i}^{x_i}, \qquad x_i \geq 0.$$

- Since $N^{\frac{1}{2}} < p-u < \sqrt{2}N^{\frac{1}{2}}$, then

$$0 < \sum_{i=1}^{\omega(M_1)} x_i \log p_i - \frac{1}{2}\log N < \frac{1}{2}\log 2.$$

- To solve this
  - The Lenstra-Lenstra-Lovasz LLL algorithm.
  - The Ferguson PSLQ algorithm.
  - Exhaustive search since $\omega(M_1) \sim \log\log M_1$.

- Since $p-u$ is $B_{\text{ecm}}$-smooth, then

$$p-u=\prod_{i=1}^{\omega(M_1)} p_i^{x_i}, \qquad x_i \geq 0.$$

- Since $N^{\frac{1}{2}} < p-u < \sqrt{2}N^{\frac{1}{2}}$, then

$$0 < \sum_{i=1}^{\omega(M_1)} x_i \log p_i - \frac{1}{2}\log N < \frac{1}{2}\log 2.$$

- To solve this
  - The Lenstra-Lenstra-Lovasz LLL algorithm.
  - The Ferguson PSLQ algorithm.
  - Exhaustive search since $\omega(M_1) \sim \log\log M_1$.

- Finally, apply Coppersmith's algorithm to find $p$ using

$$p - u = \prod_{i=1}^{\omega(M_1)} p_i^{x_i}, \qquad x_i \geq 0.$$

**Cardinality**

- $eX - (p-u)(q-v)Y = 1.$
- $1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}.$
- $|u| < N^{\frac{1}{4}}, \quad v = \left[ -\frac{qu}{p-u} \right].$
- Without loss of generality, suppose $p-u$ is $B_{\text{ecm}}$-smooth.
- Then using Hildebrand and Friedlander and Granville results on smooth numbers, we find that there are at least $N^{\frac{1}{2}-\varepsilon}$ such keys.

- Finally, apply Coppersmith's algorithm to find $p$ using

$$p - u = \prod_{i=1}^{\omega(M_1)} {p_i}^{x_i}, \qquad x_i \geq 0.$$

## Cardinality

- $eX - (p-u)(q-v)Y = 1.$
- $1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}.$
- $|u| < N^{\frac{1}{4}}, \quad v = \left[-\frac{qu}{p-u}\right].$
- Without loss of generality, suppose $p - u$ is $B_{\text{ecm}}$-smooth.
- Then using Hildebrand and Friedlander and Granville results on smooth numbers, we find that there are at least $N^{\frac{1}{2}-\varepsilon}$ such keys.

# Comparison

## Wiener's attack

- The equation :
$$ed - (p-1)(q-1)k = 1.$$
- The method :
The continued fraction algorithm
- The size of such keys :
$$\mathcal{O}\left(N^{\frac{1}{4}}\right).$$

## The new attack

- The equation :
$$eX - (p-u)(q-v)Y = 1.$$
- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :
$$\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right).$$

# Comparison

## Wiener's attack

- The equation :

$$ed - (p-1)(q-1)k = 1.$$

- The method :
  The continued fraction algorithm
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{4}}\right).$$

## The new attack

- The equation :

$$eX - (p-u)(q-v)Y = 1.$$

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right).$$

# Comparison

## Wiener's attack

- The equation :

$$ed - (p-1)(q-1)k = 1.$$

- The method :
  The continued fraction algorithm
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{4}}\right).$$

## The new attack

- The equation :

$$eX - (p-u)(q-v)Y = 1.$$

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right).$$

# Comparison

## Wiener's attack

- The equation :

$$ed-(p-1)(q-1)k=1.$$

- The method :
  The continued fraction algorithm
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{4}}\right).$$

## The new attack

- The equation :

$$eX-(p-u)(q-v)Y=1.$$

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right).$$

# Comparison

## Wiener's attack

- The equation :

$$ed-(p-1)(q-1)k=1.$$

- The method :
  The continued fraction algorithm
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{4}}\right).$$

## The new attack

- The equation :

$$eX-(p-u)(q-v)Y=1.$$

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right).$$

# Comparison

## Wiener's attack

- The equation :

$$ed - (p-1)(q-1)k = 1.$$

- The method :
  The continued fraction algorithm
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{4}}\right).$$

## The new attack

- The equation :

$$eX - (p-u)(q-v)Y = 1.$$

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right).$$

# Comparison

## Wiener's attack

- The equation :

$$ed - (p-1)(q-1)k = 1.$$

- The method : The continued fraction algorithm
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{4}}\right).$$

## The new attack

- The equation :

$$eX - (p-u)(q-v)Y = 1.$$

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

$$\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right).$$

**Thank you for your attention**

**Merci**

شكرا